Federal Act on Combating Money Laundering and Terrorist Financing

Last change: 29.07.2026

PDF generated on: 14.10.2026

ONLINE COMMENTARY
THE OPEN ACCESS
LEGAL COMMENTARY

TABLE OF CONTENTS

Art. 2 para. 1 AMLA 5
Art. 2a para. 1-2 and 4-5 AMLA 25
Art. 2 para. 2 AMLA 51
Art. 2 para. 3 AMLA 75
Art. 3 AMLA 151
Art. 7 AMLA 205
Art. 7a AMLA 231
Art. 8 AMLA 245
Art. 8a AMLA 261
Art. 9 AMLA 275
Art. 11 AMLA 359
Art. 14 AMLA 369
Art. 15 AMLA 385
Art. 20 AMLA 395
Art. 23 AMLA 411
Art. 24 AMLA 439
Art. 24a AMLA 451
Art. 25 AMLA 459
Art. 26 AMLA 471
Art. 26a AMLA 479
Art. 27 AMLA 489
Art. 28 AMLA 501
Art. 29 AMLA 509
Art. 29a AMLA 527
Art. 29b AMLA 557
Art. 30 AMLA 565
Art. 31 AMLA 593
Art. 31a AMLA 601
Art. 32 AMLA 605

Art. 33 AMLA 611
Art. 34 AMLA 627
Art. 38 AMLA 645

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 2 para. 1 AMLA

A commentary by Thomas Nagel

SUGGESTED CITATION

Thomas Nagel, Commentary of art. 2 para. 1 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Nagel, art. 2 para. 1 AMLA N. XXX

Art. 2 Scope of application

[1] This Act applies to:

a. financial intermediaries;

b. natural persons and legal entities that deal in goods commercially and in doing so accept cash (dealers).

CONTENT

I. Addressees of the AMLA: basic idea 7
II. Financial intermediaries 7
A. General 7
B. Concept and system 9
C. Exemptions 10
D. Demarcation 11
E. Duties 12
III. Dealers 13
A. General 13
B. Concept and classification 14
C. Obligations 16
IV. Territorial application of the AMLA 17
V. Outlook: possible further expansion of the group of addressees 19
Bibliography 19
Materials 21

I. ADDRESSEES OF THE AMLA: BASIC IDEA

The AMLA came into force on April 1, 1998, in response to international pressure. The original purpose of the law was to recognize and, if possible, prevent the act of concealing the origin of assets by a perpetrator, and to supplement the criminal offenses of money laundering and lack of due diligence in financial transactions. The AMLA is primarily aimed at **combating money laundering** and **ensuring due diligence in financial transactions** (see the commentary on Art. 1 AMLA). For this purpose, the law is intended to cover persons who are not necessarily involved in the predicate offense of money laundering, but who are (may be) used by criminals after the commission of the predicate offense to allow assets of illegal origin to flow into the economic cycle and thus to conceal their origin or to either extend the so-called "paper trail" or not even allow it to arise. 1

The purpose of the AMLA was expanded as of February 1, 2009. It should also serve to combat the **financing of terrorism**. A further expansion of the article on the purpose of the law to include the prevention of violations of coercive measures under the Embargo Act was sent to the consultation process in 2023 and was also retained at the draft stage (2024); the corresponding draft will (as of August 2024) be discussed by parliament in the next few months. In my opinion, the extension of the scope to include another law should be rejected. The legal bases of the EmbA are sufficient; in addition, a mixing of the two laws (EmbA and AMLA) creates further ambiguities and places demands on the AMLA that it will not be able to fulfill. 2

The scope of application of the AMLA and the duties triggered by this law are specified at various levels: by means of **ordinances** (AMLO and AMLO-FINMA), **circulars** (in particular FINMA Circular 2011/1) and **self-regulation** (e.g. CDB 20 or various regulations of self-regulatory organizations). 3

II. FINANCIAL INTERMEDIARIES

A. General

When the AMLA was drafted, the legislator was faced with the challenge of identifying service providers susceptible to acts of concealment and designating them as concisely as possible. He chose the term "**financial intermedi-** 4

ary". The term "financial" refers to the financial and monetary system on the one hand, and to the entirety of the money and banking experts working in this area on the other. An "intermediary" is a person who acts as an intermediate link. In the wording of the law, financial intermediaries are therefore persons who can be assigned to the financial sector, who interpose themselves in transactions and who act in this capacity for third parties.

5 The term "financial intermediary" is practical because, on the one hand, it is open and not very specific and, on the other hand, it is somewhat concise. However, the **vagueness of the definition** of Art. 2 para. 3 AMLA (see below, N. 7 et seq., as well as the commentary on Art. 2 para. 3 AMLA) results in a delicate degree of legal uncertainty and, in certain cases, even a violation of the sufficient level of the norm. The legislator faces a dilemma when dealing with the risks of money laundering: he has to perform a balancing act between a scope that is as open as possible and one that is clearly defined. On the one hand, the regulation must be precisely tailored to the risks of specific activities and serve as a basis for interventions in economic freedom (and thus meet the requirements of Art. 36 FC), for which a high level of standardization is required. On the other hand, regulation must take into account the development dynamics and innovation potential in different sectors and be formulated as openly as possible for this purpose. Otherwise, minor changes to business models worthy of subordination could lead to an undesirable non-coverage by the AMLA. It is important that the legislator and the authorities carefully weigh these diametrically opposed interests. To make matters worse, Swiss legal tradition (compared to legislation in neighboring countries) tends to produce fairly concise laws, deliberately leaving room for interpretation by courts and authorities.

6 Since the AMLA came into force on April 1, 1998, financial intermediaries (the only category of service providers covered by the AMLA at the time) have had to comply with various **duties.** These include, on the one hand, a duty to document the contracting party and the beneficial owners of the assets, and on the other hand, the duty to file a report in the event of suspicion so that the authorities can take action. Contrary to popular belief, the AMLA is not a criminal law, but an economic administrative law. Anyone who violates the AMLA faces administrative (e.g. Art. 29 et seq. FINMASA) and, in certain cases, criminal consequences (Art. 37 and Art. 38 AMLA). Furthermore, anyone who violates AMLA obligations may also be liable to prosecution for money

laundering (Art. 305bis SCC) or for failing to exercise due diligence in financial transactions (Art. 305ter para. 1 SCC). The concept of a financial intermediary remains in force today. However, it has been continuously defined in more detail, and also expanded in tendency, but also restricted in some cases, by legislators and regulators, official practice (initially by the Anti-Money Laundering Control Authority and since January 1, 2009 by FINMA) and case law.

B. Concept and system

Financial intermediaries are named in Art. 2 para. 1 let. a AMLA and described in Art. 2 para. 2 and 3 AMLA. In theory and practice, financial intermediaries are designated differently in accordance with Art. 2 para. 2 and 3 AMLA. For example, the financial intermediaries under Art. 2 para. 2 AMLA are referred to as "financial intermediaries in the strict sense" and the financial intermediaries under Art. 2 para. 3 AMLA as "financial intermediaries in the broader sense" or as "other financial intermediaries". Officially, the legislator, the Federal Supreme Court and FINMA use the terms "financial intermediaries under special statutory supervision" for the financial intermediaries pursuant to Art. 2 para. 2 AMLA and "financial intermediaries not subject to special statutory supervision" for the financial intermediaries pursuant to Art. 2 para. 3 AMLA. In my opinion, however, these designations are inaccurate and no longer correct. The difference between the two categories of financial intermediaries is that the financial intermediaries falling under Art. 2 para. 2 AMLA are subject to **prudential supervision**, i.e. they have to comply with other financial market laws in addition to the AMLA (e.g. FinIA, FinSA or BankG). In the view presented here, the term "financial intermediaries under prudential supervision" (Art. 2 para. 2 AMLA) is therefore the most precise. By contrast, financial intermediaries within the meaning of Art. 2 para. 3 AMLA are subject to the supervision of self-regulatory organizations and are not prudentially supervised, but only with regard to the AMLA provisions. Consequently, they should be referred to as "financial intermediaries not subject to prudential supervision" or as "**financial intermediaries subject to the supervision of self-regulatory organizations**". 7

The financial intermediaries subject to prudential supervision are listed in Art. 2 para. 2 let. a–g AMLA. The **list of** financial intermediaries not subject to prudential supervision in Art. 2 para. 3 let. a–e AMLA, on the other hand, is not exhaustive, since Art. 2 para. 3 AMLA contains a general clause and the 8

subsequent list is introduced by the word "in particular". The general clause provides leeway for including newly emerging activities and services under the AMLA, provided that certain criteria are met.

9 Pursuant to the **general clause** of Art. 2 para. 3 AMLA, financial intermediaries are persons who, on a professional basis, accept or hold assets belonging to third parties or help invest or transfer them. According to the view presented here (and probably also the prevailing view), this definition is decisive for all financial intermediaries under the AMLA, including those under Art. 2 para. 2 AMLA. The term "professionally" is defined in Art. 7 et seq. AMLO. The term "financial intermediary" under Art. 2 para. 3 AMLA is further defined in FINMA-Circ. 2011/1, where FINMA publishes its interpretation of the term. The circular may only provide information on the application and interpretation of the authorities, but may not contain any legislative provisions, since circulars are so-called administrative ordinances. FINMA Circular 2011/1 has been in need of an update for some time, not least because certain of the laws and ordinances referenced in it have since been amended.

C. Exemptions

10 There are countless exemptions from the scope of application of the AMLA. At the **statutory level**, reference is made to Art. 2 para. 4 AMLA and to the commentary on these provisions. In summary, the following persons are not covered by the AMLA: the Swiss National Bank (lit. a); tax-exempted occupational pension funds (lit. b); persons who provide their services exclusively to tax-exempted occupational pension funds (lit. c); financial intermediaries in accordance with Art. 2 para. 3 AMLA, who provide their services exclusively to financial intermediaries in accordance with Art. 2 para. 2 AMLA or to foreign financial intermediaries who are subject to equivalent supervision (lit. d); as well as limited qualified investor funds (L-QIF) in the legal form of an investment company with variable capital (SICAV) or a limited partnership for collective investments (LLPCI) if the institution responsible for management in accordance with Art. 118h para. 1, 2 or 4 CISA assumes the obligations contained in this Act (lit. e).

11 Further exemptions from the scope of application are included in Art. 2 para. 2 AMLO at the **ordinance level**. Accordingly, persons who carry out the following activities are also not financial intermediaries within the meaning of Art. 2 para. 3 AMLA and are exempt from the AMLA: The purely physical

transport or the purely physical storage of assets, subject to Art. 6 para. 1 let. c AMLO (let. a no. 1), collection activities (let. a no. 2), the transfer of assets as an accessory provision to a principal contractual service (let. a no. 3), the operation of pillar 3a pension schemes by bank foundations or insurance companies (lit. a no. 4), the provision of services between group companies (lit. a no. 5) and, subject to certain conditions, the activity as an auxiliary of a financial intermediary (lit. b). These exceptions are further specified in FINMA Circular 2011/1.

D. Demarcation

The concept of financial intermediary must be clearly distinguished from that of **dealer** (see N. 18 et seq.). A person cannot be a financial intermediary and a dealer at the same time for the same activity or service. If he is a financial intermediary and a dealer (e.g. because he trades in certificated securities and thus *de facto* fulfills the conditions of both Art. 2 para. 3 let. c AMLA and Art. 2 para. 1 let. b AMLA), he must comply with the obligations for financial intermediaries. In other words, the provisions for dealers are subsidiary to the provisions for financial intermediaries. Traders usually act as dealers; however, dealers are not usually financial intermediaries, unless they deal in banknotes and coins, money market instruments, foreign exchange, precious metals, commodities and securities (certificated and uncertificated) and their derivatives (Art. 2 para. 3 let. c AMLA). Accordingly, the potential for overlap between the provisions on dealers and those on financial intermediaries is limited. 12

Similarly, a distinction must be made between dealers and **financial service providers** under the FinSA and financial institutions under the FinIA: not all financial service providers fall under the AMLA, but only those that act as financial intermediaries. By contrast, financial institutions such as asset managers, trustees, securities firms and fund management companies are always subject to the AMLA due to the reference in Art. 2 para. 2 let. a^{bis}, b and d AMLA and are financial intermediaries under prudential supervision. The FinSA, in turn, ties in with the concept of financial intermediaries in the provisions on client segmentation (Art. 4 para. 3 let. a FinSA). 13

The criminal offence of lack of due diligence in financial transactions (Art. 305ter para. 1 SCC) contains a definition of the category of perpetrators that 14

corresponds to the general clause of Art. 2 para. 3 AMLA. However, the SCC does not use the term "financial intermediary".

E. Duties

15 Financial intermediaries shall be subject to the duties set forth by the law. These duties are divided into **due diligence obligations** (Art. 3 et seq. AMLA), such as the identification of the contracting party (Art. 3 AMLA), the identification of the beneficial owner (Art. 4 AMLA), the renewed identification or verification of the identity of the beneficial owner (Art. 5 AMLA), special due diligence requirements (Art. 6 AMLA), the documentation requirement (Art. 7 AMLA) and organizational measures (Art. 8 AMLA). The due diligence requirements must be complied with at all times.

16 Furthermore, there are **obligations that** only apply **in cases of suspected money laundering**. These are the reporting requirement (Art. 9 para. 1 AMLA), with special rules on customer orders (Art. 9a AMLA) and the termination of the business relationship (Art. 9b AMLA), the freezing of assets (Art. 10 AMLA) and the prohibition of information (Art. 10a AMLA).

17 The AMLA provides for various **supervisory concepts**: the financial intermediaries pursuant to Art. 2 para. 2 AMLA are supervised by a **federal authority** (e.g. FINMA or the SFGB, see Art. 12 AMLA). Asset managers and trustees under FinIA (Art. 2 para. 2 let. a^{bis} AMLA) are subject to ongoing supervision by a supervisory organization, which in turn is authorized and supervised by FINMA (Art. 61 para. 1 and 2 FinIA). The supervision is prudential, i.e. it relates to a variety of financial market laws and not just to the AMLA. FINMA can open enforcement proceedings against financial intermediaries in accordance with Art. 2 para. 2 AMLA and take the measures in accordance with Art. 29 et seq. FINMASA if AMLA obligations are violated.

18 By contrast, financial intermediaries as defined in Article 2, para. 3 AMLA are supervised by **self-regulatory organizations** (see Article 12, let. c in conjunction with Article 24 AMLA) and are subject only to the AMLA as the only financial market law. In the event of violations of the AMLA or the self-regulatory organization regulations, the measures provided for in the regulations of the self-regulatory organization (e.g. reprimand or exclusion) will generally apply. However, anyone who acts as a financial intermediary without being affiliated to a self-regulatory organization may also be subject to enforcement

measures by FINMA within the meaning of Art. 29 et seq. FINMASA pursuant to Art. 20 para. 1 AMLA.

III. DEALERS

A. General

Until December 31, 2015, the AMLA applied exclusively to financial intermediaries. On January 1, 2016, this paradigm, which had been in force for almost 16 years, was changed: Dealers were added to Art. 2 para. 1 lit. b AMLA as part of the Federal Act of December 12, 2014, for the Implementation of the 2012 Revised Recommendations of the Financial Action Task Force. By including dealers and by deleting the passage "in the financial sector" in the title of the AMLA as of January 1, 2016, the scope of the AMLA (nota bene a financial market law according to Art. 1 para. 1 lit. f FINMASA) was deliberately extended to **activities outside the financial sector**. In addition, the addition "for financial intermediaries" was deleted from the title of the obligations under the AMLA. Critics feared (in my opinion, rightly so) that the "Pandora's box" would be opened if, for the first time, dealers were to be covered by the AMLA. This is a trend that is (and was) continuing (which was already foreseeable at the time). 19

While the **GAFI** recommendations, even in their current version, do not necessarily cover all traders, but only precious metal and precious stone traders who accept cash in the amount of 15,000 euros or more, the **EU** has already so-called Third Money Laundering Directive (2005/60/EC) a stricter approach and subjected goods dealers to certain due diligence requirements if the transaction amount exceeded EUR 15,000. This threshold was lowered to EUR 10,000 with the Fourth Money Laundering Directive (Directive (EU) 2015/849). In the future, there should even be an upper limit for cash payments in the EU. The EU thus mistrusts the cash purchase of goods of any category, while the FATF leaves it to the states to define, in addition to precious metals and precious stones, further goods for the cash sale of which obligations are introduced. 20

The Federal Council's original proposal was to introduce a cash ban for amounts over CHF 100,000. This proposal was rejected by parliament. In the parliamentary debate, the parliamentarians agreed to impose due diligence requirements on traders instead of banning cash payments for amounts over 21

CHF 100,000. Cash payments will therefore remain possible without restriction for the time being. This **compromise solution** has been criticized as "half-hearted" in some quarters (see also the commentary on Art. 38 N. 13 f.), but it has also been welcomed.

B. Concept and classification

22 In simple terms, the reason why dealers are subject to the Act is to prevent criminal organizations from converting money of criminal origin into (luxury) goods. From an **objective point of view**, anyone who trades in goods and accepts cash in the process is deemed to be a dealer under Article 2 paragraph 1 letter b AMLA. However, this does not mean that every dealer is covered by the AMLA: AMLA only applies to persons who, in the course of their commercial activities as dealers in goods, accept cash in excess of CHF 100,000 (see Art. 8a para. 1 AMLA). A single purchase transaction in excess of CHF 100,000 is sufficient to trigger the application of AMLA. Staggering the purchase price into several tranches of less than CHF 100,000.01 also results in the trader being subject to the AMLA (Art. 8a, para. 3 AMLA): as soon as several transactions between the same parties are closely connected in terms of time or economic purpose, the partial amounts are added together, which may result in the seller being recorded as a trader. According to Art. 15 AMLO, goods are movable or immovable objects that can be the subject of a sale of movables or a sale of real estate. This excludes claims and uncertificated securities, unless they are securitized in a document. Furthermore, there must be a purchase or commission transaction in the course of which the dealer sells at least one "good" in the aforementioned sense. Service contracts are not covered. The dealer must accept cash. Cash includes all legal tender with a compulsory exchange rate, i.e. coins issued by the federal government and banknotes issued by the Swiss National Bank (Art. 2 WZG). Foreign currencies that are in circulation as physical means of payment are also considered cash under Art. 2 para. 1 let. b AMLA. If the purchase price is accepted through a financial intermediary (and not directly by the merchant), the AMLA merchant provisions do not apply to the goods merchant (Art. 8a para. 4 AMLA). Dealers thus have a choice: either they accept the cash and have to fulfill the AMLA obligations, or they persuade their customers to pay the debt through a financial intermediary (e.g. by bank transfer). The activity of the dealer must be commercial, i.e. the sale must be in connection with an independent economic activity aimed at making a profit (Art. 14 para. 1 AMLO). However, it is

irrelevant (in contrast to certain financial intermediary activities) whether the activity is accessory or not (Art. 14 para. 2 AMLO).

Both natural persons and legal entities are classified as dealers in **personal terms**. These are primarily dealers who, in their own name and for their own account (possibly through auxiliary persons), carry out purchase transactions. However, dealers also include persons who conclude a purchase contract on behalf of and for the account of a third party and thus in indirect representation, in accordance with Art. 13 AMLO. Art. 13 AMLO is to be understood in the sense that persons who conclude purchase agreements in their own name but on behalf of a third party (sale on behalf of a third party) are themselves considered dealers within the meaning of AMLA. According to the intention of the legislator, the provision is intended in particular to cover auctioneers and auction houses that carry out the purchase transaction for the seller of an item. The involvement of third parties in accordance with Art. 16 AMLO must be distinguished from the sale on behalf of a third party. In this constellation, the third party acts on behalf of a third party, is involved solely for the purpose of processing the purchase transaction and is therefore not to be classified as a dealer. He is not subject to the AMLA. Rather, it is the dealer's responsibility to ensure that the third party commissioned with the transaction complies with the due diligence requirements as defined in Art. 8a AMLA (Art. 16 AMLO). This obligation is a type of “principal's liability”. If a sale is made on behalf of a third party, it is generally a commission transaction (Art. 425 CO). Since the commission agent purchases and sells in his own name but on behalf of the principal, the commission agent is subject to the dealer provisions in accordance with Art. 13 AMLO. Brokers, on the other hand, are not covered (Art. 412 et seq. CO), since they merely provide evidence of an opportunity to conclude a contract or broker the conclusion of a contract without themselves being a party to the contract. In my opinion, the same should apply by analogy to agency contracts (Art. 418a ff. CO), in that the agents within the meaning of Art. 16 AMLO should be qualified as auxiliaries of a dealer, who is responsible for ensuring that the agents comply with the duties of due diligence in accordance with Art. 8a AMLA. In my opinion, however, the agents themselves should not be classified as dealers, since they do not accept cash or conclude legal transactions in their own name, but in the name of a third party. If an order exists (Art. 394 ff. CO), the agent always acts for the account and at the risk of the principal. Accordingly, the question of whether the agent should be recorded as a trader depends on whether they are acting

23

in their own name or in the name of a third party. In principle, both constellations are possible under the law of agency. The subject of agency without authority (Art. 419 et seq. CO) can also be legal acts. In such a case, the agent always acts in their own name, which is why, in my opinion, they can be recorded as a trader. If there is an exclusive distribution contract, the exclusive agent acts in his own name and on his own account; in my opinion, he is therefore considered to be a dealer himself, without Articles 13 and 16 AMLO applying. These statements also apply to the junk dealer in a junk contract, who also always acts in his own name and on his own account.

C. Obligations

24 In contrast to the financial intermediaries, who must comply with a large number of obligations of the AMLA, dealers (in accordance with the lower risk compared to most financial intermediaries) are only subject to the **due diligence obligations** mentioned in Art. 8a para. 1 AMLA. These are the identification of the contracting party (Art. 3 para. 1 AMLA), the identification of the beneficial owner (Art. 4 para. 1 and 2 lit. a and b AMLA) and the documentation requirement (Art. 7 AMLA). The law explicitly refers to the obligations that apply to financial intermediaries for these obligations. Deviations for dealers can only be assumed if the law or the ordinances explicitly define different rules for them. Please refer to the comments on Art. 8a AMLA.

25 Dealers are also subject to a **reporting requirement** in the event of suspicious circumstances as defined in Art. 9 para. 1bis AMLA. The reasons that trigger a reporting requirement are identical to those of Art. 9 para. 1 let. a no. 1–4 AMLA. Traders are also subject to the prohibition of information after reporting (Art. 10a para. 5 AMLA). Violation of the reporting requirement will result in criminal prosecution (Art. 37 AMLA). Please refer to the comments on Art. 9, 10a and 37 AMLA.

26 Since dealers are not supervised by a federal authority such as FINMA or a self-regulatory organization, they are subject to an **audit requirement**. They must commission an audit firm to verify that they are complying with their obligations under Chapter 2 of the Act (Art. 15 para. 1 AMLA). Violation of the duty under Art. 15, para. 1 AMLA is subject to criminal prosecution (Art. 38 AMLA). Please refer to the comments on Art. 15 and Art. 38 AMLA.

IV. TERRITORIAL APPLICATION OF THE AMLA

The law does not contain any provisions on the territorial application of the AMLA. However, Art. 2 AMLO contains provisions in this regard. Art. 2 para. 1 let. a and b AMLO stipulates that financial intermediaries (pursuant to Art. 2 para. 2 and para. 3 AMLO) and dealers (pursuant to Art. 2 para. 1 let. b AMLO) must be active **in Switzerland or operating from Switzerland** in order to fall under the AMLO. The scope defined in AMLO actually only refers to the scope of AMLO. However, according to the view presented here, it makes sense to also apply the description of the geographical scope to AMLA itself. Pursuant to Article 5 AMLO-FINMA, the AMLA has a spillover effect for branches or group companies abroad – the financial intermediary must ensure that such companies comply with the AMLO-FINMA principles. Furthermore, the risks must be monitored globally in accordance with Article 6 AMLO-FINMA. 27

FINMA Circular 2011/1 explains how the geographical scope is interpreted by FINMA. Accordingly, a person is deemed to be operating in or from Switzerland if they are domiciled or registered in Switzerland; or if they employ persons in Switzerland who permanently carry out activities subject to the AMLA in or from Switzerland or can legally obligate them to do so (de facto branch). This includes business premises of companies that are constituted under foreign law and have their main business premises abroad, but which pursue an activity requiring a license here without having formally established a branch. A de facto branch also includes persons who regularly assist the foreign financial intermediary in Switzerland or from Switzerland in carrying out essential elements of the financial intermediary activity, such as receiving or handing over assets or providing financial intermediary services. The published FINMA practice does not explain the duration required for a de facto branch to be established, but it does explicitly assume permanence. In practice, there is a great deal of uncertainty in this regard. In my opinion, however, it is necessary that a certain threshold be exceeded with regard to both the absolute duration and the regularity of the presence. According to the FINMA practice, the following circumstances, for example, fall within the territorial scope of the AMLA: (i) a foreign money transmitter uses a network of agents in Switzerland to accept or disburse funds in its name; (ii) a foreign company issues prepaid cards and distributes them through a point of sale in Switzerland; (iii) a person in Switzerland concludes loan agreements with cus- 28

tomers for a foreign company or accepts repayments for the company based on a loan agreement. On the other hand, the following situations, for example, do not fall within the territorial scope of AMLA according to FINMA practice: (i) an asset manager operating and licensed abroad is authorized by his client to dispose of the assets deposited in a Swiss bank account; (ii) a banknote dealer operating and licensed abroad supplies banknotes to a customer in Switzerland; (iii) a financial intermediary operating and licensed abroad offers financial intermediary services in Switzerland exclusively via the internet or other electronic channels; (iv) a foreign asset manager comes to Switzerland temporarily to look after his clients here.

29 By implication, it can therefore be stated that activities carried out exclusively across Switzerland's borders from abroad for customers in Switzerland ("**cross-border**") do not trigger any AMLA obligations.

30 In principle, the same rules apply to dealers as to financial intermediaries (see the wording of Art. 2 para. 1 let. b AMLO). However, according to the Federal Council's understanding, it is not the domicile/residence of the dealer or the duration of the presence in Switzerland that is significant, but the **place of execution**. According to this view, as soon as a trader accepts more than CHF 100,000 in cash in the course of a transaction that is processed in Switzerland, the elements of the offense under Art. 8a AMLA would be fulfilled and the seller would have to fulfill the corresponding AMLA obligations, even if he had traveled from abroad. This view is in part welcomed or not further critically assessed in legal doctrine, but in part also criticized. The criticism refers above all to the fact that the place of the transaction is a weak connecting criterion. Furthermore, it is absurd to provide for tougher rules for dealers (who generally exhibit a lower risk than most financial intermediaries). Furthermore, it is impossible to impose and enforce AMLA obligations on dealers who do not have their domicile or registered office in Switzerland. In particular, it would be absurd to commission an audit firm to audit Swiss law. This is to be agreed.

31 In general, it would be desirable if the geographical scope were more precisely specified and defined at the legislative level. This would be necessary due to the requirement of a sufficient level of legislation for serious encroachment on economic freedom (see Art. 36 para. 1 FC).

V. OUTLOOK: POSSIBLE FURTHER EXPANSION OF THE GROUP OF ADDRESSEES

32 The FATF Recommendations require that certain advisory services be covered by anti-money laundering law (see Recommendation 22 [due diligence], Recommendation 23 [reporting obligations] and Recommendation 28 [supervision]). After similar initiatives were launched in Switzerland in 2019 but ultimately failed in parliament, a bill to strengthen the fight against money laundering was submitted for consultation in fall 2023. The (provisional) result is the message on the Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners. In addition to the creation of a transparency register (to be introduced by the so-called Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners, or TJPG for short), so-called "**advisers**" are to be newly included as a separate group of addressees by the AMLA. Advisers include lawyers, notaries and other service providers who offer legal or accounting advice when they are professionally involved in planning or executing a specified transaction for clients. Examples of reportable transactions include the purchase of real estate, the formation or management of a company, foundation or trust, the organization of a company's fundraising, and the purchase and sale of a company. An exception to the reporting requirement is provided for professions that are subject to professional confidentiality. On the other hand, any service provider is also a so-called "consultant" if they establish a company, a foundation or a trust; if they provide a company, foundation or trust with a domicile or premises; or if they act as a shareholder in a fiduciary capacity. Although the bill fulfills the FATF recommendations, it has been met with fierce **criticism**, particularly from various professional associations.

BIBLIOGRAPHY

Burckhardt Peter/Hösli Andreas, Neue strafrechtliche Risiken für Händler bei Barzahlungen über CHF 100'000, in: Jusletter vom 1.2.2016.

De Capitani Werner, Kommentierung zu Art. 2 GwG, in: Schmidt Niklaus (Hrsg.), Kommentar Einziehung – Organisiertes Verbrechen – Geldwäscherei, Bd. I, 2. Aufl., Zürich et al. 2007 (zit. KEOVG II-De Capitani, Art. 2 GwG).

Hilf Marianne, Kommentierung zu Art. 38, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar zum Geldwäschereigesetz

(GwG), Bundesgesetz vom 10. Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Bern 2017 (zit. SHK-Hilf, Art. 38 GwG).

Kunz Michael, Umsetzung der GAFI-Empfehlungen 2012, die Geldwäschereiprävention verlässt den Finanzsektor, in: Jusletter vom 23.2.2015 (zit. Kunz, Jusletter 23.2.2015).

Lutz Peter, Die Anwaltschaft zwischen Berufsgeheimnis und Aufsichtszwang – eine Fahrt zwischen Skylla und Charybdis, 12. Zürcher Tagung zur Geldwäschereibekämpfung, Europa Institut der Universität Zürich, 1.10.2024.

Nagel Thomas, Der persönliche und sachliche Geltungsbereich des schweizerischen Geldwäschereigesetzes: Mit rechtsvergleichenden Hinweisen zu internationalen Standards, dem Recht der Europäischen Union und dem deutschen Recht, Zürich et al. 2020 (zit. Nagel, Geltungsbereich).

Nagel Thomas, Gesetzesentwurf für das Transparenzregister, Jusletter vom 2.12.2024 (zit. Nagel, Jusletter).

Nagel Thomas, Vernehmlassungsvorlage zur Stärkung der Geldwäscherei-Bekämpfung bzw. Transparenzregister: Würdigung des Vorentwurfs, RRCO 6 (2023), S. 1–4 (zit. Nagel, RRCO 6/2023).

Peyer Martin, Kommentierung zu Art. 2 Abs. 1 lit. a, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz, Basel 2021 (zit. BSK-Peyer, Art. 2 Abs. 1 lit. a GwG).

Ramelet Nicolas, Kommentierung zu Art. 2 Abs. 1 lit. b, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz, Basel 2021 (zit. BSK-Ramelet, Art. 2 Abs. 1 lit. b GwG).

Ramelet Nicolas, Sorgfaltspflichten für «Händler» – Auslegeordnung einer Kompromisslösung, AJP 2015, S. 1160–1167 (zit. Ramelet, AJP 2015).

Schären Simon, Kommentierung zu Art. 2, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar zum Geldwäschereigesetz (GwG), Bundesgesetz vom 10. Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Bern 2017 (zit. SHK-Schären, Art. 2 GwG).

Schott Ansgar/Kessler Martina A., Kommentierung zu Art. 8a, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar zum Geldwäschereigesetz (GwG), Bundesgesetz vom 10. Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Bern 2017 (zit. SHK-Schott/Kessler, Art. 8a GwG).

Wyss Ralph, Kommentierung zu Art. 2, in: Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Geldwäschereigesetz mit weiteren Erlassen (GwG), 3. Aufl., Zürich 2019 (zit. OFK-Wyss, Art. 2 GwG).

Zysset Pascal/Nagel Thomas, Der räumliche Geltungsbereich des Geldwäschereigesetzes, GesKR 2018, S. 140–155.

MATERIALS

Amtliches Bulletin Nationalrat 2014, abrufbar unter https://www.parlament.ch/centers/documents/de/NR_4916_1412.pdf, besucht am 31.8.2024 (zit. AB 2014 NR).

Amtliches Bulletin Ständerat 2014, abrufbar unter https://www.parlament.ch/centers/documents/de/SR_4916_1412.pdf, besucht am 31.8.2024 (zit. AB 2014 SR).

Botschaft zur Änderung des Geldwäschereigesetzes vom 26.6.2019, BBl 2019 5451 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2019/1932/de, besucht am 31.8.2024 (zit. Botschaft GwG 2019).

Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG) vom 17.6.1996, BBl 1996 III 1101 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1996/3_1101_1057_993/de, besucht am 31. August 2024 (zit. Botschaft GwG 1996).

Botschaft zum Bundesgesetz über die Transparenz juristischer Personen und die Identifikation der wirtschaftlich berechtigten Personen, nicht datiert (Vorabdruck), 2024, abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/87770.pdf, besucht am 31.8.2024 (zit. Botschaft TJPG 2024).

Botschaft zur Umsetzung der 2012 revidierten Empfehlungen der Groupe d'action financière (GAFI), BBl 2014 605 ff., abrufbar unter https://

www.fedlex.admin.ch/eli/fga/2014/100/de, zuletzt besucht am 31.8.2024 (zit. Botschaft GAFI 2013).

Botschaft zur Umsetzung der revidierten Empfehlungen der Groupe d'action financière (GAFI), BBl 2007 6295 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2007/938/de, besucht am 31.8.2024 (zit. Botschaft GAFI 2007).

Erläuterungsbericht zur Geldwäschereiverordnung (GwV) – Umsetzung der GAFI-Empfehlungen vom 11.11.2015, abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/41723.pdf, besucht am 31.8.2024 (zit. Erläuterungsbericht GwV 2015).

EXPERTsuisse, Ausgewählte Fragen und Antworten zu den Auswirkungen der Anpassungen des Geldwäschereigesetzes auf die Prüfung von Händlerinnen und Händlern, 23.6.2016 (zit. EXPERTsuisse).

FINMA, Rundschreiben 2011/1, Tätigkeit als Finanzintermediär nach GwG: Ausführungen zur Geldwäschereiverordnung (GwV), 20.10.2010, zuletzt geändert am 4.11.2020, abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2011-01-01-01-2017.pdf?sc_lang=de&hash=C13E76F1B7CE20DFB9B822526B383187, besucht am 31.8.2024 (zit. FINMA-RS 2011/1).

GAFI/FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation vom 16.2.2012, aktualisiert im November 2023, abrufbar unter https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf, zuletzt besucht am 31.8.2024 (zit. GAFI-Empfehlungen).

Praxis der Kontrollstelle für die Bekämpfung der Geldwäscherei zu Art. 2 Abs. 3 GwG: Der Geltungsbereich des Geldwäschereigesetzes im Nichtbankensektor, 29.10.2008 (mittlerweile ausser Kraft gesetzt), abrufbar unter https://www.finma.ch/FinmaArchiv/gwg/d/dokumentationen/publikationen/gwg_auslegung/pdf/59402.pdf, besucht am 31.8.2024 (zit. Kst, Unterstellungskommentar).

Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken zwischen der Schweizerischen Bankiervereinigung (SBVg) einerseits und den un-

terzeichnenden Banken andererseits, vom 13.6.2018, abrufbar unter https://www.swissbanking.ch/_Resources/Persistent/e/2/5/4/e254d3078d72c23dcbc13352a34223c518303ec8/SBVg_Vereinbarung_VSB_2020_DE.pdf, besucht am 31.8.2024 (zit. VSB 20).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 2a para. 1-2 and 4-5 AMLA

A commentary by Florian Adank

SUGGESTED CITATION

Florian Adank, Commentary of art. 2a para. 1-2 and 4-5 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Adank, art. 2a para. 1-2 and 4-5 AMLA N. XXX

Art. 2*a* Definitions

[1] Politically exposed persons in terms of this Act are:

a. individuals who are or have been entrusted with prominent public functions by a foreign country, such as heads of state or of government, senior politicians at national level, senior government, judicial, military or political party officials at national level, and senior executives of state-owned corporations of national significance (foreign politically exposed persons);

b. individuals who are or have been entrusted with prominent public functions at national level in Switzerland in politics, government, the armed forces or the judiciary, or who are or have been senior executives of state-owned corporations of national significance (domestic politically exposed persons);

c. individuals who are or have been entrusted with a prominent function by an intergovernmental organisation or international sports federations, such as secretaries general, directors, deputy directors and members of the board or individuals who have been entrusted with equivalent functions, (politically exposed persons in international organisations)

[2] The family members and close associates of politically exposed persons are individuals who are closely connected to persons under paragraph 1 either through their family or for social or professional reasons.

[4] Domestic politically exposed persons are no longer regarded as being politically exposed in terms of this Act when 18 months have elapsed since they relinquished their position. The general duties of due diligence for financial intermediaries are reserved.

[5] An international sports federation in terms of paragraph 1 letter c is the International Olympic Committee and the non-governmental organisations that it recognised that regulate one or more official sports at global level.

CONTENT

I. Background 28
A. Rationale 28
B. International development 29
C. The "Supervisors' PEP Working Paper 2001" 29
D. The "Wolfsberg AML Principles" 30
E. The "Customer Due Diligence for Banks" 31
F. The United Nations Convention Against Corruption 31
G. The 2003 FATF Recommendations 31
H. The 2012 FATF recommendation: PEPs within domestic public life and PEPs within international organizations 32
I. The term PEP in the European Union 33
J. The PEP term in Switzerland 35
II. Elements of the PEP concept 35
III. PEP abroad 37
A. A leading public function at the national level 37
B. Governing bodies of state-owned enterprises of national importance 39
IV. Domestic PEP 40
V. Intergovernmental organizations 42
VI. International Sports Federations 43
VII. Close associates 44
VIII. End of PEP status 46
Bibliography 48
Materials 49

I. BACKGROUND

A. Rationale

1 Article 2a AMLA implements the recommendation of the Financial Action Task Force (FATF) formulated in 2012. The federal law was adopted on December 12, 2014, and has been in force since January 1, 2016. The article defines the term **politically exposed person** (hereinafter **"PEP"**) at the legislative level.

2 PEP was not a new concept at the time the law was passed. However, the term was not consistently defined in the regulations. Before its adoption, the term PEP was defined in Art. 2 para. 1 let. a no. 1 and 2 AMLO-FINMA and in Art 10 para. 4 let. a and b of the Anti-Money Laundering Ordinance of the Federal Gaming Board (AMLO-FGB). The GwV-FINMA was aimed at financial intermediaries in accordance with Article 2 para. 2 AMLA and asset managers of collective assets, insurance institutions and securities dealers, as well as directly subordinated financial intermediaries (DSFIs) in accordance with Article 2 para. 3 AMLA. The AMLO-CFB was aimed at casinos in accordance with Article 2 para. 2 let. e AMLA. The definition did not apply to members of self-regulatory organizations to which neither GwV-FINMA nor GwV-ESBK applied. The regulation at the legislative level therefore enabled a **binding and uniform regulation of the term for all financial intermediaries** from 2016 onwards.

3 Only natural persons can be 3PEPs. Due to their position or function, they have influence within a state apparatus and have access to public funds or can award state contracts. A PEP therefore has an **increased risk** of misusing public funds for private gain or taking bribes and laundering the funds obtained in the national and international financial system. **Family members of a PEP or their close associates** may assist in hiding the funds or unlawfully profit from the PEP's influence and position. Because a PEP or a close associate may be the subject of increased media coverage, a business relationship with a PEP also exposes the financial intermediary to an increased reputational risk. To address and limit these risks, national and international institutions have defined standards for financial intermediaries for business relationships with PEPs. The measures are aimed at recognizing a business relation-

ship with a PEP and preventing illicit funds from being laundered through the national or international financial system.

B. International development

Switzerland played a major role in the development of international standards with regard to PEPs. This development was driven not least by far-reaching events for the Swiss financial center in connection with PEPs. At the end of the 1990s, it was revealed that some of the assets of the late Nigerian military dictator Sani Abacha were held in Swiss bank accounts. In view of this, a meeting was held in Lausanne in November 2000 at Switzerland's initiative with representatives of the judicial and banking supervisory bodies of Canada, France, Germany, Switzerland and the United Kingdom. The outcome of this meeting was the "**Supervisors' PEP Working Paper 2001**", which was published in November 2001. The document established the bases for identifying PEPs and the measures for limiting the associated risks. 4

C. The "Supervisors' PEP Working Paper 2001"

The introductory remarks of the "Supervisors' PEP Working Paper 2001" pointed out the urgency of regulating this area. The abuse of the financial system through the laundering of the proceeds of corruption or the misappropriation of public funds for private purposes is a matter of concern for the regulatory authorities. The document was therefore intended to help the regulatory authorities to identify the clients of financial intermediaries who are particularly affected by the risks mentioned and to recommend measures to limit the associated risks. It defined a PEP **as a natural person who is or has** been entrusted with a prominent public function, such as heads of state, high-ranking politicians, officials, representatives of the judiciary and military or members in leading positions of state-owned enterprises, as well as important officials of a party. The definition explicitly included individuals at high levels, not at lower or middle levels, of the hierarchy. Family members of PEPs or persons close to PEPs were mentioned, but the assessment of the risks associated with this relationship to the PEP was not the same as for PEPs. In this context, the "Supervisors' PEP Working Paper 2001" used the subjunctive, i.e. business relationships with family members of PEPs or persons close to PEPs *could pose* the same reputational risk as a business relationship with the PEP itself. The definition explicitly included all legal forms controlled by a PEP or 5

for which a PEP is the beneficial owner. Because the usual checks for opening and the measures for monitoring a business relationship do not correspond to the risks of a business relationship with a PEP, the "Supervisors' PEP Working Paper 2001" recommended special measures for checking and monitoring business relationships with PEPs. The decision to authorize the opening of a business relationship with a PEP should be made by a member of the management. In addition, the approval for the continuation of the business relationship should be renewed annually at the same hierarchical level. However, these measures only applied to business relationships with PEPs with a function in a country that was not the same as the domicile of the account-holding financial intermediary ("non-resident PEP"). Business relationships with a PEP with a function in a country that was identical to the domicile of the account-managing financial intermediary ("local PEPs") were therefore explicitly excluded from the measures.

D. The "Wolfsberg AML Principles"

6 In October 2000, the Wolfsberg Group, an association of 11 global banks at the time, published the Wolfsberg AML Principles. The Wolfsberg Group is named after the location of its first meeting, Wolfsberg Castle in the canton of Thurgau in Switzerland. The organization develops and defines rules for "Know Your Customer" (KYC) and for directives to combat money laundering and terrorist financing. The guidelines have become the standard in the international financial industry. The "Wolfsberg AML Principles" of October 2000 were the association's first publication. In this document, the term "public official" was mentioned as a customer group for which special monitoring measures were to be taken due to the risks associated with this function. The functions associated with this term are almost identical to those of the "Supervisors' PEP Working Paper 2001". In contrast to the "Supervisors' PEP Working Paper 2001", however, the definition also included **family members of a "public official" or persons close to them**. The definition in the "Wolfsberg AML Principles" made no distinction as to whether the business relationship involved a "public official" in the home country or abroad. The term "PEP", which was used for the first time in the aforementioned "Supervisors' PEP Working Paper 2001", was to become established, however. In the guidelines on the subject published in the following years, the Wolfsberg Group also used the term PEP. In 2003, the "Guidance on Politically Exposed Persons (PEP)" and in 2008 the "Frequently Asked Questions (FAQ) on Politi-

cally Exposed Persons (PEP)" were published. Both publications were replaced in 2017 by the "Wolfsberg Group PEP Guidance".

E. The "Customer Due Diligence for Banks"

One month before the publication of the "Supervisors' PEP Working Paper 2001", the working group of the Basel Committee on Banking Supervision and representatives of the Association of Offshore Centers had published the "Customer Due Diligence for Banks". The document published in October 2001 also contained a definition of PEP, which already included the functions for PEP mentioned in the "Supervisors' PEP Working Paper 2001". However, it included **"persons or companies apparently associated with a PEP"**. The definition contained therein was supplemented with a reference to the risks associated with business relationships with PEPs, especially those from countries where corruption is widespread. 7

F. The United Nations Convention Against Corruption

In 2003, the United Nations Convention against Corruption (UNCAC) was adopted in New York. Switzerland acceded to the UNCAC in September 2009. With the agreement, Switzerland is committed to fighting corruption. In this sense, Art. 52 para. 1 stipulates that Switzerland requires financial institutions to "conduct enhanced due diligence on accounts requested or maintained by or for persons who are or have been entrusted with prominent public functions and their family members and close associates". The Convention does not define PEP. Rather, it addresses corruption by persons who exercise a public office in general terms. Consequently, there is a close connection to the topic of PEPs. 8

G. The 2003 FATF Recommendations

The most significant initiative on the topic of PEPs came from the Financial Action Task Force (FATF). The FATF was founded in 1989 by the leading industrial nations of the time, Germany, France, Italy, Japan, Canada, the United Kingdom and the United States. The FATF sets out rules for combating money laundering, terrorist financing and the financing of weapons of mass destruction, which it publishes in the form of recommendations and continuously updates. It regularly monitors compliance with its rules in the member states and publishes the results. The FATF currently has around 40 member states. More 9

than 200 countries and jurisdictions have now committed to implementing the FATF rules.

10 Since 1990, the FATF has published its recommendations for combating money laundering. In October 2001, the FATF added further explanations or guidelines to combat terrorist financing. Due to the constantly changing threats, the FATF has continuously updated its recommendations ever since. The Forty Recommendations published in 2003 contained a definition of PEP with mostly already known elements. The examples of a PEP-relevant function listed in the definition were the same as those mentioned in the "Supervisors' PEP Working Paper 2001" of October 2001. The restriction from the paper of the same name, that a PEP is exclusively a person at a high, and not medium or low, level of the hierarchy, was adopted in the definition. The FATF's definition was limited to **natural persons and their close associates who perform a relevant function abroad**. In view of the known risks associated with business relationships with PEPs or close associates of PEPs, the FATF recommended that members of senior management should authorize the opening of such business relationships. In contrast to the "Supervisors' PEP Working Paper 2001", the FATF did not distinguish between a business relationship with a natural person who is close to a PEP for family or other reasons and a business relationship with the PEP himself when assessing reputational risks. Business relationships with persons close to PEPs therefore entail the same reputational risks as a business relationship with the PEP himself.

H. The 2012 FATF recommendation: PEPs within domestic public life and PEPs within international organizations

11 In the explanatory notes to the recommendations published in 2003, the FATF advised that the PEP term and the associated measures should also be extended to a PEP with a function within domestic public life. In the updated 40 Recommendations of February 2012, the FATF extended the term to include a domestic PEP, i.e. a natural person who is entrusted with a prominent public function at domestic level. This includes heads of state, high-ranking politicians, officials, representatives of the judiciary and military or members in leading positions of state-owned enterprises, as well as important officials of a party. **A domestic PEP differs from a foreign PEP in terms of the country that has granted the function, taking into account the domicile**

of the financial intermediary with whom the PEP has a business relationship. If the same PEP has a bank managing his/her account abroad, then the bank in question regards the PEP as foreign. Both the PEP abroad and the PEP in the home country are functions of a higher and not middle or lower hierarchy level. In this recommendation, the FATF also designated for the first time a person who holds a leading position in an international organization as a PEP. In the glossary, the FATF defined international organizations as an entity that exists by virtue of an intergovernmental agreement. Their leading functions, such as persons with the rank of director, deputy director or member of the supervisory board or similar management functions, meet the criteria for this new category. The list of functions shows that, as with foreign PEPs, only functions at the top hierarchical level of the organization qualify as PEPs. The FATF justified the broadening of the term by referring to Article 52 of the United Nations Convention against Corruption (UNCAC) of 2003. The convention is generally aimed at corruption of persons who hold public office. In the PEP guidelines issued in 2013, the FATF made it clear that the definition of PEP should be the same as that in Art. 52 UNCAC.

The guidelines included definitions of foreign PEPs, domestic PEPs, natural persons holding certain leading positions in international organizations, as well as a list of characteristics of persons who are recognizably close to a PEP for family or other reasons. Depending on the cultural background, the group of persons who fulfill this criterion may extend beyond persons who are directly related to a PEP (e.g. parents, siblings, partners and children) and may also include, for example, distant relatives (e.g. cousins). However, a person may also be close to a PEP for other reasons. For example, on the basis of a partnership (e.g. romantic relationship) or business relationship (e.g. joint ownership of an operating company). The decisive factor for the assessment is the risk that the close **person of a PEP can abuse their relationship with the PEP to** help the PEP hide illicitly acquired funds from corruption or to profit from them themselves. 12

I. The term PEP in the European Union

The Third EU Money Laundering Directive from 2005 included a definition of PEP and specified measures for dealing with business relationships with PEP. PEPs are persons who "are or have been entrusted with prominent public functions, and immediate family members, or persons known to be close 13

associates". The terms were defined more precisely in the European Commission's Directive 2006/70/EC of August 1, 2006. This made it clear that, as a rule, only public offices at the national level are considered "important", although public offices whose "political exposure" is identical to a similar function at the national level may also be "important". Article 2 of the directive contained a list of functions whose holders are to be qualified as PEPs. These included, for example, heads of state, heads of government, ministers, deputy ministers and state secretaries, but also "members of supreme courts whose decisions are not subject to further appeal in exceptional circumstances". The provisions explicitly excluded middle or lower-level functions from the PEP definition. The policy also defined who was included under the term "immediate family members". Parents, spouses or partners were mentioned. A "known associate" was a person who, for example, shared beneficial ownership of a legal entity with a PEP. The addition of the word 'known' indicates that the person's relationship to a PEP must be publicly known. The directive explicitly states that 'active inquiry' is not required. Finally, an end to the PEP status was determined by the requirement that a PEP must be considered politically exposed for at least one year after giving up the relevant function. The Fourth Anti-Money Laundering Directive, adopted in 2015, aligned European anti-money laundering and anti-terrorist financing rules with the 2012 FATF recommendations. The requirements of the European Commission's PEP Directive 2006/70/EC of August 1, 2006, were adopted, but were supplemented by "directors, deputy directors and members of the management body or equivalent function in an international organization". The EU's fifth anti-money laundering directive was adopted on May 30, 2018. Article 20a of the directive requires the member states and the Commission itself to publish lists specifying the individual functions that are considered **"important public functions"** according to the respective national requirements and those of the Commission, and whose holders qualify as a PEP. The member states should also require national organizations that have their registered office in the territory of the respective member state to maintain lists of equivalent functions. The Commission, member states and international organizations in the territory of a member state are obliged to keep the lists up to date and to make them public. The Commission complied with the regulation by publishing the list at the EU level in May 2022. In November 2023, the EU member states published the lists of the most important public offices in the respective country.

J. The PEP term in Switzerland

In Switzerland, the Swiss Federal Banking Commission (SFBC) already expressed its expectation in 1986, in the aftermath of the Marcos case, that business relationships with politically exposed persons could only be opened with the approval of the most senior management. The SFBC set out its expectations in greater detail in Circular SFBC-RS 98/1, which came into force on July 1, 1998. In it, the SFBC granted the executive board "sole authority" to approve business relationships with politically exposed persons and the duty to "regularly review" such business relationships. The definition of PEP in the circular was extended to persons "who have significant public functions for a foreign state or persons who are recognizably close to such officials". When the Anti-Money Laundering Act (AMLA) came into force on April 1, 1998, the supervisory authorities were able to define the due diligence requirements for the financial intermediaries under their supervision by means of Art. 16 AMLA. The resulting AMLO-SFBC, which entered into force on July 1, 2003, contained a definition of PEP that was limited to persons in **prominent public positions abroad and persons close to them**. This regulation remained in force until AMLA Art. 2a entered into force on January 1, 2016. 14

II. ELEMENTS OF THE PEP CONCEPT

Before the introduction of Art. 2a AMLA, the term PEP was defined in Art. 2 para. 1 let. a no. 1 and 2 of the old AMLO-FINMA and Art. 10 para. 4 let. a and b of the old AMLO-SFBC. The definition included foreign PEPs, i.e. persons who, due to their function abroad, are to be qualified as PEPs. The new provision also covered **domestic PEPs** and natural persons in leading positions in **intergovernmental organizations** and **international sports federations**. 15

A PEP is exclusively a natural person. The definitions of PEP in the aGwV-FINMA and aGwV-ESBK also included legal entities. In practice, however, this change has no significant consequences because the financial intermediary is obliged under Art. 4 AMLA to identify and verify the beneficial owner of a contracting party, who may also be a legal entity. If the verification of the beneficial owner of a contracting party shows that it is a PEP, enhanced due diligence must be applied to the business relationships. 16

The amendment has the consequence that state-owned enterprises are not PEPs. However, by applying a risk-based approach, a financial intermediary 17

may still come to the conclusion that there are increased risks in the case of such an enterprise. The deciding factor here may be that a natural person plays a role in the company's controlling bodies that is not explained by the company's function or mandate. This may be the case, for example, if the person is also a member of the ruling family of the country in question in addition to his or her role in the state-owned enterprise. Under these circumstances, there may be an increased risk of corruption because **independent higher control mechanisms are lacking**. Furthermore, information on a country's corruption risk, any substantial risk indications found in public sources with regard to the state-owned enterprise (e.g. business activities in a high-risk sector such as armaments) may also be relevant for the assessment.

18 Art. 2a AMLA contains vague legal terms such as “leading public function”, “national level”, “supreme bodies of state-owned companies of national importance” or “recognizably close”. This makes it impossible to derive a list of functions that correspond to PEPs within the meaning of Art. 2a AMLA. In most cases, therefore, a comprehensive assessment based on the available information is required. This is even the case when lists or databases from private providers are used. Such lists should be understood as merely a relevant piece of information to be checked. The information they contain may be out of date or the sources cited may no longer be available on the internet at the time of the assessment. It may also be that the provider applies its own criteria for PEPs that are not identical to those in Art. 2a AMLA. Finally, lists from private providers or databases cannot show all possible indications of a PEP connection. For example, information on known close associates is not always publicly available. For this reason, it is essential that the financial intermediary contacts the contracting partner directly in order to obtain relevant information for assessing whether there is a connection to a PEP. When applying the assessment, it is advisable to adopt a conservative approach, i.e. the financial intermediary is advised to classify as a PEP anyone who **could fulfill the attributes**.

19 The PEP concept is a formalistic approach. If the contracting party, the controlling person, the beneficial owner of the assets or the authorized person is a PEP according to Art. 2a AMLA, the business relationship according to Art. 13 para. 5 AMLO-FINMA entails **increased risks** and must be treated as risky. The legal requirements must be adhered to. However, to reduce the workload, the specific implementation of the audit measures can be risk-

based, for example, taking into account the country risk, the risk of the function and the services offered.

III. PEP ABROAD

A foreign PEP is a natural person who is or was active in a leading public function abroad. This is in contrast to a domestic PEP, who has or has had a corresponding function in the home country. The domicile of the natural person is not decisive for this, but rather **the country that has assigned the relevant function**. The relevant factor for the distinction is whether the financial intermediary maintaining the account that has to carry out the assessment is domiciled in the country that has assigned the relevant function to the PEP. For example, a person domiciled in Switzerland may qualify as a foreign PEP because they have accepted or held a mandate abroad. By contrast, a financial intermediary in Switzerland will classify a natural person who is a PEP because of a mandate in Switzerland, for example, as a domestic PEP. A financial intermediary abroad, on the other hand, will treat the same person as a foreign PEP regardless of their domicile. 20

A. A leading public function at the national level

A "public" function is one that, by virtue of the mandate, gives the holder access to state resources or a say in the allocation of such resources. The function may or may not be exercised by virtue of an election, and it need not be a political function. Accordingly, the article refers not only to politicians but also to officials in the administration, judiciary and military, or the governing bodies of state-owned enterprises of national importance. What is **decisive for the risk assessment is the potential access to state resources**. High-ranking officials of political parties at the national level are exceptions under certain circumstances, but they are also mentioned. For example, secretaries general may also be employed by an organization under private law and therefore have no access to state resources. 21

The attribute "leading" refers to a function at the top and not at the middle or bottom of an organization's hierarchy, in line with the FATF recommendation. This interpretation is underscored by the listed functions in Art. 2a para. 1 AMLA, which emphasize a higher hierarchical level. The latter is particularly evident in the list of functions of heads of state and government. Persons in these functions are at high risk of corruption because **they often have ex-** 22

tensive access to state resources and/or influence due to their position and power. The assessment of whether a function meets the criteria of Art. 2a para. 1 let. a AMLA must therefore be made in this context. In doing so, other factors may also be taken into account, such as an assessment of the political structure and legal system of the country, the function itself, an assessment of the country's susceptibility to corruption, the remuneration of the function and its significance in the awarding of public contracts. The assessment must also be made in the knowledge that the holder of such functions is in the public spotlight and therefore also represents a reputational risk.

23 In line with the FATF recommendation, to qualify as a foreign PEP, the function in question must be at the highest hierarchical level at "national level". This requirement takes into account the fact that senior positions at national level generally have no supervisory organization above them, which is why these positions are exposed to a high risk of corruption. In its message concerning the implementation of the FATF recommendations, however, the Federal Council pointed out that the financial intermediary may also qualify a function at the sub-national level as a foreign or domestic PEP on **the basis of self-developed risk criteria.** In its guideline, the FATF also explains that, depending on the structure of the state, the significance of the function and taking into account the factors already mentioned, a function at the sub-national level can also be a PEP. In this sense, for example, a natural person who has or had the function of mayor of a larger metropolis abroad or who was or is the governor of a province of a country can also qualify as a PEP. An assessment of these functions as PEP can be justified by the number of inhabitants of a city, the associated responsibility and budget authority, as well as the political structure of the respective country, for example if the function of a governor of a province has extensive powers.

24 Because the FATF did not mention the **deputy of a leading public function** in its definition of foreign and domestic PEPs, this function is not listed in the article. However, in its message on the implementation of the FATF recommendations, the Federal Council pointed out that a deputy of a function can also qualify as a foreign PEP on the basis of one or more risk criteria. In practice, however, the financial intermediary is free to qualify a deputy of a PEP-relevant function as a foreign PEP even without risk criteria, especially since it is obvious that this function, whose authorizations must be designed in such a way that it can act as a deputy, represents the same risk as the PEP itself.

B. Governing bodies of state-owned enterprises of national importance

Natural persons who perform or have performed a function on the "governing body" of a "state-owned enterprise of national importance" abroad qualify as foreign PEPs. "State-owned enterprises" are entities that are majority-owned or controlled by the state and often, but not necessarily, produce services or products and thus pursue commercial objectives. This may also include a nationally financed organization that fulfills a public function. Based on this understanding, it may include, for example, a state-owned university at the national level, a national regulatory authority for a specific industry, a state-owned pension and survivors' insurance for a country, or independent state-owned organizations with a specific purpose (e.g. economic development of a country). In practice, the addition of "of national importance" is often understood to mean that the state-owned enterprise or organization provides a service in a sector that is strategically important for the country (e.g. infrastructure). However, this addition can also be understood as follows: because a leading public function at the national level qualifies as a foreign PEP, the addition attempts to reflect this attribute at the level of "state-owned enterprises" as well. The attribute "of national importance" already existed in Art. 2 para. 1 let. a aGwV-FINMA and is probably a national peculiarity. The "Supervisors' PEP Working Paper 2001" of November 2001, which was prepared by representatives of banking supervisory authorities from major financial centers, including Switzerland, and which, as is well known, laid the foundation for the PEP principles, did not include the addition of "nationally significant" to "state-owned enterprises". The FATF recommendation designates persons in the supreme bodies of state-owned corporations as PEPs and does not contain any similar addition. It cannot therefore be proven beyond doubt from the preparatory work mentioned that "state-owned companies of national importance" within the meaning of Art. 2a para. 1 let. a AMLA refers only to companies or organizations that produce goods or services that are strategically important to a country. In practice, however, it often turns out that organizations and companies maintained at the national level actually offer such goods or services. These do not necessarily have to be active in a sector that is strategically relevant for a country in the conventional sense, but may also be state organizations or companies that, for example, manage a country's cultural heritage (e.g. archaeological finds). The latter can also be

25

justified by the fact that such functions in countries with a high risk of corruption can also entail the corresponding risks. **The application of a risk-based approach when assessing the term "of national importance" is therefore not excluded**. It is also recommended for a subsidiary of a state-owned company that has its own governing body. Decisive criteria may include, among other things, the legal basis, the size of the company and the significance of the function for the economic development of a country or, equally, the strategic importance for a country of the products or services provided by the company. "Top management" refers to functions at the highest level of an organization's hierarchy, the structure and designation of which may vary from country to country and industry to industry. This is probably why the FATF only refers to 'senior executives' without defining the term. In practice, this refers to those functions that are responsible for the supervision and management of the respective organization.

26 A country's rule of law situation may also be a deciding factor in the assessment. If a country's democratic institutions are weak, individuals who control a country's significant economic resources can have a great deal of influence on the country's politics and economy. Such individuals do not have to have a leading public function within the meaning of Art. 2a AMLA. However, they may enjoy a special status due to their position that gives them **easier access to government contracts**. These individuals may also have a large network within the political and economic elite of a country. There is therefore a risk of corruption. In line with a risk-based approach, such individuals may also be designated as PEPs for the reasons mentioned.

IV. DOMESTIC PEP

27 The FATF uses the same terms for the definition of foreign and domestic PEPs, which ensures that a function that qualifies as a domestic PEP domestically also fulfills the criterion for a foreign PEP abroad. Article 2a para. 1 let. b AMLA is therefore similarly formulated, **but adapted to the Swiss situation**. For example, the functions such as "heads of state and government and high-ranking politicians" mentioned in Art. 2a para. 1 let. a AMLA are missing from the article when listing the functions of domestic PEPs. Domestic PEPs are natural persons who are or have been active in leading public functions at the national level in politics, administration, the military and the judiciary. As with foreign PEPs, the specific functions cannot be clearly assigned on the basis of

this information. It is probably for this reason that the functions that are meant are listed in the message on the implementation of the FATF recommendations. These include federal councillors, the federal chancellor, national and state councillors, directors of offices and secretaries general of the federal administration, the Federal Attorney, federal prosecutors, federal judges, senior staff officers in the army, presidents of national parties and the secretaries general of national parties.

28 Domestic PEPs are also members of the board of directors or the management of state-owned companies of national importance. In this context, the message "specifically" refers designated the Post Office, Swisscom, Swiss Federal Railways (SBB), Swiss National Accident Insurance Fund (SUVA), Federal Office for Defence Procurement (ArmaSuisse), the arms manufacturer Aktiengesellschaft (RUAG), the Swiss Federal Laboratories for Materials Testing and Research (EMPA) and the Swiss Federal Nuclear Safety Inspectorate (ENSI) as state-owned companies of national importance. Due to the use of the term "in particular", the list is not exhaustive. However, based on the selected organizations, it allows the conclusion that the **term "company" must be interpreted broadly, in line with the analogous application to foreign PEPs under Art. 2a para. 1 let. a AMLA.** In this context, Greter points out that the list includes not only Swisscom, a state-owned company with commercial objectives, but also the ENSI, the Swiss Federal Nuclear Safety Inspectorate. The ENSI emerged from the Federal Office of Energy and has existed as an independent public-law institution since January 1, 2009. It can therefore be assumed that the term "enterprise" also refers to organizations that carry out activities that were originally performed by the federal administration but were later transferred by law to an independent public-law institution. Based on the explanations regarding the term "national significance" in the case of foreign PEPs, this primarily refers to state-owned enterprises that are held by the Swiss Confederation and not by the canton. On this basis, the following organizations, for example, may be state-owned enterprises of national importance: the Swiss Federal Institute of Technology (ETH), the École Polytechnique Fédérale de Lausanne (EPFL), the Swiss Financial Market Supervisory Authority FINMA, the Swiss National Bank (SNB), the Swiss Export Insurance (SERV), the Swiss National Museum, Pro Helvetia, the Federal Audit Oversight Authority (FAOA), the Federal Institute of Metrology (METAS) or even identidad AG, an organization for setting up and operating the Swiss animal database. Based on the same term for foreign PEPs, the financial inter-

mediary is also free to classify a state-owned company at the subnational level as a state-owned company of national importance based on the aforementioned analogous criteria. Applying the criteria, for example, companies designated by the Swiss government as systemically important electricity suppliers that are owned by cantons may be classified as state-owned companies of national importance. On this basis, their members of the board of directors or the executive board would be domestic PEPs.

29 The FATF recommendation was implemented by focusing on functions at the national level. Functions at the subnational level, such as members of the cantonal government, cantonal attorneys general, presidents of cantonal political parties or public functions at the municipal level, are not covered by the article. In the dispatch, however, the Federal Council encouraged financial intermediaries to develop their own criteria for also listing functions at the cantonal or municipal level as a domestic PEP in line with a risk-based approach. This request also includes the board of directors and senior management of companies that are managed at the cantonal level.

V. INTERGOVERNMENTAL ORGANIZATIONS

30 Art. 2a para. 1 let. c AMLA covers persons who are or have been entrusted with a "leading function" in an "intergovernmental organization" or in "international sports federations". **Intergovernmental organizations are based on an agreement between states, in which their rights and duties are regulated.** They are considered to be separate subjects of international law and are not necessarily treated the same as other organizations in their countries of domicile. The agreement may, for example, contain a special status with immunities and privileges. Examples of intergovernmental organizations are the United Nations (UN) and its sub-organizations, the International Monetary Fund (IMF), the European Union (EU) and its sub-organizations, the World Health Organization (WHO), the European Organization for Nuclear Research in Geneva (CERN), but also the International Committee of the Red Cross (ICRC). This does not include international private-law organizations that were not established by an agreement between states, such as non-governmental organizations like Greenpeace, Amnesty International, United Nations Children's Fund (UNICEF) Switzerland Liechtenstein. International sports organizations such as the International Olympic Committee (IOC) or the Fédération Internationale de Football Association (FIFA) are also not in-

cluded under this term. However, the latter are treated separately in Art. 2a para. 5 AMLA.

The definition of a "leading function" within an intergovernmental organization is determined by its organization. In principle, however, it can be assumed that this refers to the **representatives at the highest hierarchical level**, i.e. secretaries-general, directors, deputy directors, but also members of the highest governance bodies, such as the chief financial officer (CFO) of an intergovernmental organization. 31

VI. INTERNATIONAL SPORTS FEDERATIONS

Art. 2a para. 1 lit. c AMLA also covers persons who have or have had a "leading function" in "international sports federations". This addition is not based on a recommendation of the FATF. It is also not included in the message on the law. In March 2014, the Council of States decided to introduce this addition in view of the susceptibility to corruption of international sports organizations based in Switzerland. The National Council then added a definition of "international sports federations" under Art. 2a para. 5 AMLA. According **to this section, the IOC "as well as non-governmental organizations recognized by it that govern one or more official sports at the global level" fall under this definition.** According to this understanding, the IOC's organizations such as the Association of Summer Olympic Federations (ASOIF), the Winter Olympic Federations (WOF) or the International World Games Association (IWGA) fall under this definition. Examples of international sports federations recognized by the IOC are FIFA, the International Ice Hockey Federation (IIHF), the World Bridge Federation (WBF) and the World Dance Sport Federation (WDSF). This information is available on the IOC website. Accordingly, regional organizations such as the Union of European Football Associations (UEFA), the Swiss Football Association or organizations that are not currently recognized by the IOC, such as the International Boxing Association (IBA), are not "international sports federations" within the meaning of Art. 2a para. 5 AMLA. 32

The PEP concept is based on a **risk-based approach**. It is therefore up to the financial intermediary to decide whether to register natural persons who have or have had a leading function in a regional sports organization or who work or have worked in a sports organization not recognized by the IOC as PEPs within the meaning of Art. 2a para. 1 let. c AMLA. Possible criteria may in- 33

clude, for example, the size of the organization, references in the media to possible reputational risks in connection with the organization itself or with exponents in a leading function.

VII. CLOSE ASSOCIATES

34 The conviction that the same risks may emanate from family members of PEPs or persons close to PEPs as from the PEPs themselves was a decisive factor for the initiators of the PEP concept. The "Supervisors' PEP Working Paper 2001" of November 2001 still used the subjunctive when assessing the risks of a person close to a PEP. However, this assessment did not prevail. In the 40 Recommendations published in 2003, the FATF made it clear that the reputational risks of PEPs and persons close to PEPs are the same. Art. 2 para. 1 let. aa of the FINMA Anti-Money Laundering Ordinance therefore also designated persons who were clearly close to the PEP for family, personal or business reasons as PEPs. This paragraph was adopted in Art. 2a para. 2 AMLA, but, as already mentioned, limited to natural persons. For the reasons already mentioned, persons close to PEPs do not **present a different risk** compared to the PEPs themselves. Accordingly, business relationships with persons close to PEPs are treated the same as a business relationship with the PEP themselves in accordance with Art. 6 para. 3 and 4 AMLA.

35 The term 'close associate' is not defined in Art. 2a para. 2 AMLA. However, it is clear from the context that 'close associate' describes a relationship between a natural person and a PEP that suggests a **mutual familiarity**. The FATF had described the closeness referred to as 'family members' and 'close associates'. Art. 2 para. 1 lit. a aGwV-FINMA specified the reasons for "close" to the three characteristics "family", "personal" or "business". However, it is a challenge for a financial intermediary to recognize the closeness of a natural person within the meaning of Art. 2a AMLA. For this reason, the attribute "identifiable", which was already included in Art. 2 para. 1 let. a aGwV-FINMA, was deliberately retained. This is to protect the financial intermediary from the accusation of incomplete fulfilment of the due diligence obligations if, after an ordinary clarification has been carried out when a business relationship is established, relevant indications should arise at a later point in time. This also makes it clear that the term "discernible" refers to indications that may arise during standard checks when opening a business relationship and during the ongoing proper monitoring of business relationships and the transactions

carried out within those relationships. In practice, this includes questioning the contracting partner when the account is opened, using lists of names of PEPs and persons close to PEPs when comparing customer data, taking into account the restrictions mentioned, and, last but not least, the attention of the staff responsible for these process steps through appropriate training on this topic, which is provided as part of the regular training process on regulatory topics. The financial intermediary is not required to take any measures beyond those mentioned in order to identify a natural person as a PEP.

Close family members of the PEP, such as partners, siblings, children, parents or grandparents, are considered to be related to the PEP for "family" reasons. The group of persons concerned depends on the **social, cultural or religious environment.** For example, there are large ruling families on the Arabian peninsula whose members enjoy privileges due to their origin, without them performing a public function in the government and without any direct connection to the PEP other than the same family name, but who may still be deemed to be close associates of a PEP. Taking the above criteria into account when selecting the persons concerned also means, however, that evidence of a verifiable estrangement between the natural person and the PEP, in the form of a divorce, for example, can be taken into account in the assessment. Possible criteria include the duration of the separation, a clear separation of assets and the origin of assets between the PEP and the natural person. 36

Based on the understanding of "familial" reasons, "personally" close can **only mean a close relationship with the PEP without a familial relationship.** This category includes natural persons who are close to a PEP due to an affair or friendship. The risk-based approach means that the selection of this group of persons always requires an assessment of the quality of the relationship. The assessment takes into account the cultural, social and religious environment, but also personal aspects of the relationship, such as its long-standing and uninterrupted duration. As a result of such an assessment, a relationship with a godchild may fall into this category, as may long-standing relationships between natural persons within organizations (e.g. clubs, associations, religious sects). Such relationships can also change, so that after a time there is no longer any recognizable closeness. Criteria for this assessment may include, for example, the dissolution of the partnership, which also includes a comprehensible separation of joint assets. The category of "personally" close does not include demonstrably fleeting encounters with a PEP, such as an appear- 37

ance by a person at a public event with a PEP that can be explained by their respective functions in relation to the event.

38 Accordingly, "business" close describes the relationship of trust between a PEP and a natural person that exists or has arisen on the basis of jointly conducted business. This category therefore includes long-standing business partners who jointly bear the entrepreneurial risks of their projects, which is why mutual financial dependencies also exist. In its FAQ on PEPs from 2017, the Wolfsberg Group also referred to personal advisors of PEPs, in particular those who manage PEP funds in a fiduciary capacity, as business-related. The nature of the relationship in this sense is therefore based on **common business and financial interests**, whereby the relationship between the natural person and the PEP must also include elements of mutual familiarity. Thus, an employment relationship with a PEP, which may also include the activity described in the FAQ mentioned above, or the fact that a natural person is on the board of directors of a company together with a PEP and other members, is not in itself an indication of a person closely associated with a PEP for business reasons. Even long-standing employees of a company that is majority-owned or controlled by a PEP are not necessarily business associates, especially if the natural person has demonstrably pursued a professional career outside the company concerned, in which case it can be assumed that the person is not fully financially dependent on the PEP.

VIII. END OF PEP STATUS

39 Experience has shown that the risks for the financial intermediary of business relationships with a PEP connection do not end with the termination of the mandate qualifying as a PEP. Investigations in cases of corruption, **indications of misappropriated funds or risks to reputation that could impact the reputation of the financial intermediary usually only become known after the termination of the function or even after the PEP has passed away.** The risk depends on the political situation and corruption risk of the country in question that has awarded the PEP-relevant mandate, but also on the PEP's mandate and the influence associated with it. Because these are individual factors, there is no generally valid statement as to how long the PEP status should exist. Two concepts attempt to limit the associated risks: either never to limit the PEP status ("once a PEP always a PEP") or to choose a risk-based approach ("once a PEP could always be a PEP"). In line with the

FATF and the Wolfsberg Group, the Federal Council preferred a risk-based approach. Parliament, on the other hand, decided to introduce a time limit for domestic PEPs: According to Art. 2a para. 4 AMLA, the status for domestic PEPs lapses 18 months after they have ceased to hold office. However, for the reasons mentioned, the end of the qualification for domestic PEPs does not mean that there are no longer any risks associated with the business relationship. Under certain circumstances, the financial intermediary can continue to classify the business relationship as a higher-risk relationship.

40 The risk-based approach to assessing PEP status after the function has been abandoned is therefore applied to foreign PEPs or to PEPs based on a function in an intergovernmental organization or in international sports federations. Several factors should be considered in these deliberations. These include the corruption risk of the country or organization that has awarded the function. The political structure of the country in question should also be taken into account, such as whether it has a functioning separation of powers. The Wolfsberg Group provided a comprehensive list of criteria in its FAQ on PEPs published in 2017. This also includes any negative reporting about the PEP in public sources. The FAQ recommends applying the risk-based approach even to deceased PEPs, because in this case the risks remain unchanged. For living persons, the FATF considers whether the PEP will continue to have influence after leaving office or whether any new function assumed is in any way connected to the past one. Consequently, the termination of the PEP qualification must also have an impact on the same qualification of PEP-related persons, i.e. PEP-related persons also lose their qualification in this case. When assessing the end of the PEP status, it is not decisive whether the financial intermediary has a business relationship with the PEP himself or with the PEP-related person. The risks associated with a PEP exist regardless of how distantly connected the PEP is to the close associate. The end of the PEP qualification 18 months after giving up the function at domestic PEP can also be read as an indication that the legislator considers the domestic PEP to be a lower risk compared to foreign PEP or in the case of a PEP based on a function in an intergovernmental organization or in an international sports federation according to Art. 2a para. 1 lit. a or Art. 2a para. 1 lit. c AMLA as posing a lower risk. Consequently, the 18-month period can also be applied as a **minimum period** for the PEP qualification after giving up the function for foreign PEPs or for PEPs based on a function in an intergovernmental organization or in an international sports federation. In the case of existing PEP re-

lationships, the continuation of which must be approved annually in accordance with Art. 19 para. 1 lit. a GwV-FINMA, this practice may be applied if two previous authorizations have been granted without complaint. When the PEP designation is removed, it is advisable to carry out clarifications in accordance with Art. 15 GwV-FINMA and Art. 6 AMLA in order to fulfill any reporting requirements.

BIBLIOGRAPHY

Arbeitsgruppe KYC, Working Paper of Financial Institutions Supervisory Authorities on the Handling of Accoungs Linked to Politically Exposed Persons – PEPs ("Supervisors" PEP Working Paper 2001"), in: https://www.finma.ch/finmaarchiv/ebk/f/archiv/2002/pdf/neu090702-03f.pdf, besucht am 4.8.2024 (zit.: Arbeitsgruppe KYC, «Supervisors' PEP Working Paper 2001»).

Basler Ausschuss für Bankenaufsicht, Sorgfaltspflicht der Banken bei der Feststellung der Kundenidentität, Bank für Internationalen Zahlungsausgleich, Oktober 2001, in: https://www.bis.org/publ/bcbs85g.pdf, besucht am 4.8.2024 (zit.: Basler Ausschuss für Bankenaufsicht, Sorgfaltspflicht der Banken bei der Feststellung der Kundenidentität).

Bruppacher Balz, Die Schatzkammer der Diktatoren, Der Umgang der Schweiz mit Potentatengeldern, Zürich 2020.

Bundesrat. Geldwäschereibekämpfung in der Schweiz. Broschüre vom 25.10.2002, in: https://www.finma.ch/FinmaArchiv/ebk/d/archiv/2002/pdf/gw_broschuere_dt.pdf, besucht am: 5.1.2025 (zit. Broschüre Geldwäschereibekämpfung).

Financial Action Task Force (FATF), FATF Guidance Politically Exposed Persons (Recommendation 12 and 22), Juni 2013, in: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-PEP-Rec12-22.pdf.coredownload.pdf, besucht am: 22.10.2024 (zit.: FATF, Guidance Politically Exposed Persons).

Financial Action Task Force (FATF), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, November 2023, in: FATF Recommendations 2012.pdf.coredownload.inline.pdf (fatf-gafi.org), besucht am: 25.8.2024 (zit.: FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation).

Financial Action Task Force (FATF), The forty recommendations, June 20, in: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202003.pdf, besucht am 4.8.2024. (zit.: FATF, The Forty Recommendations).

Greter Alexander, Kommentierung zu Art 2a, in: Peter Ch. Hsu/Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Hawkins Fiona, Kommentierung zu Art 2a, in: Kunz, Peter V./Jutzi, Thomas/Schären, Simon (Hrsg.). Geldwäschereigesetz, Bern 2017.

Eidgenössische Bankenkommission, Rundschreiben: Richtlinien zur Bekämpfung und Verhinderung der Geldwäscherei (Geldwäscherei) vom 26.3.1998, in: https://www.finma.ch/finmaarchiv/ebk/d/publik/mitteil/1998/m3-98-2.pdf, besucht am: 25.8.2024. (zit.: Eidgenössische Bankenkommission, Rundschreiben: Richtlinien zur Bekämpfung und Verhinderung der Geldwäscherei).

The Wolfsberg Group, Global Anti-Money-Laundering Guidelines for Private Banking, Oktober 2000, in: http://www.bahamasb2b.com/b2b/big_picture/download/Guidelines.pdf, besucht am: 4.8.2024 (zit.: Wolfsberg, AML Guidelines 2000).

The Wolfsberg Group, Wolfsberg Guidance on Politically Exposed Persons (PEP), 2017, in: https://db.wolfsberg-group.org/assets/3867d9cf-7c9b-41bc-9fad-6685bbabd52c/4.%20Wolfsberg-Guidance-on-PEPs-May-2017.pdf, besucht am: 22.10.2023 (zit.: Wolfsberg, PEP Guidelines 2017)

Wyss Ralph, Kommentierung zu Art. 2a, in: Thelesklaf, Daniel/Wyss, Ralph / van Thiel, Mark / Ordolli Stiliano, GwG Kommentar, 3. aktualisierte Aufl., Zürich 2019.

MATERIALS

Botschaft zur Umsetzung der 2012 revidierten Empfehlungen der Groupe d'action financière (GAFI) vom 13.12.2013, BBI 2014, abrufbar unter https://www.fedlex.admin.ch/eli/fga/2014/100/de, besucht am 22.10.2023. (zit. Botschaft GwG 2014).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in French. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 2 para. 2 AMLA

A commentary by Joane Etienne

SUGGESTED CITATION

Joane Etienne, Commentary of art. 2 para. 2 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Etienne, art. 2 para. 2 AMLA N. XXX

Art. 2 Scope of application

[2] Financial intermediaries are:

a. banks as defined in Article 1*a* of the Banking Act of 8 November 1934 (BankA) and the persons defined in Article 1*b* BankA;

a^{bis}. portfolio managers and trustees as defined in Article 2 paragraph 1 letters a and b of the Financial Institutions Act of 15 June 2018 (FinIA);

b. fund management companies as defined in Article 2 paragraph 1 letter d FinIA;

b^{bis}. licensees in accordance with Article 13 paragraph 2 letters b–d the Collective Investment Schemes Act of 23 June 2006, (CISA) and the managers of collective assets in accordance with Article 2 paragraph 1 letter c FinIA;

c. insurance institutions as defined in the Insurance Supervision Act of 17 December 2004 that deal in direct life insurance or offer or distribute shares in collective investment schemes;

d. securities firms in accordance with Article 2 paragraph 1 letter e FinIA;

d^{bis}. central counterparties and central securities depositories in accordance with the Financial Market Infrastructure Act of 19 June 2015 (FinMIA);

d^{ter}. payment systems that require authorisation from the Swiss Financial Market Supervisory Authority (FINMA) in accordance with Article 4 paragraph 2 FinMIA;

d^{quater}. trading facilities for DLT securities in accordance with Article 73*a* FinMIA (DLT trading facilities);

e. casinos as defined in the Gambling Act of 29 September 2017 (GamblA);

f. promoters of large-scale games under the GamblA;

g. trade assayers and group companies in accordance with Article 42bis of the Precious Metals Control Act of 20 June 1933 (PMCA).

CONTENT

I. Scope of application for financial intermediaries within the meaning of Art. 2 para. 2 54
A. General remarks 54
B. Scope of application based on the person 54
C. Scope of application in terms of subject matter 56
D. Territorial scope 56
II. Regulated financial intermediaries subject to 57
A. Banks and persons within the meaning of Art. 1b BA 57
B. Asset managers and trustees 58
C. Fund management companies 59
D. Collective investment schemes and collective asset managers 61
E. Insurance institutions 63
F. Securities dealers 65
G. Central counterparties and central securities depositories 65
H. Payment systems 66
I. Trading systems based on DLT 67
J. Casinos 67
K. Large-scale gaming operators 68
L. Commercial assayers 69
Bibliography 70
Materials 71

I. SCOPE OF APPLICATION FOR FINANCIAL INTERMEDIARIES WITHIN THE MEANING OF ART. 2 PARA. 2

A. General remarks

1 In accordance with Art. 2 para. 1 AMLA, the AMLA applies to financial intermediaries and natural or legal persons who, on a professional basis, trade in goods and receive cash in payment (traders). There are two categories of financial intermediaries, each subject to a different supervisory regime: **regulated financial intermediaries**, which are defined in Art. 2 para. 2 AMLA and are subject to prudential supervision, which also covers AMLA aspects, and **unregulated financial intermediaries**, which are defined in Art. 2 para. 3 AMLA and are subject to supervision covering only AMLA aspects. The supervision of regulated financial intermediaries falls within the remit of their respective supervisory authorities (see Art. 12 AMLA).

2 The **OBA** applies, among others, to all regulated financial intermediaries (Art. 2 para. 1 let. a OBA). In this regard, it should be noted that until the end of 2022, the OBA only applied to unregulated financial intermediaries. Since January 1, 2023, Art. 2 para. 1 let. a AMLO has been amended to also include regulated financial intermediaries, insofar as the new Section 3 of Chapter 2 of the Ordinance on Obligations in Cases of Suspicion of Money Laundering also applies to them. The AMLO -FINMA applies only to regulated financial intermediaries pursuant to Art. 2 para. 2 let. a to d and d^{quater} AMLA (see Art. 3 para. 1 OBA-FINMA).

B. Scope of application based on the person

3 Art. 2 para. 2 AMLA contains a list of **financial intermediaries subject to supervision** who are subject to the AMLA by law, due to their respective qualifications and their subjection to the relevant special laws and, in principle, regardless of the activities actually carried out (subject to let. c, cf. N. 38, and subject to Art. 2 para. 4 lit. c, cf. Art. 2 para. 4 N. 7 ff.). This list must be considered exhaustive, not only because of its wording, but also in view of the message of the law and the fact that the provision has been regularly adapted to cover new institutions.

Persons who do not fall under the list in Art. 2 para. 2 AMLA may, where applicable, fall within the scope of the AMLA pursuant to Art. 2 para. 3 AMLA, depending on the **activities** actually carried out. 4

It should be noted that the classification as a financial intermediary and thus the subjection to the AMLA for institutions under letters a to g is not linked to the obtaining of the respective **authorizations** or **licenses**. In other words, even in the absence of the authorizations or licenses required for the various institutions under the applicable special laws, e.g., in the case of fund management or the acceptance of deposits from the public without FINMA authorization, the institution concerned will nevertheless be classified as a financial intermediary within the meaning of Art. 2 para. 2 AMLA and will be subject to the AMLA. 5

In practice, regulated financial intermediaries will in principle be **legal entities**. In this case, the obligations of the AMLA apply directly to the legal entity, and not to its individual organs or employees. In accordance with Art. 8 AMLA, the necessary organizational measures must be taken to prevent money laundering and terrorist financing, particularly in terms of controls and personnel, who must receive adequate training. It is the responsibility of the bodies of the legal entity to implement these organizational measures, in particular those defined in Art. 23 ff. AMLA-FINMA, and to ensure that appropriate controls are carried out. 6

In certain cases, the financial intermediary may be a **natural person** or a **partnership**. With regard to natural persons, the provisions of the AMLA apply directly to them. In the case of partnerships, a case-by-case analysis must be carried out. According to doctrine, in a simple partnership, any person who carries out an activity as a financial intermediary must be classified as a financial intermediary and is thus directly subject to the AMLA in a personal capacity; in the case of general partnerships or limited partnerships, provided that the latter have a certain legal capacity, the companies must be considered as financial intermediaries, and not their individual partners. 7

When a natural or legal person acts as an **auxiliary agent** of a regulated financial intermediary, they will not be considered a financial intermediary if the conditions of Art. 2 para. 2 let. b ch. 1 to 6 AMLA are met; their actions will be covered by the authorization of the regulated financial intermediary for whom they are acting. 8

C. Scope of application in terms of subject matter

9 Since regulated financial intermediaries are subject to the AMLA due to their prudential status, it is necessary to determine the specific **activities** for which the obligations under the AMLA must be complied with, and the business relationships in which the due diligence obligations must be applied.

10 In practice, regulated financial intermediaries apply the provisions of the AMLA to the activities they carry out when these constitute **financial intermediation**. In the same vein, when conducting a prudential audit of a regulated institution, prudential audit firms verify compliance with the due diligence obligations under the AMLA in the context of business relationships that are subject to the AMLA, i.e., the business relationships of the institution's activities that constitute financial intermediation. Referring to Art. 1 of the Act, which defines the scope of the AMLA in relation to financial transactions, legal doctrine adheres to this practice and considers that the scope of application of the AMLA for regulated institutions is limited to financial transactions and related business relationships, which inherently involve a risk of money laundering. In order to determine which activities constitute financial intermediation and are therefore subject to the AMLA, Art. 2 para. 3 AMLA, the list of activities in letters a to g, and FINMA Circular 11/1 "Financial intermediary activities within the meaning of the AMLA" may be taken into account.

D. Territorial scope

11 While the AMLA does not contain any provisions defining its **territorial** scope, this is specified in the ordinance (Art. 2 para. 1 AMO) on the basis of Art. 41 para. 1 AMLA. Until the end of 2022, with regard to financial intermediaries, the AMLO applied only to unregulated financial intermediaries within the meaning of Art. 2 para. 3 AMLA, and the territorial scope was specified in the AMLO only for this category of financial intermediaries (see N. 2). Legal scholars were divided on the question of the territorial scope of the law for regulated financial intermediaries, with some authors considering that Art. 2 para. 1 OBA should also be applied analogously to regulated financial intermediaries, while others considered that such a broad interpretation was not necessary. The issue has now been resolved, as the new wording of Art. 2 para. 1 let. a OBA, in force since January 1, 2023, is clear and now also covers regulated financial intermediaries under Art. 2 para. 2 of the law.

In accordance with Art. 2 para. 1 let. a OBA, the OBA applies to financial intermediaries who carry out their activities **in Switzerland** or **from Switzerland**. This provision is similar to the territorial scope of application of the LEFin and the OEFin for financial institutions. Thus, by analogy with financial institutions under the FinIA, the decisive factors are not the location of the financial intermediaries' registered office or domicile, the place where the clients are domiciled, or the place where the assets involved in the business relationship are located. The decisive factor for the application of the AMLA and its implementing ordinances is the location of the financial intermediary's activity, which must be determined on the basis of all the circumstances. 12

FINMA Circular 11/1 "Financial intermediary activities within the meaning of the AMLA," which clarifies the application of Art. 2 para. 3 AMLA and thus applies to unregulated financial intermediaries, sets out **FINMA's practice** with regard to territorial scope and can be taken into account in a similar manner for regulated financial intermediaries, since the latter are now also expressly included in Art. 2 para. 2 let. a AMLO (see N. 11). According to FINMA, a financial intermediary conducts its business in Switzerland or from Switzerland if it has a domicile in Switzerland or is registered in the Swiss commercial register, or if it employs persons in Switzerland who perform or conclude financial intermediary business for it on a long-term basis in Switzerland or from Switzerland, or who can legally commit it to such business (de facto branch). 13

Regulated financial intermediaries who conduct their business abroad **without a physical presence** in Switzerland are therefore not, in principle, covered by Art. 2 para. 2 or 3 AMLA and are therefore not subject to the AMLA, even if they have some business activity in Switzerland, e.g. if they have clients in Switzerland, if they visit their clients in Switzerland or if they seek new clients, solely on a "fly-in-fly-out" basis, without a legal branch or de facto branch in Switzerland. 14

II. REGULATED FINANCIAL INTERMEDIARIES SUBJECT TO

A. Banks and persons within the meaning of Art. 1b BA

In accordance with Art. 2 para. 2 let. a AMLA, banks within the meaning of Art. 1a of the Banking Act and persons within the meaning of Art. 1b of the Banking Act are classified as financial intermediaries. They are subject to su- 15

pervision by **FINMA** and require authorization from FINMA in order to carry out their activities.

16 Persons who are primarily active in the financial sector and who i) professionally accept deposits from the public in excess of CHF 100 million or solicit the public to obtain them, ii) professionally accept deposits from the public up to CHF 100 million or cryptoassets designated by the Federal Council, or solicit the public to obtain them and invest or remunerate these deposits or assets, or (iii) obtain significant refinancing from several banks that do not have a significant stake in their capital for the purpose of financing, in any manner whatsoever, an indefinite number of persons or companies with which they do not form an economic entity (Art. 1a BA).

17 Persons within the meaning of Art. **1b BA** are persons primarily active in the financial sector who i) professionally accept deposits from the public up to a maximum of CHF 100 million or cryptoassets designated by the Federal Council, or solicit the public to obtain them, and ii) do not invest or remunerate these deposits or assets (Art. 1b para. 1 BA).

18 The **Swiss National Bank** and **mortgage bond issuing centers** are not subject to the BA (see Art. 1 para. 5 BA) and are therefore not financial intermediaries within the meaning of Art. 2 para. 2 let. a AMLA (with regard to the Swiss National Bank, see also Art. 2 para. 4 let. a AMLA).

19 In accordance with Art. 35 FINMA-BAO, **CDB 20** applies to banks for the verification of the identity of the contracting party and the identification of the controlling person and the beneficial owner of the assets. For persons under Art. 1b BA, **Title 5 of the AMLO-FINMA** (Art. 43a ff. AMLO-FINMA) applies.

B. Asset managers and trustees

20 In accordance with Art. 2 para. 2 let. a^{bis} AMLA, asset managers and trustees referred to in Art. 2 para. 1 let. a and b FINMASA must be classified as financial intermediaries. They are subject to supervision by a **supervisory body** authorized and supervised by FINMA and require authorization from **FINMA** in order to carry out their activities.

21 Persons who, on the basis of a mandate, may professionally dispose of their clients' assets within the meaning of Art. 3 let. c ch. 1 to 4 FSIA (Art. 17 para. 1

AMLA) on behalf of and for the account of clients are considered **asset managers**. . These are primarily "traditional" independent asset managers, who have power of attorney with discretionary management authority over their clients' assets deposited with a bank in Switzerland or abroad. It also covers persons engaged in any other form of "management" in connection with individual portfolios, e.g., advisory activities followed by the execution of transactions, or solely the receipt and transmission of client orders, as soon as there is a power of attorney or fiduciary holding of assets, even in the absence of any discretionary management.

Furthermore, in accordance with Art. 24 para. 2 LEFin, asset managers who operate below the "**de minimis**" threshold (see N. 34) are also considered asset managers within the meaning of Art. 17 para. 1 LEFin. 22

Persons who, on a professional basis, manage separate assets or dispose of them in favor of a beneficiary or for a specific purpose, on the basis of a trust deed, are considered **trustees** (Art. 17 para. 2 FISA). 23

Persons who are active in management or trustee activities but benefit from an **exception**, in particular on the basis of Art. 2 para. 2 LEFin, and are therefore not covered by the LEFin, e.g. single family offices or private trust companies (PTCs), are not to be classified as financial intermediaries within the meaning of Art. 2 para. 2 let. b AMLA. They may, where applicable, fall within the scope of the AMLA pursuant to Art. 2 para. 3 AMLA (see N. 4). 24

Title 5 of the FINMA-BAO (Art. 43a ff. FINMA-BAO) applies to managers and trustees and specifies, in particular, the requirements for verifying the identity of the contracting party and identifying the beneficial owner. 25

C. Fund management companies

In accordance with Art. 2 para. 2 let. b AMLA, fund management companies within the meaning of Art. 2 para. 1 let. d FINMASA qualify as financial intermediaries. They are subject to supervision by **FINMA** and require authorization from FINMA in order to carry out their activities. 26

Persons who, on behalf of investors, independently and in their own name, manage investment funds in accordance with Art. 15 para. 1 let. a CISA or assume the administration of SICAVs referred to in Art. 13 para. 2 let. b CISA (Art. 32 FINSA) are considered **fund managers**. . 27

28 In the area of fund management, the risk of money laundering is considered moderate. This is because there are no direct financial flows between investors and collective investments; instead, investments are made at the fund custodian bank by the bank of the final investors, which involves checks at various levels by institutions subject to prudential supervision. Certain relaxations have therefore been granted. With regard to investors, fund managers must verify the identity of the **subscriber** when subscribing to unlisted Swiss collective investment schemes and identify the controlling party or beneficial owner of the assets only if the subscription amount exceeds CHF 15,000 (Art. 40 para. 1 OBA-FINMA) . Initially set at CHF 25,000, the threshold was lowered in 2020 on the basis of FATF Recommendation 10, which provides for a threshold of USD 15,000, due to the change in the CHF/USD exchange rate. This provision establishes an obligation vis-à-vis the subscriber or beneficial owner at the time of subscription as a single obligation, rather than obligations vis-à-vis the investor based on a business relationship. The term "subscriber" refers to either subscription on one's own behalf or subscription in the name and on behalf of a client. Pursuant to Art. 40 para. 2 OBA-FINMA, fund management companies may not require explanations regarding the controlling owners or beneficial owners at the time of subscription if the subscriber is a financial intermediary pursuant to Art. 2 para. 2 lit. a to d AMLA or a foreign financial intermediary subject to anti-money laundering and counter-terrorist financing regulations and adequate prudential supervision. FINMA did not wish to define the term "adequate," considering that this term cannot be assessed in a schematic manner. It is therefore up to the financial intermediary to assess adequacy on a case-by-case basis, using the country assessment reports and high-risk country lists published by the FATF. It should be noted that in practice, fund units are most often subscribed to by such financial intermediaries (in particular banks and securities firms), so that Art. 40 para. 2 OBA-FINMA is frequently applied and there is no need to identify the controlling party or beneficial owner.

29 Furthermore, in practice, fund management companies entrust the performance of due diligence and documentation obligations in relation to managed collective investment schemes to the **custodian banks** of said collective investment schemes on the basis of Art. 40 para. 3 OBA-FINMA. This is because not only do fund management companies generally not have access to information about investors due to banking secrecy, but more importantly, the custodian bank is responsible for issuing and redeeming fund units (Art. 73

para. 1 LPCC) and thus maintains direct contact with the subscriber. In this context, the custodian bank already applies the due diligence obligations under the AMLA on its own behalf itself in relation to subscribers of fund units. When the fund management company entrusts the execution of due diligence obligations in accordance with this provision to the custodian bank, this does not, in our view, constitute outsourcing or a delegation of essential tasks within the meaning of Art. 14 FINMASA and FINMA Circular 18/3 "Outsourcing." This option is explicitly provided for in Art. 40 para. 3 FINMA-BAO, which constitutes a special law, and fund management companies do not have the option of appointing a third-party delegate of their choice. They must designate fund custodian banks, which are also supervised by FINMA.

In accordance with Art. 40 para. 4 OBA-FINMA, CDB 20 applies to the methods used to identify the counterparty, the controlling party and the beneficial owner of the assets, as well as to any other activities of the fund management company that are relevant to the AMLA. 30

D. Collective investment schemes and collective asset managers

In accordance with Art. 2 para. 2 let. b^{bis} AMLA, holders of a license under Art. 13 para. 2 let. b to d CISA, i.e., SICAVs, SCmPCs and SICAFs, as well as collective asset managers pursuant to Art. 2 para. 1 let. c FINIA, must be classified as financial intermediaries. They are subject to supervision by **FINMA** and require authorization from FINMA in order to carry out their activities. This does not include L-QIFs in the form of SICAVs and SCmPCs, as they do not have FINMA authorization and are not subject to FINMA supervision (Art. 118a para. 1 let. d LPCC). This provision was clarified in this sense when the amendments relating to L-QIFs in the LPCC came into force on March 1, 2024. In principle, L-QIFs are not subject to the LBA (see Art. 2 para. 4 let. e LBA) . 31

This provision does not cover all institutions that require authorization under Art. 13 LPCC. **Representatives** of collective investment schemes are not included and therefore do not qualify as financial intermediaries within the meaning of Art. 2 para. 2 AMLA. Furthermore, **custodian banks** are also not affected; however, since they must be a bank within the meaning of the Banking Act (Art. 72 CISA), they are financial intermediaries under Art. 2 para. 2 let. a AMLA. 32

33 SICAVs, SCmPCs, and SICAFs are collective investment schemes in **corporate** form. SICAVs are open-ended funds, while SCmPCs and SICAFs are closed-ended funds (see Art. 8 and 9 LPCC). While SICAVs and SCmPCs are frequently used in practice, there are currently no SICAFs due to regulatory constraints and tax implications, which make the product unattractive.

34 In accordance with Art. 40 para. 1 and 2 OBA-FINMA, SICAVs, SCmPCs, and SICAFs must verify the identity of the **subscriber** when subscribing to unlisted Swiss collective investment schemes and identify the controlling person or beneficial owner in the same cases as fund management companies (see N. 27). They also entrust the custodian bank with the performance of due diligence and documentation obligations, based on Art. 40 para. 3 OBA-FINMA, in a similar manner to fund management companies (see N. 28).

35 Persons who professionally manage assets in the name and on behalf of collective investment schemes or pension funds are considered to be **collective asset managers** (Art. 24 para. 1 FINMASA). As with asset managers (N. 21), this includes not only "traditional" discretionary management activities, but also advisory activities involving the transmission of orders or "execution only" activities, provided that there is a power of attorney or fiduciary holding of assets, even in the absence of any discretionary management.

36 Collective asset managers who operate below the "**de minimis**" threshold are considered asset managers within the meaning of Art. 17 para. 1 FIDL and are therefore classified as financial intermediaries within the meaning of Art. 2 para. 2 let. a^{bis} AMLA. This primarily concerns collective asset managers managing collective investment schemes whose investors are qualified within the meaning of Art. 10 para. 3 or 3*ter* CISA, if the value of the funds they manage does not exceed CHF 100 million in total, including values acquired by means of leveraged financial instruments, or CHF 500 million in total if the funds do not contain any leveraged financial instruments and do not grant any rights to redemption for a period of five years from the date of the initial investment (closed-end funds) (Art. 24 para. 2 let. a FinIA). This also applies to collective asset managers managing the assets of pension funds where the assets of the latter do not exceed CHF 100 million in total or, in the mandatory area, 20% of the assets of a single pension fund (Art. 24 para. 2 let. b LEFin).

37 The FINMA AIFM Regulations contain specific provisions for **managers of collective assets of foreign collective investment schemes**. These provi-

sions do not apply to managers of Swiss collective investment schemes, as in this case the identification obligations are incumbent on the fund management company (see N. 27 f.). In accordance with Art. 41 para. 1 FINMA AEO, managers of collective assets of foreign collective investment schemes must identify the subscriber and identify the controlling person or beneficial owner of the assets of the foreign collective investment scheme i) if neither the foreign collective investment scheme nor its asset management company is subject to anti-money laundering and counter-terrorist financing regulations and adequate prudential supervision, (ii) if they do not provide evidence of the application of adequate anti-money laundering and counter-terrorist financing regulations by another financial intermediary subject to adequate prudential supervision, and (iii) if the amount invested exceeds CHF 15,000. With regard to the concept of subscriber and adequate regulation and supervision, see N. 27. Thus, the application of due diligence obligations in relation to subscribers will depend, in addition to the amount subscribed, mainly on the country of domicile of the managed foreign fund or its management company. Pursuant to Art. 41 para. 2 OBA-FINMA, it is not necessary to obtain a declaration concerning the controlling owner or beneficial owner of the assets if the subscriber is a financial intermediary pursuant to Art. 2 para. 2 lit. a to d AMLA or a foreign financial intermediary subject to adequate anti-money laundering and counter-terrorist financing regulations and prudential supervision. This provision is similar to that for fund management companies, see N. 27.

In accordance with Art. 41 para. 3 AMLO-FINMA, **CDB 20** applies to the methods used to identify the counterparty, the controlling party and the beneficial owner of the assets, as well as to any other activities of the asset manager that are relevant to the AMLA. 38

E. Insurance institutions

In accordance with Art. 2 para. 2 let. c AMLA, insurance institutions within the meaning of the ISA, i.e. "insurance companies" according to the terminology used by the ISA, are to be classified as financial intermediaries if they carry out direct life insurance business or if they offer or distribute units in collective investment schemes. Insurance companies under the ISA are subject to supervision by **FINMA** and require authorization from FINMA in order to carry out their activities. 39

40 Unlike the other types of regulated institutions listed in Art. 2 para. 2 AMLA, which must always be classified as financial intermediaries due to their prudential status, regardless of the activities they actually carry out, the scope of application is limited for insurance companies, which are to be classified as financial intermediaries and are therefore subject to the AMLA pursuant to Art. 2 para. 2 AMLA only if they carry out **direct life insurance activities** or **distribute collective investments**. For these activities, the due diligence obligations under the AMLA must be complied with. In addition, the due diligence obligations under the AMLA must also be complied with for any other activity that qualifies as financial intermediation, as is the case for any regulated financial intermediary (see N. 10).

41 Insurance companies subject to the ISA are those that engage in **private insurance** in the form of direct insurance or reinsurance. Insurance companies that are not subject to the ISA, e.g. social insurance companies or public insurance companies (in particular cantonal building insurance companies) are not covered by Art. 2 para. 2 let. c AMLA. Insurance intermediaries pursuant to Art. 40 ff. ISA are also not covered by this provision.

42 **Life insurance** means personal insurance (as opposed to property insurance) and includes a savings component. Pure risk insurance and insurance contracts under pillars 2 and 3a are not affected (Art. 43 FINMA AEOIF), nor are property insurance, other personal insurance (in particular health or accident insurance) or reinsurers.

43 With regard to the **distribution of collective investment schemes**, this activity is considered to be financial intermediation and is subject to the AMLA pursuant to Art. 2 para. 2 AMLA if the insurance company, in addition to distributing funds, simultaneously accepts assets from its clients/insured persons. The simple distribution of funds does not involve any elements of financial intermediation and is therefore not subject to the AMLA.

44 Furthermore, insurance companies, including insurance companies other than those referred to in Art. 2 para. 2 let. c AMLA, remain subject to the AMLA if they engage in **financial intermediation** as defined in Art. 2 para. 3 AMLA, in particular when granting mortgages.

45 In accordance with Art. 12 AMLA, FINMA is responsible for supervising insurance companies in accordance with Art. 2 para. 2 let. c AMLA. With regard to due diligence obligations, these are governed, for insurance companies in the

areas of life insurance and mortgage lending, by the provisions of the **Regulations of the Self-Regulatory Organization of the Swiss Insurance Association** (SIA) for the prevention of money laundering and terrorist financing pursuant to Art. 42 para. 1 OBA-FINMA, regardless of whether they are members of the SIA-SIA. If an insurance company carries out other financial intermediation activities unrelated to insurance, outside the regulatory remit of the SIA-SIA, e.g. asset management or lending, the general provisions of the FINMA AMLA on money laundering and the identification requirements of Art. 44 to 71 FINMA AMLA are decisive and applicable according to FINMA. In this context, it would have been welcome to have a Title 5 and a less restrictive description of the scope of application in Art. 43a AMLA-FINMA in order to avoid any contradictions and thus legal uncertainty.

F. Securities dealers

In accordance with Art. 2 para. 2 let. d AMLA, securities dealers referred to in Art. 2 para. 1 let. e FINMASA must be classified as financial intermediaries. They are subject to supervision by **FINMA** and require authorization from FINMA in order to carry out their activities. 46

Securities dealers are persons who, on a professional basis, i) trade in securities in their own name, **on behalf of clients**, ii) trade in securities on a short-term basis **on their own account**, are primarily active on the financial market and could jeopardize the proper functioning of the market, operate as a member of a trading platform or operate an organized trading facility within the meaning of Art. 42 FINMASA, or iii) trade in securities on a short-term basis on their own account and offer the public, on a permanent basis or on request, a price for certain securities (market makers) (Art. 41 FINMA). 47

In accordance with Art. 35 OBA-FINMA, **CDB 20** applies to securities firms for the verification of the identity of the contracting party and the identification of the controlling person and the beneficial owner of the assets. 48

G. Central counterparties and central securities depositories

In accordance with Art. 2 para. 2 let. d^{bis} AMLA, central counterparties and central securities depositories within the meaning of the LIMF are to be classified as financial intermediaries. They are subject to supervision by **FINMA** and require authorization from FINMA in order to carry out their activities. 49

50 **Central counterparties** are organizations based on common rules and procedures that interpose themselves between the counterparties to a securities transaction or other financial instrument contract, thereby becoming the buyer to every seller and the seller to every buyer (Art. 48 FIDMA).

51 Operators of a central depository or a securities settlement system are considered **central depositories** (Art. 61 para. 1 FINMASA). A central depository is an organization that provides centralized custody of securities and other financial instruments under common rules and procedures (Art. 61 para. 2 FINMASA). A securities settlement system is an organization that clears and settles transactions in securities and other financial instruments in accordance with common rules and procedures (Art. 61 para. 3 LIMF).

52 In accordance with Art. 17 let. a LBA, FINMA is competent to specify due diligence obligations by means of an ordinance. However, the FINMA AMLO does not apply to central counterparties and central securities depositories (Art. 3 para. 1 FINMA AMLO a contrario). In practice, FINMA will determine the modalities for implementing due diligence obligations as part of its licensing and supervisory activities.

H. Payment systems

53 In accordance with Art. 2 para. 2 let. d^{ter} AMLA, payment systems, insofar as they require authorization from FINMA within the meaning of Art. 4 para. 2 AMLA, are to be classified as financial intermediaries. They are subject to supervision by **FINMA** and require authorization from FINMA in order to carry out their activities.

54 Organizations based on common rules and procedures that serve to clear and settle payment obligations are considered **payment systems** within the meaning of the LIMF (Art. 81 LIMF). The operator of a payment system must obtain authorization from FINMA if the functioning of the financial markets or the protection of financial market participants so requires and if the payment system is not operated by a bank (Art. 4 para. 2 AMLA).

55 Other payment systems that are not covered by Art. 2 para. 2 let. d^{ter} AMLA, i.e. payment systems that do not require authorization from FINMA under the FIML, may nevertheless fall under Art. 2 para. 3 AMLA, in particular let. b (services in the field of payment transactions).

In accordance with Art. 17 let. a AMLA, FINMA is competent to specify due diligence obligations by means of an ordinance. However, the FINMA AMO does not apply to payment systems (Art. 3 para. 1 FINMA AMO a contrario). As with central counterparties and central securities depositories (see N. 51), FINMA will in practice determine the modalities for implementing due diligence obligations as part of its licensing and supervisory activities. 56

I. Trading systems based on DLT

In accordance with Art. 2 para. 2 let. d^{quater} AMLA, trading systems for securities based on distributed ledger technology (DLT) within the meaning of Art. 73a FINMASA qualify as financial intermediaries. They are subject to supervision by **FINMA** and require authorization from FINMA in order to carry out their activities. 57

Professionally operated organizations intended for the multilateral trading of securities based on DLT, aimed at the simultaneous exchange of offers between several participants and the conclusion of contracts according to non-discretionary rules, and fulfilling at least one of the following conditions, are considered **trading systems based on DLT**: a. they admit participants referred to in Art. 73c para. 1 let. e LIMF; b. they ensure the centralized custody of securities based on TRD on the basis of common rules and procedures; or c. they clear and settle securities transactions based on TRD on the basis of common rules and procedures (Art. 73a para. 1 LIMF). 58

Trading systems based on DLT have been added to the list in Art. 2 para. 2 AMLA with effect from August 1, 2021, as part of the adaptation of federal law to developments in distributed ledger technology, since they are likely to carry out activities that are considered to be **financial intermediation**. Title 5 of the FINMA AEOF (Art. 43a ff. FINMA AEOF) is applicable and specifies, in particular, the requirements for verifying the identity of the contracting party and identifying the beneficial owner. 59

J. Casinos

In accordance with Art. 2 para. 2 let. e AMLA, casinos within the meaning of the Gaming Act (LJAr) are to be classified as financial intermediaries. In addition, the Gaming Act also stipulates that they are subject to the AMLA (see Art. 67 para. 1 LJAr). Casinos within the meaning of the Casinos Act must ob- 60

tain a license from the **Federal Council** (Art. 5 and 6 Casinos Act) and authorizations from the **Federal Gaming Board** (FGB) for the casino games they operate (Art. 16 Casinos Act). They are supervised by the FSTC, particularly with regard to compliance with money laundering obligations (Art. 97 para. 1 let. a ch. 2 LJAr and Art. 12 let. b AMLA). The FSTB is also responsible for specifying the due diligence obligations under the AMLA (Art. 1 para. 1 let. b AMLA), which it has done by means of the FSTB AMLO.

61 In accordance with Art. 67 para. 2 LJAr, the scope of **due diligence** obligations in the fight against money laundering depends on the risk and characteristics of the game and the distribution channel. For games operated online, the identification of the contracting party at the time of establishing the business relationship may be based on a self-declaration (Art. 68 para. 1 LJAr). The identity of the contracting party must be verified in accordance with Art. 3 para. 1 AMLA when the monthly stakes or winnings, whether one-off or cumulative over a month, reach a significant amount (Art. 68 para. 2 LJAr). The amounts considered to be significant for casino games are determined by the FMCA and currently stand at CHF 4,000 (Art. 3 OBA-CFMJ).

K. Large-scale gaming operators

62 In accordance with Art. 2 para. 2 let. f AMLA, large-scale gaming operators within the meaning of the LJAr are to be classified as financial intermediaries. In addition, the LJAr also stipulates that they are subject to the AMLA (see Art. 67 para. 1 LJAr). Large-scale gaming operators must obtain a gaming license from the inter-cantonal supervisory and enforcement authority referred to in Art. 105 LJAr (Art. 24 para. 1 LJAR). They are supervised by the aforementioned inter-cantonal authority, in particular with regard to compliance with money laundering obligations (Art. 107 para. 1 let. a ch. 2 LJAr and Art. 12 let. b^{bis} AMLA). The **FDJP** is responsible for specifying the due diligence obligations under the AMLA (Art. 1 para. 1 let. c AMLA), which it has done by means of the OBA-FDJP.

63 In accordance with Art. 67 para. 2 LJAr, the scope of **due diligence** obligations in the fight against money laundering depends on the risk and characteristics of the game and the distribution channel. Relief has been provided for operators of large-scale games that are not operated online or are operated online. Operators of large-scale games that are not operated online only have to comply with the due diligence obligations under Art. 3 to 7 AMLA when a

player wins a large amount (Art. 67 para. 3 LJAr). In the case of operators of large-scale games that are operated online, the identification of the contracting party at the time of establishing the business relationship may be based on a self-declaration (Art. 68 para. 1 LJAr). The identity of the contracting party must be verified in accordance with Art. 3 para. 1 AMLA only when the monthly stakes or winnings, whether one-off or cumulative over a month, reach a significant amount. The FDJP is responsible for determining the amounts considered significant, taking into account the dangers associated with the games concerned (Art. 67 para. 4 LJAr). To date, the thresholds are set at between CHF 5,000 and CHF 25,000 depending on the type of game and the risk of the business relationship between the operator and the player (Art. 3 and 4 OBA-DFJP).

L. Commercial assayers

In accordance with Art. 2 para. 2 let. g AMLA, commercial assayers and group companies referred to in Art. 42bis LCMP must be classified as financial intermediaries. Pursuant to Art. 42bis para. 1 LCMP, commercial assayers who trade in bank precious metals on a professional basis, either themselves or through a group company, must obtain a license from the **Central Office for the Control of Precious Metals** (Central Office). They are subject to supervision by the Central Office with regard to compliance with AMLA obligations (Art. 42ter LCMP and Art. 12 para. b^{ter} AMLA). The **FDFA** is responsible for specifying the due diligence obligations under the AMLA (Art. 17 para. 1 let. d AMLA), which it has done by means of the OBA-FDFA. 64

Before the status of financial intermediary directly subject to FINMA supervision (IFDS) was repealed with the entry into force of the FinIA and the related amendments to the AMLA, commercial assayers who traded in bank precious metals and were thus considered financial intermediaries within the meaning of the AMLA were, for the most part, directly subject to FINMA supervision as DFI. With the abolition of DFI status, they would have had to join a SRO for AMLA supervision, which would have created various practical difficulties. During the consultation process on the FinIA, it was therefore decided, on the basis of a proposal by the Swiss Precious Metals Manufacturers and Traders Association (ASFCMP), to strengthen the powers of the central office by also assigning it AML supervision of commercial assayers. The AMLA supervisory powers of FINMA and the SROs were thus transferred to the Central Office 65

with effect from January 1, 2023, without any material changes, as the Central Office had largely adopted FINMA's practices. The **centralization of powers** relating to AMLA and LCMP supervision within a single authority is entirely justified. This has improved the effectiveness of supervision, avoided duplication, and limited costs for supervised entities, while ensuring the use of a state body that is known, understood, and accepted internationally.

BIBLIOGRAPHY

Bovet Christian/Bacharach Jeremy, Commentaire de l'art. 2 LBA, in: Cassani Ursula, Bovet Christian, Villard Katia (éd.), Commentaire Romand (CR), Loi sur le blanchiment d'argent, 1ère édition, Bâle 2022.

Commentaire du Règlement de l'OAR-ASA, https://www.sro-svv.ch/fr/textes-juridiques/commentaire-du-reglement-oar-asa, visité le 23.8.2024.

Jutzi Thomas/Abbühl Andri, Fintech und DLT, Privat- und finanzmarktrechtlich Grundlagen in der Schweiz, Bern 2023.

Nagel Thomas, Der persönliche und sachliche Geltungsbereich des schweizerischen Geldwäschereigesetzes (GwG), Zürich 2020.

Nagel Thomas, Der persönliche und sachliche Geltungsbereich des schweizerischen Gelwäschereigesetzes (GwG) – Mit rechtsvergleichenden Hinweisen zu internationalen Standards, dem Recht der Europäischen Union und dem deutschen Recht, in: SSFM – Schweizer Schriften zum Finanzmarktrecht Band/Nr. 132 Zürich 2020, S. 91-135.

OFDF, Négoce de métaux précieux bancaires, https://www.bazg.admin.ch/bazg/fr/home/themes/controle-des-metaux-precieux/handel-mit-bankedelmetallen.html#context-sidebar, visité le 27.8.2024.

Peyer Martin, Kommentierung zu Art. 2 Abs. 2 GwG, in: Hsu Peter Ch., Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, 1. Aufl., Basel 2021.

Schären Simon, Kommentierung zu Art. 2 Abs. 2 GwG, in: Peter V. Kunz, Jutzi Thomas, Schären Simon (Hrsg.), SHK – Stämpflis Handkommentar, 1. Aufl., Bern 2017.

Wyss Ralph, Kommentierung zu Art. 2 GwG, in: Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), OFK – Orell Füssli Kommentar, Geldwäschereigesetz, 3. Aufl., Zürich 2019.

Zysset Pascal/Nagel Thomas, Der räumliche Geltungsbereich des Geldwäschereigesetzes, GesKR 2018, S. 140-155.

MATERIALS

Message relatif à la loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués (TRD), FF 2020 223, disponible sous https://www.fedlex.admin.ch/eli/fga/2020/16/fr, visité le 10.9.2024.

Message concernant la modification de la loi sur les placements collectifs (Limited Qualified Investor Fund, L-QIF), FF 2020 6667, disponible sous https://www.fedlex.admin.ch/eli/fga/2020/1852/fr, visité le 10.9.2024.

Message relatif à la loi fédérale concernant la lutte contre le blanchissage d'argent dans le secteur financier (Loi sur le blanchissage d'argent, LBA) du 17 juin 1996, disponible sur https://www.fedlex.admin.ch/eli/fga/1996/3_1101_1057_993/fr, visité le 10.9.2024.

Commentaires relatifs à la modification de l'ordonnance sur la lutte contre le blanchiment d'argent et le financement du terrorisme, 31 août 2022, disponible sous https://www.newsd.admin.ch/newsd/message/attachments/73350.pdf, visité le 10.9.2024.

Département fédéral des finances (DFF), Commentaires relatifs à l'ordonnance sur les services financiers (OSFin), l'ordonnance sur les établissements financiers (OEFin) et l'ordonnance sur les organismes de suveillance (OOS), 6 novembre 2019, disponible sous https://www.newsd.admin.ch/newsd/message/attachments/58957.pdf, visité le 10.9.2024.

Département fédéral des finances (DFF), Commentaires relatifs à la révision de l'ordonnance sur les banques "Autorisation FinTech", 30 novembre 2018, disponible sous https://www.newsd.admin.ch/newsd/message/attachments/54882.pdf, visité le 10.9.2024.

FINMA, Commentaires relatifs à la révision partielle de l'ordonnance de la FINMA sur le blanchiment d'argent (OBA-FINMA), 27 octobre 2022,

disponible sous https://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/anhoerungen/laufende-anhoerungen/20221102-gwv-finma/erlaeuterungen_gwv_finma_20221027_de.pdf?sc_lang=fr&hash=C7B88C0C76850E0F78D15EB2D92AB997, visité le 10.9.2024.

FINMA, Rapport explicatif sur la révision partielle de l'OBA-FINMA, 4 septembre 2017, disponible sous https://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/anhoerungen/laufende-anhoerungen/rs-gwv/20170904-eb-gwv-finma.pdf?sc_lang=fr&hash=61DE46F996C89A314261C90D50555E82, visité le 10.9.2024.

FINMA, Rapport explicatif sur la révision totale de l'OBA-FINMA, 11 février 2015, disponible sous https://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/8news/medienmitteilungen/2015/02/20150211-eb-gwv-finma.pdf?sc_lang=fr&hash=1230CA31F493FFD305859491E973444E, visité le 10.9.2024..

FINMA, Rapport sur les résultats de l'audition relative à l'OBA-FINMA, 3 juin 2015, disponible sous https://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/anhoerungen/abgeschlossene-anhoerungen/20150603-gwv-finma-revision/ab_gwv_finma_20150603_de.pdf?sc_lang=fr&hash=1DFF5386AFA05F276AB6AAA6E0AEB28F, visité le 10.9.2024.

FINMA, Circulaire 2011/1 Activité d'intermédiaire financier au sens de la LBA, Précisions concernant l'ordonnance sur le blanchiment d'argent, 4 novembre 2020, disponible sous https://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2011-01-01-01-2017.pdf?sc_lang=fr&hash=9314F3466AA57D97A85B0E1C82707B9F, visité le 10.9.2024.

FINMA, Circulaire 2018/3 Outsourcing, Externalisations dans le secteur des banques, des entreprises d'assurance et de certains établissements financiers au sens de la LEFin, 4 novembre 2020, disponible sous https://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2018-03-01012021_de.pdf?

sc_lang=fr&hash=4A3159F8525175E2EF67A8DB0F742AED, visité le 10.9.2024.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 2 para. 3 AMLA

A commentary by Doris Hutzler / David Meirich

SUGGESTED CITATION

Doris Hutzler/David Meirich, Commentary of art. 2 para. 3 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Hutzler/Meirich, art. 2 para. 3 AMLA.

Art. 2 Scope of application

[3] Financial intermediaries are also persons who on a professional basis accept or hold on deposit assets belonging to others or who assist in the investment or transfer of such assets; they include in particular persons who:

a. carry out credit transactions (in particular in relation to consumer loans or mortgages, factoring, commercial financing or financial leasing);

b. provide services related to payment transactions, in particular by carrying out electronic transfers on behalf of other persons, or who issue or manage means of payment such as credit cards and travellers' cheques;

c. trade for their own account or for the account of others in banknotes and coins, money market instruments, foreign exchange, precious

metals, commodities and securities (stocks and shares and value rights) as well as their derivatives;

d. ...

e. ...

f. make investments as investment advisers;

g. hold securities on deposit or manage securities.

CONTENT

I. Basis 79
A. Purpose and relationship between paragraphs 2 and 3 79
B. Regulatory cascade 79
C. Structure of the provision 80
D. Interpretation of the provision 81
E. Recommended assessment method 82
II. Scope 83
A. Geographical 83
B. Personal and factual 84
III. Exceptions 85
A. General 85
B. Non-regulated financial intermediaries 86
C. No financial intermediation activities 86
1. Physical transport and storage 86
2. Debt collection 86
3. Ancillary transfer 88
4. Pillar 3a 90
5. Services within the group 90
D. Auxiliary persons 91
E. State action 92
IV. List of criminal offenses (Art. 2 para. 3 lit. a–g AMLA) 92
A. Introduction 92
B. Credit business (lit. a) 93
1. General 93
2. Mortgage loans and other cash loans 94
3. Consumer loans 95
4. Trade finance 96
5. (Financial) leasing 96
6. Factoring 96
7. Credit agreements not subject to the AMLA 97
C. Payment transaction services (lit. b) 99
1. General 99
2. Execution of payment orders / electronic transfers 100
3. Assistance with the transfer of virtual currencies 102
4. Means of payment and payment systems 105
5. Money or value transfer business 109
D. Trading activity (lit. c) 112
1. General 112
2. Trading in banknotes and coins (cash) 113
3. Foreign exchange trading (book money) 114

4. Trading in bank precious metals (gold, silver, platinum, palladium) 115
5. Currency exchange 116
6. Trading in commodities (on and off the exchange) 117
7. Securities trading 119
8. Money market instruments 120
E. Making investments as an investment advisor (lit. f) 121
F. Custody or management of securities (lit. g) 122
G. Activity as an organ of domiciliary companies 125
H. Insurance intermediaries 128
I. Attorneys and notaries 130
J. Real estate sector 132
V. General clause 134
A. Structure 134
B. Third-party assets 134
C. Financial intermediary activity 135
VI. Professionalism 137
A. Fundamentals 137
B. General criteria (Art. 7 AMLO) 138
C. Credit business (Art. 8 AMO) 140
D. Money and value transfer business (Art. 9 AMLO) 141
E. Trading business (Art. 10 AMLO) 141
VII. Consequences of the obligation to comply 141
A. SRO affiliation 141
B. Supervisory and criminal consequences of non-compliance 143
Bibliography 144
Materials 148

I. BASIS

A. Purpose and relationship between paragraphs 2 and 3

According to Art. 2 para. 1 AMLA, the Anti-Money Laundering Act applies primarily (lit. a) to **financial intermediaries** and secondarily (lit. b) to natural and legal persons who trade in goods on a commercial basis and accept cash in the process (dealers). The term "financial intermediaries" encompasses all natural and legal persons described in paragraphs 2 and 3 of the Act. 1

The list in Art. 2 para. 2 AMLA initially refers exclusively to institutions that are directly or indirectly **supervised** by FINMA as financial intermediaries, whereby reference is made to the respective special laws for their definition. 2

However, since institutions without FINMA authorization can also engage in financial intermediation activities that are (also) "particularly susceptible to money laundering" but "where the risk of abuse for money laundering purposes is less obvious," the so-called parabanking sector has been made subject to money laundering legislation under the supervision of self-regulatory organizations approved by FINMA in accordance with Art. 24 para. 1 AMLA. The activities covered correspond to the scope of Art. 305ter para. 1 of the Swiss CC. In addition to the general clause, Art. 2 para. 3 lit. a–g AMLA lists **a catalog of criminal offenses**. While Art. 2 para. 2 AMLA thus refers to the respective license category, Art. 2 para. 3 AMLA refers specifically to the activities covered. How these activities are classified under contract law is not decisive. 3

Para. 3 is a subsidiary **final provision** in relation to para. 2. This means that the same financial intermediary cannot be subject to both para. 2 and para. 3 at the same time and that para. 3 can only apply if a financial intermediary is not already subject to para. 2 of the AMLA. 4

B. Regulatory cascade

Based on Art. 41 para. 1 AMLA, the Federal Council specifies the scope of application of Art. 2 para. 3 AMLA in Art. 2 ff. of the **Ordinance** on Combating Money Laundering and Terrorist Financing (Money Laundering Ordinance, AMLO) of November 11, 2015. 5

6 In its **Circular 2011/1** "Activities as a financial intermediary under the AMLO – Explanatory notes on the Anti-Money Laundering Ordinance (AMLO)", FINMA set out its practice for interpreting money laundering legislation, including examples of activities that are subject to the Anti-Money Laundering Act. The FINMA circular has no independent regulatory effect, but is very relevant in practice as a guideline.

7 FINMA Circular 2011/1 replaces the **subordinate commentary** of the former Money Laundering Control Authority dated October 29, 2008 (UK Kst. AMLA), which continues to serve as an interpretative aid in doctrine and practice due to its more detailed explanations.

C. Structure of the provision

8 Art. 2 para. 3 AMLA contains a **general clause** with an abstract definition. According to this, persons who "accept or hold assets of third parties on a commercial basis or participate in their investment or transfer" are initially considered financial intermediaries.

9 The paragraph then contains a specific list of **catalogued circumstances**, which is not exhaustive according to the connecting term "in particular." Here, too, the catalogued circumstances take precedence over the general clause in the sense of a *lex specialis*. It must therefore first be examined whether a circumstance under Art. 2 para. 3 lit. a–g AMLA exists. If this is not the case, the second step is to examine whether the general clause could be fulfilled. One argument in favor of this approach is that some of the catalog cases impose special requirements on professional conduct.

10 Both the law and the ordinance contain **exemptions** that must be observed. Art. 2 para. 4 AMLA excludes certain activities and institutions from the scope of the AMLA. Art. 2 para. 2 AMLO contains specific exemptions that refer to Art. 2 para. 3 AMLA. These exceptions apply to both the general clause and the special circumstances.

11 The exemplary list of activities in Art. 2 para. 3 AMLA should not obscure the fact that some of the cases listed in the catalog go beyond the scope of the general clause. Accordingly, not every person who meets the criteria of a case listed in the catalog necessarily also meets those of the general clause. Rather, the catalog contains separate **special circumstances** that extend the scope of application of Art. 2 para. 3 AMLA and have an independent meaning.

From a legal perspective and for better understanding, it would be desirable to indicate this accordingly in the wording of the law.

D. Interpretation of the provision

The interpretation of the AMLA by the AMLA supervisory authority was based on the purpose of the AMLA (Art. 1) with corresponding materials in a form that deliberately aimed to apply the AMLA only to persons active in the financial sector. Accordingly, only activities attributable to the financial sector, including those listed in the catalog in Art. 2 para. 3 lit. a–g AMLA, should be subject to Art. 2 para. 3 AMLA. This catalog should form the "starting point for the interpretation of the general clause." Activities that are comparable or very similar to those listed in the catalog should be examined on a case-by-case basis and, if necessary, be subject to the AMLA via the general clause. Other activities such as real estate, antiques, or art trading are expressly excluded. These findings remain valid even though the scope has been extended to include trading since 2016 and, according to the ongoing revision of the law, will also include consulting services outside of financial intermediation in the future. Art. 2 para. 3 AMLA remains reserved even with the latest revision of financial intermediation and is clearly distinguished from other services. 12

The general clause of Art. 2 para. 3 AMLA is formulated in abstract and open terms in order to subject activities that are attractive for money laundering and are neutral in terms of technology and innovation to the due diligence and reporting obligations of the AMLA. New forms of financial intermediation should not have to be regulated retrospectively. According to the case law of the Federal Supreme Court, the interpretation of subordination must therefore be handled restrictively. The "regulatory technique used, which merely describes the group of financial intermediaries in an open and exemplary manner, requires that, in addition to the wording, the meaning and purpose of the norm be taken into account more strongly in its interpretation." In legal doctrine, this consideration is interpreted to mean that the application of money laundering regulations is only justified in cases where there are activities and circumstances that pose a **money laundering risk**. However, if such a risk is only low, the scope of the due diligence obligations should also be adjusted accordingly. This approach is reflected in particular in the simplified due diligence obligations under the GwV-FINMA. 13

14 The **Federal Administrative Court** has clarified that it is not the intention of the AMLA or the AMLO to require proof or justification of a specific money laundering risk in addition to the legally defined elements of the offense in order to be subject to the law. If an activity meets the legal criteria, it is justified that it is subject to the law without further proof of risk. This is appropriate because the legislator has only included circumstances with an inherent money laundering risk in the law, which is why a further risk assessment by the authorities applying the law is not necessary.

E. Recommended assessment method

15 The following assessment scheme can be used to determine whether an activity is subject to the AMLA:

Schritt	Frage	Ja	Nein
1	Liegt ein FI nach Abs. 2 vor? (z.B. Bank, Vermögensverwalter etc.)	Abs. 3 nicht anwendbar (Unterstellung nach Art. 2 Abs. 2)	Weiter zu Schritt 2
2	Liegt die Tätigkeit im räumlichen Geltungsbereich des GwG (Art. 2 Abs. 1 lit. a GwV)?	Weiter zu Schritt 3	keine Unterstellung in der Schweiz
3	Liegt eine Ausnahme nach Art. 2 Abs. 4 GwG oder Art. 2 Abs. 2 GwV oder gem. FINMA-RS 2011/1 vor? (z.B. SNB, Säule 3a, Inkasso, physischer Transport, Hilfsperson, staatliches Handeln etc.)	keine Unterstellung	Weiter zu Schritt 4
4	Ist bei einer Tätigkeit ein Katalogtatbestand (lit. a-g i.V.m. Art. 3 ff. GwV) erfüllt? (z.B. Leasing, Konsumkredit, Zahlungsdienstleistung, Money Transmitter, VASP, Organ einer Sitzgesellschaft etc.)	Weiter zu Schritt 5	Weiter zu Schritt 6
5	Wird die Tätigkeit berufsmässig ausgeübt - unterschiedliche Anforderungen, je nach Katalogtatbestand i.S.v. Art. 7 ff. GwV? (über einem bestimmten Bruttoerlös, Anzahl Geschäftsbeziehungen, Transaktionsvolumen etc.)	Unterstellung	Weiter zu Schritt 6
6	Ist der Grundtatbestand erfüllt? (fremde Vermögenswerte, finanzintermediäre Handlung)	Weiter zu Schritt 7	keine Unterstellung
7	Wird die Tätigkeit berufsmässig ausgeübt (*nur* Art. 7 GwV)?	Unterstellung	keine Unterstellung

II. SCOPE

A. Geographical

In contrast to financial intermediaries under Art. 2 para. 2 AMLA, the **geographical scope** of financial intermediaries under Art. 2 para. 3 AMLA is expressly regulated in the Anti-Money Laundering Ordinance (AMLO). According to Art. 2 para. 1 lit. a AMLO, the AMLA applies to financial intermediaries who **actually** operate in Switzerland or from Switzerland. 16

According to FINMA practice, a financial intermediary operates **in Switzerland or from Switzerland** if it has its registered office in Switzerland or is entered in the commercial register (formal establishment) or if it employs persons in Switzerland who permanently carry out or conclude financial intermediation activities for it in Switzerland or from Switzerland or who can legally oblige it to do so (de facto branch). The geographical scope of the AMLA is therefore determined by the place where the financial intermediation activity is predominantly carried out. 17

In the case of a **formal establishment** or branch office, the geographical reference point is the place of residence (for natural persons/sole proprietorships) or the registered office (for legal entities) as the formal center of activity. A company with its registered office in Switzerland is therefore subject to the AMLA, even if it only has a C/O address here and both its actual management and the focus of its operational financial intermediation activities are located abroad. 18

Persons who permanently support the foreign financial intermediary in carrying out significant parts of its financial intermediation activities in Switzerland or from Switzerland fall under the category of **de facto branches**, but not those constellations in which only the customer has a connection to Switzerland. Accordingly, branches of companies that are incorporated under foreign law and have their headquarters abroad, but whose financial intermediation activities are mainly carried out from Switzerland, are subject to regulation. An activity is carried out from Switzerland if, for example, the contractual relationship with the client is managed by the financial intermediary in Switzerland, even if the transactions are executed by the branch abroad. 19

According to FINMA practice, subordination under the AMLA requires a certain **degree of permanence** of the activity in Switzerland, while purely tem- 20

porary activities are not considered permanent. The element of permanence is not defined in more detail in FINMA Circular 2011/1 and requires a case-by-case assessment. The criteria used in doctrine are the absolute duration of the activity, the regularity of presence, the type of financial intermediary activity, and the mechanism for exercising physical presence.

21 The **personal connection** implies a distinction from a purely mechanical connection. A server or purely online services in Switzerland therefore do not constitute an activity relevant to the AMLA. As long as a financial intermediary in Switzerland has staff who merely acquire customers and maintain customer relationships, but in no way commits the financial intermediary, i.e., does not conclude contracts on behalf of the represented party and does not carry out financial intermediation transactions or essential components of such transactions, there is no physical presence in Switzerland within the meaning of Art. 2 para. 1 lit. a AMLO. Purely administrative or technical support therefore does not fall within the scope of the AMLA.

22 In the case of financial intermediaries **domiciled or headquartered abroad**, as with financial intermediaries headquartered in Switzerland, it must be examined on a case-by-case basis whether their activities in Switzerland meet the requirements for professional activity as a financial intermediary in accordance with Art. 7 AMLO. If this is the case, they are subject to the AMLA. The decisive factor for subordination is the activity actually carried out in Switzerland.

B. Personal and factual

23 Anyone who **actually** carries out the financial intermediary activities defined in Art. 2 para. 3 AMLA is personally subject to the AMLA. A person is only subject to the AMLA in relation to these activities. Accordingly, the due diligence obligations of the AMLA must only be observed in business relationships that are related to financial intermediary activities.

24 It is conceivable that a supervised activity may be carried out by **several persons**. In such a case, only the joint action of all persons fulfills the criteria of Art. 2 para. 3 AMLA. In such cases, all persons involved are considered financial intermediaries within the meaning of para. 3.

25 The **financial intermediary** may be a natural or legal person. The following applies to partnerships: If activities relevant to supervision are carried out by

a general partnership or a limited partnership, the partnership itself is a financial intermediary. If they are the subject of a simple partnership, each partner individually becomes a financial intermediary. In the latter case, the provisions of the partnership agreement are decisive for practical implementation.

The decisive factor for subordination is the exercise of the activity described in Art. 2 para. 3 AMLA and commented on below. Finally, it should be noted that even financial intermediation activities that meet the criteria only fall within the material scope of the AMLA if the requirement of commercial practice set out in Chapter VI is met and none of the exceptions described in Chapter III apply. 26

III. EXCEPTIONS

A. General

In the present case, a distinction must be made between **exceptions** under the law, under the ordinance, and under FINMA practice, whereby these are not (only), as might be expected, uniformly defined in accordance with the regulatory cascade, but represent different types of exceptions. 27

Art. 2 para. 4 AMLA provides for **general** exceptions to the registration requirement for institutions and activities that are considered financial intermediation but are not subject to registration due to the absence of money laundering risk. 28

Art. 2 para. 2 AMLO lists **specific** activities within the financial sector that are not classified as financial intermediation. FINMA has clarified these exemptions in a circular (see III.B. below). 29

Art. 2 para. 2 lit. b AMLO also provides for exceptions for **auxiliary persons** who carry out financial intermediation activities but are already covered by the client and therefore do not require separate supervision (see III.C. below). 30

In addition, in its practice, **FINMA** provides for financial intermediation activities in the form of (state) sovereign activities as a further exception to the obligation to comply (see III.D. below). 31

With regard to the **list of criminal offenses** in Art. 2 para. 3 lit. a–g AMLA, further information that could be described as "exceptions" can be found in Art. 3 ff. AMLO. For example, Art. 3 AMLO lists a catalog of credit relation- 32

ships that are not to be understood as credit transactions within the meaning of the AMLA. In the present case, such exceptions are examined in the context of the positive elements of the offense (see Chapter IV.B.7.). The absence of a professional activity could also be considered an "exception" (Art. 7 ff. AMLO). In the present case, however, this is also understood as a positive criterion and is therefore examined separately in Chapter VI. The same applies to the "exception" already outlined above, namely the absence of a connection to the geographical scope of Switzerland in accordance with Art. 2 para. 1 lit. a AMLA (see Chapter II.F.). The absence of a connection to the financial sector is also not considered an exception, but must be examined as a positive prerequisite in the general clause (see Chapter V.C.).

B. Non-regulated financial intermediaries

33 According to Art. 2 para. 2 and para. 3 AMLA, institutions whose activities are unlikely to be abused for money laundering would also be subject to the AMLA. The law provides for general **exceptions to** the obligation to comply in Art. 2 para. 4 AMLA.

C. No financial intermediation activities

1. Physical transport and storage

34 According to Art. 2 para. 2 lit. a no. 1 AMLO, persons who are engaged in the purely **physical transport** or purely physical storage of assets are not considered financial intermediaries. This refers to the transport of assets from one place to another and the purely physical storage of assets. The custody of securities is expressly reserved (Art. 6 para. 1 lit. c AMLO).

2. Debt collection

35 Debt collection pursuant to Art. 2 para. 2 lit. a no. 2 AMLO is also not considered financial intermediation. This is the case when a person collects a due claim on behalf of a creditor. The agent acts either as the direct representative of the creditor or in their own name vis-à-vis the debtor after the claims have been transferred to them by the creditor on a fiduciary basis. The decisive factor is that the agent has carried out the transfer on behalf of the creditor, which must be determined on the basis of circumstantial evidence. As a rule, the service is remunerated by the client.

Debt collection can also be considered to have taken place if the agent acts within a closed circle of **recipients of goods or services**. The purpose of the assignment is to ensure the smooth processing and simplification of payments to the supplier of the goods or services. 36

If the agent only has a contractual relationship with the creditor of the claim and acts on their behalf, this is usually a **debt collection order**, which does not constitute a financial intermediation activity. However, if the assets thus received are not forwarded to the creditor itself but to a third party in accordance with the creditor's instructions, this forwarding in turn constitutes a financial intermediation activity, whereby the party that previously collected the claim then acts as a financial intermediary between the creditor and the third party. 37

All due diligence obligations under the AMLA are linked to a contractual customer relationship. However, the (main) customer of a debt collection agency is always the creditor and never the debtor. If there is no contractual relationship between the debt collection agency and the debtor, the flow of money is considered debt collection, which is not subject to the AMLA. In this sense, debt collection activities on behalf of the creditor are excluded from the scope of the AMLA, as the debtor from whom the assets originate is not usually a contractual partner of the agent and therefore cannot be **identified**. 38

Thus, a **property manager** who, in the course of normal property management, receives amounts on behalf of, at the instruction of, and for the account of the property owner is not a financial intermediary within the meaning of the AMLA. If a real estate agent collects the purchase price from the buyer on behalf of the seller and is remunerated by the seller, this is also a collection activity that is not subject to the AMLA. 39

If the operator of a **crowdfunding platform** collects due support contributions on behalf of borrowers, this does not constitute a collection activity within the meaning of the AMLA. The same applies to a company in the field of **e-commerce** or the development and sale of software solutions for payments via the Internet, mobile phones, or similar, which additionally collects due receivables on behalf of the creditor and forwards them to the latter. In some cases, **telecommunications providers** offer, in addition to telecommunications services, the option of purchasing other services and goods and paying for them via mobile phone. However, if the rights and obligations of 40

the contracting parties with regard to the payment of goods and services are regulated, such a contractual relationship differs from a debt collection order, as a contractual regulation of the payment terms is atypical for debt collection activities. The close contractual relationship with the customer with regard to the terms of payment cannot be limited to a pure debt collection activity by the telecommunications company. In addition, the customer can usually decide whether to pay the provider of value-added services in cash, by credit card, by Maestro card, or by postpaid or prepaid. In such cases, the client for the transfer is therefore the debtor of the service and not the creditor. Without collection activities, such offers are therefore considered to be presumed payment services. When purchasing digital content, however, the question arises as to whether this is an ancillary service.

41 In connection with the operation of an **internet platform**, e.g., for the purchase, sale, rental, or exchange of services and products, goods, everyday items, etc., there may be indications of a collection activity in the above sense if (a) the payment processor only has a contractual relationship with the creditor; (b) in most cases, the payment processor charges the creditor a fee for providing the service; (c) the economic interest in the payment flow lies mainly with the creditor; (d) the relationship between the payment processor and the debtor is limited to the collection of the claim due, with no further rights and obligations existing or these serving only to ensure the debtor's confidence in the proper processing of payments and the smooth functioning of the platform. The following factors argue against debt collection activities (a) The debtor has an e-account on the payment processor's internet platform, to which they can add credit at will and from which the amount owed is debited when a service is used, or (b) payment via the payment processing system in question is only one of several payment options, and the debtor themselves becomes the principal when they choose a particular payment method. Since such platforms come in many different forms, it is not possible to give a general answer to the question of whether a platform is subject to the AMLA.

3. Ancillary transfer

42 According to Art. 2 para. 2 lit. a no. 3 AMLO, the transfer of assets as an **ancillary service** to a main contractual service is not subject to the AMLA.

43 According to FINMA practice, four criteria must be cumulatively met in order for a **ancillary service** to be assumed:

It is essentially an ancillary service that is part of a contractual relationship that is not attributable to the financial sector;

- the contracting party providing the main service also provides the ancillary service;
- This ancillary service is of secondary importance in relation to the main service, which can generally be assumed if no additional remuneration is charged for the ancillary service apart from the cost-covering expenses.
- The ancillary service is closely related to the main service, so that the provision of the main service without the provision of the ancillary financial intermediation service would entail particular difficulties for the contracting parties.

FINMA cites as a typical **example** the case in which a retirement and nursing home, in addition to the contractual main service, pays for goods or services from third parties on behalf of its customers from a deposit previously set up for this purpose. If visitors to a festival can use a chip to top up their festival wristband with credit (up to a certain maximum amount) in order to purchase goods at stands, with the remaining credit being transferred back to the visitors at the end of the event, this may also constitute an ancillary service that is not subject to supervision. The transfer of assets for digital content (e-newspapers, online games, or video-on-demand) by a telecommunications provider may also be an ancillary service. The ancillary service consists of providing billing options to service operators at the expense of the users of the services. In addition, the provision of billing options indirectly supports the distribution of digital content. As a rule, there is a close factual link between the main service and the ancillary service. However, in the case of value-added services based on physical products/goods (purchases), there is no ancillary service. The purchase of physical products/goods has no close factual link with the telecommunications services to be provided. Furthermore, the provision of the main service without the provision of the supplementary financial intermediation service does not pose any particular difficulties for the contracting parties, as the service user can switch to alternative payment options. 44

The execution of payment orders by accountants in addition to **accounting services** is generally not considered ancillary. Classifying such payment transactions as ancillary services would contradict the spirit and purpose of 45

Art. 4 para. 1 lit. a AMLO and mean that in the case of a power of attorney for a bank account and the execution of fiduciary or bookkeeping accounting, the AMLA would no longer apply. This is precisely not the intention of the legislator.

4. Pillar 3a

46 According to Art. 2 para. 2 lit. a No. 4 AMLO, the operation of **pillar 3a** pension funds by bank foundations or insurance companies does not constitute financial intermediation. Since the assets in pillar 3a pension funds are generally tied up for the long term and the amount of the payments and their tax exemption are limited by law, this activity is not considered particularly susceptible to money laundering.

47 While insurance policies are reviewed by FINMA and insurance companies are subject to FINMA supervision, **bank foundations** are subject to the cantonal BVG supervisory authorities. The bank foundation must manage the pension assets at a bank supervised by FINMA (account solution) or through its intermediary (securities account). This exception thus prevents multiple supervision and takes into account the principle of proportionality.

5. Services within the group

48 According to Art. 2 para. 2 lit. a No. 5 AMLA, the provision of services between group companies does not constitute financial intermediation either. In this context, the **group** is considered an economic unit of companies within the meaning of the AMLA if one company directly or indirectly holds more than half of the votes or capital of the other company or otherwise controls it. A group company that performs cash management or treasury functions within an industrial or commercial enterprise is therefore not a financial intermediary within the meaning of the AMLA. The regulation also applies to structures that are not managed by a legal entity but by a natural person.

49 However, the obligations under money laundering law do not apply to the activities of a supervised financial intermediary which, due to the **group exemption** within the meaning of Art. 2 para. 2 lit. a No. 5 AMLO, would not in themselves lead to supervision as a financial intermediary under the AMLA. It should also be noted that the issuance of means of payment that can be redeemed by customers at one or more group companies is subject to Art. 2 para. 3 lit. b AMLA.

D. Auxiliary persons

According to Art. 2 para. 2 lit. b AMLO, **auxiliary persons** of financial intermediaries that are licensed in Switzerland or affiliated with a self-regulatory organization (SROs) are considered to be covered by their license/SRO membership if the requirements under no. 1–6 are met. This exception therefore does not depend on the type of activity, but on the fact that the auxiliary persons are already subject to due diligence obligations through their clients. For this exception to apply, the auxiliary persons must: 50

- be carefully selected by the financial intermediary and be subject to its instructions and control (No. 1);
- be included in the financial intermediary's organizational measures and receive appropriate training and continuing education (No. 2);
- act exclusively on behalf of and for the account of the financial intermediary (No. 3);
- be remunerated by the financial intermediary and not by the end customers (No. 4);
- in the case of money or value transfer transactions, they must work exclusively for a single licensed financial intermediary or a financial intermediary affiliated with an SRO ("exclusivity clause," No. 5);
- they must have concluded a written agreement with the financial intermediary regarding compliance with the above requirements (No. 6).

The financial intermediary that engages the auxiliary person remains responsible under supervisory law for compliance with the due diligence obligations under the AMLA. With the exception of money or value transfers, auxiliary persons may work for several financial intermediaries that are licensed or affiliated with SROs. The latter exception primarily concerns **money transfer service providers**. In practice, individuals act as auxiliary persons for the responsible financial intermediary in the day-to-day business of money transfer service providers. It is the responsibility of the financial intermediary to ensure that there is an exclusive partnership with the auxiliary persons. 51

One of the prerequisites for the activity of the auxiliary person not to be considered independent financial intermediation is that they act exclusively **in the name and on behalf of** the financial intermediary (Art. 2 para. 2 lit. b no. 52

3 AMLO). In contrast, the activity as an organ can only be carried out in its own name. Subsidiaries of financial intermediaries cannot claim the status of an auxiliary person for themselves.

E. State action

53 According to FINMA practice, **state action** is not subject to the AMLA if it is carried out within the scope of sovereignty, even if the activity itself would be classified as financial intermediation. It must be examined in each individual case whether the activity is carried out within the scope of state sovereignty or not. Indications of a sovereign activity that is not subject to the AMLA include an explicit legal basis, a relationship of subordination, a public task, or the supervisory authority of a higher-level authority.

54 The state is therefore only subject to the AMLA when it acts within the scope of its non-sovereign activities. Since the fulfillment of sovereign tasks can also be transferred to private individuals, it is irrelevant from a money laundering law perspective in what "form" or organizational structure state action takes place and whether the legal relationships in question are to be classified as private law or administrative law contracts. The decisive factor is the criterion of **sovereignty**, which must be examined on the basis of the criteria described above.

55 According to FINMA practice, debt collection and bankruptcy offices, liquidators, guardians, pension fund administrators, estate administrators, and executors are not financial intermediaries. However, the latter two are subject to the AMLA if they provide financial intermediary services outside the scope of their mandate, for example in connection with their involvement in the distribution of an estate.

IV. LIST OF CRIMINAL OFFENSES (ART. 2 PARA. 3 LIT. A–G AMLA)

A. Introduction

56 Despite the use of the term "in particular," the list of criminal offenses in Art. 2 para. 3 lit. a–g AMLA in some cases goes beyond the general clause in Art. 2 para. 3 and, as the respective *lex specialis*, takes precedence over it. The list is therefore not exhaustive.

Since its introduction, the provision has been revised several times. For example, with effect from January 1, 2006, the Investment Fund Act (IFG) removed the supervisory requirement for investment fund distributors under letter d due to the lack of money laundering risk. The most significant **change** occurred with the introduction of the FinIA on January 1, 2020, which made asset management subsumed under letter e subject to a licensing requirement and moved asset managers and trustees as financial intermediaries subject to special legislation to Art. 2 para. 2 lit. a^{bis} AMLA. This also repealed letter e. However, due to the different thresholds for professional activity in the AMLA and the FinIA, asset managers and trustees who are not subject to the licensing requirement under the FinIA may still fall within the scope of the AMLA via the general clause or via Art. 2 para. 3 letters a–g AMLA letters f or g. 57

Art. 3 ff. AMLO specifies and, in some cases, restricts the **list of criminal offenses**, whereby it should be noted that Art. 4 AMLO in particular has undergone significant changes in 2021 due to technological developments in the area of payment transactions. 58

B. Credit business (lit. a)

1. General

According to Art. 2 para. 3 lit. a AMLA, persons are considered financial intermediaries if they conduct **credit transactions** and are not already subject to the special legal supervision of Art. 2 para. 2 AMLA (e.g., as a bank). Examples of this are consumer or mortgage loans, factoring, trade financing, and finance leasing. The provision covers activities that are similar to banking business but do not involve the acceptance of public funds and where refinancing is carried out to a significant extent by the group. 59

Art. 3 AMLO does not specify these activities in a positive sense, but by means of a **negative list** of activities that are expressly not considered credit transactions. For its part, FINMA specifies the negative list in the GwV-FINMA in its Circular 2011/1 and also sets out its practice for defining cash and consumer loans as well as trade financing, classifying transactions according to their purpose rather than the type of loan. 60

According to prevailing opinion, the **term "loan"** is interpreted broadly and functionally with reference to international guidelines and materials. In a 61

credit transaction, the lender undertakes to grant the borrower a monetary advantage, and the borrower undertakes to pay interest and repay the debt. This includes all transactions that have such financing as their purpose, are assigned to the financial sector, are carried out professionally, and do not fall under the exceptions. Traditionally, the term "credit" is also understood to mean a loan. In the case of a credit, the lender sets a limit within which the borrower can make withdrawals. In the case of a loan, the lender makes the entire loan amount available to the borrower from the outset, in accordance with the legal definition in Art. 312 of the Swiss Code of Obligations. According to FINMA practice, the term covers any transfer of money to a borrower in return for the borrower's obligation to repay the amount received and pay interest on it.

62 Legal scholars disagree on whether the credit business clarifies or expands the general clause. In any case, the **money laundering risk** of the credit business is unanimously seen in the assumption of interest and principal payments and is generally considered to be rather low. The specific risk is that assets from predicate offenses will be used to repay loans. There are a number of known cases in which funds from drug trafficking and fraud have been laundered through loans. However, the risk of terrorist financing through the misuse of loans is considered to be significantly greater. Providers of consumer loans are particularly at risk in this regard.

63 No money flows when a **settlement** is made. Accordingly, there is no possibility of using criminally acquired funds to repay loans. The risk of money laundering, which is why credit transactions are subject to the AMLA, cannot therefore arise in the first place. Although there is a flow of payments, the situation is comparable to unregulated debt collection.

64 The designation and categorization of credit transactions in the law, the ordinance, and the FINMA circular is inconsistent. The following therefore only deals with the **types of credit** mentioned as examples in the law that need to be discussed in practice.

2. Mortgage loans and other cash loans

65 Mortgage loans (lit. a) are defined as financing transactions for the acquisition and use of real estate or the construction or renovation of buildings, whereby the loan is secured by real estate.

According to FINMA practice, mortgage loans – in addition to overdraft facilities, bill discounting, Lombard loans, and long-term loans such as participation loans and subordinated loans – fall under the category of **cash loans**. It is irrelevant whether the loans are secured by collateral or other means. Pawnshops that grant loans against collateral are subject to the AMLA. 66

Crowdfunding – in particular its subtypes crowdlending and crowdinvesting – also counts as a credit business outside the banking sector and is a generic term for the financing of a project by a large number of investors via an internet platform (with or without consideration). Crowd investing usually refers to the financing of companies in an early stage of development. In return, investors receive shares in the company. Crowd lending focuses on the granting of loans from private individuals to private individuals (with the help of a platform). In return, borrowers pay interest to lenders. Due to the repayment of the loan, crowd lending is susceptible to money laundering. 67

If the **platform** acts as a lender to the borrower and refinances itself through crowdlending, the platform operator is conducting a lending business that is subject to supervision under Art. 2 para. 3 lit. a AMLA (and may require a special license, e.g., as a bank). A platform that does not act as a lender but allows the lenders' loan amounts to pass through its accounts is not conducting a lending business but may be providing a payment service. If the platform merely offers borrowers the opportunity to find lenders but does not otherwise perform any other functions in the credit relationship between the lenders and the borrower, this is generally not considered a credit business subject to supervision. Even if loans are granted via a platform, each lender remains responsible for checking whether they are subject to the AMLA. On the other hand, the platform operator also has an interest in ensuring that participants comply with regulatory requirements and in obtaining confirmation of this from participants in practice. 68

3. Consumer loans

According to the wording of Art. 2 para. 3 lit. a AMLA, **consumer loans** are also subject to the AMLA. However, the reference to the KWG in the FINMA circular requires clarification. The definition in the KWG can be used temporarily. However, loans that are exempt from the KWG due to their specific purpose (consumer protection) remain subject to the AMLA. Conversely, the exemptions in the AMLO do not necessarily apply to the KWG. 69

4. Trade finance

70 The **pre-financing** of a contracting party in the context of commercial transactions is also considered a loan. According to FINMA Circular 2011/1, the term "trade finance" generally includes discount loans, assignment loans, and finance leases, but also trade credits and sales financing. Trade financing is not subject to the AMLA if it constitutes an ancillary credit grant within the meaning of Art. 3 lit. f AMLO or if the interest and principal payments are not made by the contracting party.

5. (Financial) leasing

71 **Finance lease agreements**, which are expressly mentioned in Art. 2 para. 3 lit. a AMLA, are subsumed by FINMA under trade financing, but may also constitute a form of consumer credit. Ultimately, this depends on the leased asset (consumer goods or commercial goods) and ultimately makes no difference, as both forms are expressly subject to the AMLA.

72 In finance leases, in addition to the manufacturer, supplier or dealer and the lessee, there is a leasing company that acts as a third party. This company transfers the asset to the lessee for use for a non-cancellable contract term. In return, it receives a fixed lease payment, which is paid directly to the lessor. Ownership of the leased object remains with the lessor. The obligation to comply therefore applies to the **lessor** as the lender and pre-financier.

6. Factoring

73 In **factoring**, which is also expressly mentioned in Art. 2 para. 3 lit. a AMLA, the so-called factor can assign a creditor's claims from its business operations in return for payment. The due claim is collected from the debtor. Due to the change of creditor, repayment is not made by the pre-financier, but by a third party (whose debtor). Since, according to FINMA practice, Federal Supreme Court case law, and prevailing opinion, money laundering appears to be effectively ruled out in these activities if the cash flow does not originate from the (pre-financed) contractual partner but from a third party, factoring *contra legem* (analogous to forfaiting) does not fall under the AMLA. However, there are special types of factoring that do fall under the AMLA, as the repayment of the funds is made by the contractual partner. Factoring may therefore fall under the AMLA if it also fulfills a credit function, i.e., if the factor pays the sup-

plier the amount for the goods before the debtor's payment has been received.

7. Credit agreements not subject to the AMLA

In addition to those just mentioned (operating leases, factoring, etc.), Art. 3 AMO excludes further agreements from **subjection to** the AMLA, although this list is not to be understood as exhaustive ("in particular"). 74

The **borrower** is not subject to Art. 2 para. 3 lit. a AMLA (Art. 3 lit. a AMLO). Although a money laundering risk on the part of the lender cannot be ruled out with regard to the disbursement of the loan amount, the money laundering risk is traditionally associated with interest and principal payments. As a rule, however, a borrower is not professionally active. The question becomes more relevant in connection with crowdlending, where a borrower faces a large number of lenders. In this case, the money laundering risk on the part of the lenders is likely to be higher than in traditional lending business. 75

According to Art. 3 lit. b AMLA, the granting of loans **without interest and fees** is not profit-oriented and therefore does not constitute a form of credit similar to banking business. It is therefore not subject to the AMLA, even if pure repayment payments may also pose a money laundering risk. Furthermore, the requirement of professional activity is not met. 76

The granting of loans between **a company and its shareholders** is also not subject to the AMLO if the respective shareholder holds at least 10 percent of the capital or votes of the company (Art. 3 lit. c AMLO). The basis for this is the capital of the company (share capital including equity capital, share capital). This practice applies to credit relationships with all legal entities in which a capital or voting rights participation is possible. 77

If a lending **sister company** holds a direct or indirect participation of more than 10 percent in the other sister company, in our opinion the granting of credit is not subject to the AMLA, even if the threshold for professional activity is reached. However, the lending sister company cannot take into account the parent company's participation in the sister company. Without direct or indirect participation between sister companies, the exception in Art. 3 lit. c AMLA does not apply. 78

79 The granting of loans between **employers and employees** is also not subject to the AMLA, provided that the employer is obliged to pay social security contributions for the employees involved in the credit relationship. If this condition is not (or no longer) met, the employer becomes a financial intermediary.

80 Credit relationships between **affiliated persons** within the meaning of Art. 7 para. 5 AMLA are also not subject to the AMLA (Art. 3 lit. e AMLA).

81 The granting of loans that are **accessory** to another legal transaction is not subject to the AMLA (Art. 3 lit. f AMLO). This is an important distinction in practice. It refers to the granting of a subordinate credit in addition to a main transaction that is not attributable to the financial sector (e.g., purchase of goods, etc.). Examples of this are deferral of payment, granting of a payment deadline, or installment payment agreements. FINMA has developed the following cumulative criteria to determine whether a loan is ancillary:

- Provision of a good or service that is not attributable to the financial sector;
- The provider of the main service additionally grants a loan to its contractual partner;
- The granting of the loan is objectively related to the main service;
- The granting of the credit is of secondary importance in relation to the main service; and
- The funds used to grant the credit come from the general funds of the provider of the main service.

If the criteria for an **ancillary service** are met, there is no need to check whether the activity is carried out on a commercial basis within the meaning of Art. 7 ff. AMLO.

82 Operating leases (Art. 3 lit. g AMLA) and, as a rule, direct leases are not subject to the AMLA. In contrast to finance leases, **operating leases** have a relatively short transfer period for items and/or are easily terminable. The lessor generally bears the costs and risks of the leased item. The situation is comparable to a rental agreement, which is why it does not constitute the granting of credit. The granting of credit in the case of **direct leasing**, where the manufacturer or dealer is the lessor, is generally considered to be ancillary.

Contingent liabilities in favor of third parties, such as sureties or guarantees, are also not considered credit transactions (Art. 3 lit. h AMLA). The contractual partner granting the contingent liability is therefore not subject to the AMLA. 83

Credit intermediation does not constitute an activity subject to supervision. An obligation to comply with the AMLA only arises if, in addition to the intermediation activity, an activity pursuant to Art. 2 para. 3 AMLA is carried out (e.g., receiving and transferring funds on behalf of a customer). 84

Subsidiaries that receive refinancing from the parent company within the group may fall under the group exemption of Art. 2 para. 2 lit. a No. 5 AMLA. For the purposes of the AMLA, a group is considered an economic unit of companies if one company directly or indirectly holds more than half of the votes or capital of the other company or companies or controls them in another way. 85

Venture capital can be invested in a new company by various investors (private individuals, banks, venture capital companies) and in various forms (equity participation, loans). Anyone who participates in the capital of a company is not a lender but an investor and therefore, unlike a lender, not a financial intermediary. In the case of venture capital companies, the difference is even less clear, as they are only allowed to use their funds in the form of equity investments, subordinated loans, or other claims comparable to venture capital. It therefore does not seem justified to consider venture capital companies that grant subordinated loans as financial intermediaries, but not those that invest in capital. It should be noted that risk investments that (may) lead to the loss of criminally obtained funds do not constitute money laundering activities. 86

C. Payment transaction services (lit. b)

1. General

Art. 2 para. 3 lit. b AMLA regulates the special case of "**payment transaction services**," which is particularly relevant in practice. The law specifically mentions persons who "make electronic transfers for third parties or issue or manage means of payment such as credit cards and traveler's checks." The provision was originally introduced for payment transactions developed by the former PTT (Post-, Telefon- und Telegrafenbetriebe; now PostFinance) and for 87

services related to credit cards and traveler's checks and bank checks outside the banking sector. Payment transactions are defined as all payment transactions that transfer means of payment from the sender to the recipient.

88 Art. 4 AMLO also specifies payment services using non-exhaustive abstract definitions. FINMA Circular 2011/1 contains important information on FINMA's practice in this area. Payment service providers generally also comply with the general clause of Art. 2 para. 3 AMLA, as they accept third-party assets and help to transfer them. Technological developments and changes in this area show that the term "by name" is particularly important here and that some of the examples described in the law, ordinance, and FINMA practice are now obsolete (e.g., traveler's checks, etc.).

89 The **risk** of money laundering in payment transactions is classified as medium to high overall. The inclusion of payment services under the AMLA is justified due to the high liquidity of the assets involved, which are particularly suitable for money laundering due to the possibility of concealing their origin.

90 In the context of **artificial intelligence** in the financial sector, regardless of the method used, the question arises as to whether the provider in question qualifies as a financial intermediary on the basis of its activities. In this respect, AI-based applications do not pose any particular challenges when assessing whether they are subject to the AMLA.

2. Execution of payment orders / electronic transfers

91 According to Art. 4 para. 1 lit. a AMLO, a payment transaction service in the form of an **electronic transfer** exists if the financial intermediary transfers liquid financial assets to a third party on behalf of its contracting party and thereby takes physical possession of these assets, has them credited to its own account, or orders the transfer of the assets in the name and on behalf of the contracting party.

92 In addition to the general requirements of the general clause in Art. 2 para. 3 AMLA (financial intermediation, professional activity, activity in the financial sector), subordination under Art. 4 para. 1 lit. a AMLA therefore requires the following **criteria** to be met:

1. Power of disposal: The financial intermediary must obtain power of disposal over the assets that do not belong to it.

2. Liquid financial assets: The term is not defined in Art. 4 para. 1 lit. a AMLO. However, it seems appropriate to understand the term "financial assets" in the same way as the term "assets" within the meaning of the general clause in Art. 2 para. 3. This means that only assets that can be attributed to the financial sector are covered. Financial assets are "liquid" if they can be easily converted into cash or other assets.
3. Transfer to a third party: According to FINMA practice, all transfers and forwarding of funds carried out on behalf of the debtor are subject to the AMLA. The financial intermediary must have a contractual relationship with both parties to the transfer transaction (so-called tripartite relationship).

If this condition is met, **subordination** applies regardless of whether the debtor compensates the financial intermediary before or after the transfer or forwarding to the third party. This also applies to persons who execute payment orders for third parties by bank proxy, including via e-banking, or if book money payments are forwarded to a beneficiary via a transit account in accordance with the debtor's instructions. Payment orders relating to e-money are also covered by the requirement. 93

Operators of **crowdfunding platforms** that enable investments in companies are also subject to this requirement if the platform operator itself accepts funds and forwards them to the respective companies. 94

A large proportion of **payment orders** in Switzerland are processed by banks and the postal service via clearing systems (with foreign countries usually via correspondent banks). While banks are subject to prudential supervision within the meaning of Art. 2 para. 2 lit. a AMLA, the postal service qualifies as a financial intermediary for this area of business in accordance with Art. 2 para. 3 lit. b AMLA. Clearing service providers are not subject to the AMLA if, as is customary in practice, they operate vis-à-vis financial intermediaries within the meaning of Art. 2 para. 2 AMLA (exemption from supervision pursuant to Art. 2 para. 4 lit. d AMLA). 95

The execution of **salary payments** on behalf of third parties is generally an activity subject to the AMLA, unless the salary payments are made on an ancillary basis and by means of a limited power of attorney by the person who also manages the payroll accounting. 96

97 Transfers are also not subject to the AMLA if the financial intermediary only has a contractual relationship with the creditor and acts on their behalf, and the assets are not forwarded after **collection** (collection exception).

3. Assistance with the transfer of virtual currencies

98 According to Art. 4 para. 1 lit. b AMLO, a payment service is also provided if the financial intermediary assists in transferring **virtual currencies** to a third party, provided that it has an ongoing business relationship with the contracting party or exercises power of disposal over virtual currencies on behalf of the contracting party, and he does not provide the service exclusively to appropriately supervised financial intermediaries. In addition to these elements, the general requirements of the general clause pursuant to Art. 2 para. 3 AMLA (professional activity and activity in the financial sector) must also be met for the AMLA to apply.

99 Virtual currencies are tokens that are actually or, according to the intention of the organizer or issuer, used as a means of payment for the purchase of goods or services or serve to transfer money and value (Art. 4 para. 1bis lit. c AMLA), i.e. **payment tokens** as defined by FINMA's categorization. The category of payment tokens usually includes stablecoins with a payment function and the cryptocurrencies Bitcoin and Ether. The risk-specific feature of cryptocurrencies compared to other assets lies in the combination of pseudonymity, speed, and mobility.

100 According to FINMA's previous practice, **assistance with transfer** within the meaning of the general clause of Art. 2 para. 3 AMLA is characterized by (1) a power of attorney, whereby even a collective signature is considered sufficient co-determination, and (2) a change in ownership or creditor status. Financial intermediary activity therefore consists of supporting actions that normally result in the transfer of ownership of third-party assets or a change of creditor. However, since transfers in the blockchain sector take place between pseudonymous wallet addresses, it is often not possible to clearly determine the ownership structure. In this context, the term “assistance” should therefore be interpreted to mean that the financial intermediary provides support for the successful transfer of virtual currencies from one blockchain address to another, which makes the transfer much easier.

Assistance with the transfer of virtual currencies can generally be considered in the context of all applications that facilitate the **transfer of** payment tokens to a third party via a blockchain (e.g., by means of a smart contract). Examples of this are crowdfunding platforms and payment service providers that accept and forward virtual currencies. Access providers that provide an interface for accessing third-party applications in Switzerland or abroad can also provide such assistance with transfers. However, simply providing an IT infrastructure for data transmission without making a significant contribution to the actual transfer of assets is often not sufficient to fulfill the criteria. 10 1

Assistance with the transfer of virtual currencies that is subject to supervision requires **alternatively** either power of disposal over the virtual currencies or the existence of a permanent business relationship (without power of disposal). The ongoing business relationship was included as a criterion for subordination (despite criticism from academia) because it is difficult in practice to clarify whether there is legally relevant power of disposal within the framework of a technical solution. This is intended to enable legally secure, risk-based, and practicable subordination decisions without the need for a time-consuming examination of technical circumstances. Particularly where there is a long-term customer relationship and the availability of the service is necessary for the use of the technical solution, the line into financial intermediation is crossed, even though the service provider may not have sole power of disposal. 10 2

The **power of disposal** over virtual currencies can be exercised either directly by means of private keys to sign transactions or indirectly by means of control of administered smart contracts or other software applications (e.g., in off-chain payment applications that trigger a transfer in virtual currencies) to confirm, release, and/or block orders. Direct power of disposal is exercised, for example, by **custodial wallet providers**, who have a private key via multi-signature, which is required to sign the transaction before it can be successfully executed. This also includes **operators of central trading platforms** who hold customer funds in their own accounts or wallets and act as intermediaries between customers in a trilateral relationship. Indirect power of disposal can be exercised in the context of the administration of a smart contract by means of a single or multi-signature or by the members of a DAO (Decentralized Autonomous Organization) exercising control of the so-called admin key by majority vote. 10 3

10 4 A **long-term business relationship** must exist between the financial intermediary and its contracting party on whose behalf the financial intermediary transfers the virtual currencies to a third party. The lack of a definition of a long-term business relationship has led to different interpretations in academic circles. The prevailing opinion requires a certain degree of intervention and control over transactions in order to fulfill this criterion. FINMA interprets the term broadly and applies the criterion in particular in the context of decentralized finance as a criterion for subordination. While a business relationship can already result from an implied service, brokerage, or software usage agreement, the permanence of this business relationship usually lies in the continuous nature of the transfer assistance as a contractual service provided by the financial intermediary, which goes beyond one-time interactions. In this context, even the technical connection of a wallet to a smart contract for the purpose of concluding transactions can establish a business relationship. The peculiarities of blockchain technology have prompted FINMA to develop attribution criteria with regard to a permanent business relationship. Such criteria include, in particular, the maintenance of an interface as the front end of a blockchain application, the generation of fees or control and influence over assets, access (e.g., by means of a whitelisting process) or other aspects of the protocol (e.g., by controlling the majority of governance tokens as part of a DAO's governance process).

10 5 **Durability** may refer to the behavior of the contracting party and be reflected in continuous use through the creation and management of a wallet or account, repeated transaction orders, or ongoing return generation. With regard to the services of the financial intermediary, the permanence of the business relationship may lie, for example, in the regular collection of fees or the performance of regular updates (bug fixes and product enhancements), configurations (parameter adjustments), or other additional services. However, one-time transactions do not generally constitute a permanent business relationship.

10 6 Assistance with the transfer of virtual currencies may, for example, take the form of **non-custodial staking**. In this case, the customer always remains in possession of the private keys that enable them to control the locked assets. The provider generally has only limited power of disposal over the customer's assets, but helps the customer to generate staking rewards by delegating staking rights to the provider (as an indirect instruction) within the framework of

operating a validator node on behalf of the customer as a delegator, which constitutes a permanent business relationship.

Providers who merely provide **software** and the necessary licensing, but not such additional services for triggering or executing payments, should not be subject to the AMLA. On the other hand, services for the secure storage of private keys are covered within the scope of non-custodial wallets, even if the latter (e.g., in the context of smart cards) are encrypted and must generally be decrypted by the customer. The risks involved are fundamentally comparable to those of money transmitters. Actual **non-custodial wallet providers** are therefore subject to the AMLA if, in addition to providing and licensing the software, they also provide additional services (e.g., updates or the connection of third-party service providers for the execution of exchange transactions). 10 7

In contrast, completely **autonomous systems** without a permanent business relationship are excluded from the obligation to comply with the AMLA. Decentralized trading platforms that merely bring buyers and sellers together and process transactions without smart contracts with access to the trading platform are not generally subject to the AMLA. This is purely an intermediary activity without involvement in the transfer of virtual currencies. However, practice shows that such systems are rarely completely autonomous. Instead, such applications often have aspects that make it necessary to attribute them to the developers or operators. 10 8

An **exception** to the obligation to comply applies if the financial intermediary provides transfer assistance exclusively to financial intermediaries that are subject to appropriate supervision (in Switzerland or abroad) (Art. 4 para. 1 lit. b AMLO). A financial intermediary subject to the AMLA is generally considered to be adequately supervised. In the case of foreign financial intermediaries, the decisive factor is whether a level of protection comparable to that provided by the AMLA exists abroad. 10 9

4. Means of payment and payment systems

According to Art. 4 para. 1 lit. c AMLO, a payment service is provided if the financial intermediary issues or manages **means of payment** that are not cash and uses them to make payments to third parties on behalf of its contracting party. This refers to the issuance of means of payment and the operation of a payment system. 11 0

11 1 Art. 4 para. 1bis AMLO specifies **means of payment**, without limitation, as credit cards (lit. a), traveler's checks (lit. b) and (since 2021) virtual currencies that are used as a means of payment for the purchase of goods or services or serve to transfer money and value (lit. c), i.e., payment tokens.

11 2 According to the FINMA circular, the issuance of payment instruments and the operation of payment systems are subject to the AMLA beyond the examples mentioned above whenever a **three-party relationship** exists. The activity is not subject to the AMLA if the issuing entity is also the user of the means of payment within the framework of a two-party relationship, i.e., if it is also the seller of the goods for which the means of payment is used. Vouchers are also not subject to the AMLA as means of payment if they can only be redeemed with the issuing entity. However, it should be noted that if redemption is possible at other group companies, there is no longer a two-party relationship.

11 3 For the question of subordination, it is irrelevant whether the use of payment instruments or systems is restricted to a specific **group of users** (*closed loop* vs. *open loop* system). A professional issuer of payment instruments or operator of payment systems is always a regulated financial intermediary, provided that the business model is not only conducted between two parties.

11 4 The **value** of the payment instrument must be fixed at the time of issue. This also includes, for example, non-rechargeable e-money data carriers. Other examples include debit cards, prepaid cards, mobile payments, and payment tokens. Book money/giro money also falls under this category, but is usually "created" by prudentially supervised institutions, which means that this provision hardly ever applies.

11 5 Since the **money laundering risk** associated with the use of credit cards lies with the cardholder, in situations involving four or more parties (credit card organization, acquirer, issuer, processing company), the party that provides the cardholder with access to the payment system and thus has direct customer contact is subject to the AMLA. If credit cards are issued by national issuers, they are subject to the AMLA.

11 6 For **issuers** of payment instruments, certain thresholds pursuant to Art. 11 and Art. 12 GwV-FINMA apply, which result in a reduction in the AMLA due diligence obligations.

The operation of a **payment system** is also only subject to the AMLA if it is operated by an organization that is not identical with the users of the payment system. This includes systems that either allow access to a credit balance available on the basis of data storage (reloadable e-money data carriers, debit cards) or allow the storage of a debt that is subsequently invoiced by the payment system operator (credit cards, store cards in three-party relationships, etc.). Prepaid cards that can be used for payment not only with the issuer but also with third parties (e.g., Paysafecard or Aplauz) can be used in a three-party relationship and therefore qualify as a means of payment within the meaning of the AMLA. Since the money laundering risk is located on the end customer side, in addition to the issuer of the means of payment, the party that provides the end customer (purchaser of goods, initiator of the payment transaction) with access to the payment system and thus has direct customer contact (known as the "distributor") is also subject to the AMLA. The sale of AMLA payment instruments by distributors can take place either in their own name and on their own account (sales model) or as a direct representative of the issuer or another financial intermediary (brokerage model). In principle, both the sales model and the intermediary model are subject to the AMLA, because both models involve direct customer contact and provide end customers with access to the payment system. In the case of the intermediary model, it should be noted that if the legal requirements for the auxiliary person exemption pursuant to Art. 2 para. 2 lit. b AMLO are met, the distributor may be exempted from independent supervision. Operating a payment system necessarily means that the service provider obtains power of disposal over the assets of its customers who use the payment system to transfer their assets to third parties. Services such as PayPal, Click&Buy, Twint, and Tapit are considered payment systems. 11 7

Payment systems within the meaning of Art. 81 FinMIA, such as SIC (SIX Interbank Clearing) require a **FINMA license** in accordance with Art. 2 para. 2 lit. d^{ter} AMLA in conjunction with Art. 4 para. 2 FinMIA if the functioning of the financial market or the protection of financial market participants so requires and it is not already operated by a bank subject to licensing. While Art. 2 para. 3 lit. b AMLA links qualification as a financial intermediary to payment services, Art. 2 para. 2 lit. d ter AMLA classifies payment systems requiring a license as financial intermediaries under special legislation. 11 8

119 According to FINMA's categorization, payment tokens are considered **virtual currencies**. The category "payment tokens" (synonymous with "cryptocurrencies") includes tokens that are actually or, according to the issuer's intention, accepted as a means of payment for the purchase of goods or services or serve to transfer money and value (Art. 4 para. 1bis lit. c AMLO). Qualification as a payment token may therefore also result from the fact that a means of payment purpose is only intended in the future or that tokens serve as discount points on a platform for the purchase of third-party goods. Even if a token is linked to gold, it may still qualify as a payment token if it has a corresponding denomination and potential use as a means of payment. An ICO of payment tokens constitutes an issue of means of payment subject to supervision as soon as they can be technically transferred on a blockchain infrastructure. This may already be the case at the time of the ICO or later.

120 If only products or services of the token issuer, but not of third parties, can be paid for with the issued tokens, this constitutes a normal **two-party relationship** and the token issuer does not qualify as a financial intermediary within the meaning of Art. 2 para. 3 lit. b AMLA. When issuing payment tokens, the purpose of the means of payment must also be the main function of the token and must not merely be an ancillary service to the usage function or main contractual service (see Art. 2 para. 2 lit. a no. 3 AMLO).

121 If a token is used exclusively for the payment of blockchain-related transaction fees by users to validators, this does not constitute a relevant payment function, provided that the mechanism is technically necessary for the operation of the **blockchain**. In this case, the payment function is merely ancillary to the usage function within the blockchain infrastructure and does not result in the issuance of a payment instrument subject to regulation (provided that the token cannot also be used to pay fees for other functions or services of the blockchain, such as data storage or computing services).

122 The issuance of payment tokens by a **smart contract** that has been programmed and activated by a person is, despite the algorithmic issuance of the tokens, attributable to the area of responsibility of the person who activated the contract in terms of an overall assessment as an issuance of means of payment subject to the AMLA.

123 In the case of an **airdrop**, despite the free issuance, professional activity may be deemed to have been carried out in this context, in particular if the issuer

of a payment token enters into business relationships with more than 20 contracting parties per calendar year in accordance with Art. 7 para. 1 AMLO (lit. b) that are not limited to the one-time activity of issuance, or if the airdrop exceeds a total volume of CHF 2 million (token price x number of tokens issued) per calendar year (lit. d).

If **stablecoins** are issued as a means of payment on an open-access transaction system such as the Ethereum blockchain, particular attention must be paid to the increased risks relating to money laundering, terrorist financing, and sanctions evasion. Due to the openness of the system, once the stablecoin has been issued, the issuer only has the option of exercising control when the underlying value is redeemed. If no appropriate technical measures are taken, the due diligence obligations under money laundering law can only be fulfilled in relation to the first and last persons who have access to the stablecoin. Persons who buy or sell the stablecoin on the open platform in between are beyond the control of the issuing institution. According to FINMA Supervisory Notice 06/2024, all persons holding stablecoins must be adequately identified by the issuing institution or by appropriately supervised financial intermediaries. In order to address the risks and meet money laundering requirements, contractual and/or technological transfer restrictions are necessary when stablecoins are issued by supervised institutions. The technical implementation of the requirements is left to the stablecoin issuers. However, the requirements can be implemented, for example, by means of a whitelisting process or transfer restrictions programmed into the smart contract. 12 4

5. Money or value transfer business

According to Art. 4 para. 1 lit. d AMLO, a payment service is also provided when the financial intermediary carries out a "**money or value transfer business**." According to the legal definition in Art. 4 para. 2 AMLO, this includes the transfer of assets by accepting cash, precious metals, virtual currencies, checks, or other means of payment in combination with a payout of a corresponding sum in cash, precious metals, or virtual currencies (lit. a) or a cashless transfer or remittance via a payment or settlement system (lit. b). FINMA does not comment on this situation in its circular. 12 5

As with electronic transfers (Art. 4 para. 1 lit. a AMLO) and in contrast to currency exchange (Art. 5 para. 1 lit. a AMLO), money or value transfer transactions pursuant to Art. 4 para. 1 lit. d AMLO always involve a **three-party rela-** 12 6

tionship. In addition, the requirements of the general clause pursuant to Art. 2 para. 3 (financial intermediation, activity in the financial sector) must continue to be met. In particular, the financial intermediary must have power of disposal over the assets.

12 7 **Cash** is defined as legally issued means of payment with a fixed exchange rate that are physically issued, i.e., coins issued by the federal government and banknotes issued by the Swiss National Bank (Art. 2 WZG). This also includes all foreign currencies that are in circulation as physical means of payment.

12 8 Precious metals within the meaning of the Precious Metals Control Act (EMKG) are gold, silver, platinum, and palladium (Art. 1 para. 1 EMKG). According to Art. 178 EMKV, bank precious metals are gold bars and granules with a minimum fineness of 995 thousandths (lit. a), bars and granules of silver with a minimum fineness of 999 thousandths (lit. b), and bars and sponges of platinum and palladium with a minimum fineness of 999.5 thousandths (lit. c).

12 9 **Virtual currencies** are crypto-based assets that are actually used or intended by the organizer or issuer to be used as a means of payment for the purchase of goods or services (Art. 4 para. 1bis lit. c GwV). In terms of FINMA's token categorization, this refers to payment tokens.

13 0 **Checks** can be used in payment transactions to transfer money across borders, making them suitable for money laundering. However, payment by check is in sharp decline due to various risks, such as forgery, which also reduces their attractiveness for money laundering.

13 1 Other means of payment include credit or debit cards, prepaid cards, mobile devices such as cell phones with payment functions, e-money, and book money. E-money is any electronically (i.e., also magnetically) stored monetary value in the form of a claim against the issuer, which is issued against payment of a sum of money in order to carry out payment transactions and which is also accepted by natural or legal persons other than the e-money issuer (Art. 2 E-Money Directive). Book money refers to credit balances at commercial banks and at PostFinance that can be converted into cash at any time.

13 2 Even when exchanging virtual currencies such as bitcoins for official currencies (as opposed to currency exchange, which involves a two-party relationship and constitutes a trading activity within the meaning of Art. 5 para. 1 lit. a AMLO), a **three-party relationship** may exist. When using Bitcoin exchange

machines, it is conceivable that a person other than the one from whose wallet the equivalent value in Bitcoins was transferred to the machine withdraws the cash from the machine. Similarly, Bitcoins purchased with cash can also be credited to the wallet of a third party at the machine. It is also possible that cash is deposited at a Bitcoin exchange machine, the equivalent value in Bitcoins is transferred to another machine and credited to the wallet of a third party there. It is also possible that cash is deposited at a Bitcoin exchange machine, the equivalent value in Bitcoins is transferred to another machine, and withdrawn there in cash by a third party. Due to the unavoidable three-party relationship, the execution of such transactions qualifies as a money transmission business. A two-party relationship can only be assumed if technical measures ensure beyond doubt that the customer is also the actual recipient of the equivalent value in cash or bitcoins. The distinction is important insofar as money transmission is considered a professional activity due to the associated increased money laundering risks, unless the activity is carried out for a related person and generates gross proceeds of no more than CHF 50,000 per calendar year (Art. 9 AMLO). In addition, stricter due diligence requirements apply to such transactions.

Money transmitters play the main role in the money and value transfer business, with cash flows in this sector relating predominantly to transfers from Switzerland to other countries, particularly countries without a reliable banking system. In addition to these money transmitters, which operate globally as generalists, there are also other specialized money transfer agencies for specific countries. The funds transferred are primarily intended to support relatives in the countries of origin. Money transmitters thus fulfill a social function, as they are the only way to receive funds transferred from abroad in certain countries. Given its advantages, this sector presents a high risk of money laundering due to the speed and ease with which funds can be transferred abroad and the interruption of the paper trail. Customers mainly transfer cash, the origin and beneficial ownership of which are more difficult to determine, as Switzerland and the recipient country often have different control and detection options. 13 3

Examples of **money or value transfer businesses** include the Hawala network, Western Union, Moneygram, and agents or e-money agents. Agents are generally considered to be auxiliary persons within the meaning of Art. 1 para. 2 lit. b AMLO. In money or value transfer transactions, an auxiliary person 13 4

may only act on behalf of a single licensed financial intermediary or a financial intermediary affiliated with an SRO (Art. 2 para. 2 lit. b no. 5 AMLO), whereas an auxiliary person may act on behalf of several financial intermediaries in all other cases.

13 5 However, pursuant to Art. 2 para. 2 lit. a no. 1 AMLO, purely physical transport is also **excluded** from this provision, which is why some form of electronic transfer must take place. Furthermore, the mere payment for goods or services in virtual currencies, as well as the provision of corresponding services in exchange for payment in bitcoins, does not constitute financial intermediation within the meaning of the AMLA.

D. Trading activity (lit. c)

1. General

13 6 According to Art. 2 para. 3 lit. c AMLA, financial intermediaries are also persons "who **trade in** banknotes and coins, money market instruments, foreign exchange, precious metals, commodities and securities (securities and rights) and their derivatives for their own account or for the account of others."

13 7 According to FINMA Circular 2011/1, this provision only covers trading in **financial instruments**, although the list in lit. c is not intended to be exhaustive according to prevailing opinion and practice. Art. 5 GwV specifies which other instruments are also covered. The Financial Services Act (FIDLEG), which came into force in 2020, provides a narrower definition in Art. 3 lit. a FIDLEG, which, however, applies for the purposes of the FIDLEG (consumer protection) and does not necessarily apply per se to the AMLA (money laundering prevention). FINMA-RS 2011/1 lists banknotes, coins, foreign currency, precious metals, and securities as typical financial instruments in the context of trading activities under Art. 2 para. 3 lit. c AMLA.

13 8 Trading in **emission allowances** does not generally fall under the AMLA. However, it could be classified as a security and, in some cases, as a derivative if, for example, a tokenized emission right conveys a contractual claim to it or if its economic function consists wholly or partly in an investment.

13 9 Trading in **goods**, which also includes art, real estate, and luxury goods, is not a financial intermediary activity and is not covered by the provision. However, transactions carried out in the course of the activities of traders within the

meaning of Art. 2 para. 1 lit. b AMLA may be subject to the AMLA under certain circumstances (see Art. 8a AMLA and Art. 13 ff. AMO).

Trading activities also expressly include, in some cases, **proprietary trading,** i.e. trading in one's own name, with one's own assets, at one's own risk and in one's own interest. The wording of the provision thus goes beyond the basic requirement ("own account"), which is considered contrary to the system in legal doctrine. However, the AMLO restricts this extension in Art. 5 AMLO by stipulating that proprietary trading is only subject to the AMLA for certain financial instruments (circulating coins, banknotes, bank precious metals). 140

2. Trading in banknotes and coins (cash)

According to Art. 5 para. 1 lit. a AMLO, the purchase and sale of **banknotes and coins** on behalf of third parties is subject to supervision. Art. 5 para. 1 lit. b AMLO also covers trading on one's own account with "circulating coins and banknotes at market value." Persons who trade in banknotes and coins on their own account or on behalf of third parties are therefore generally subject to supervision. 141

In its Circular 2011/1, FINMA specifies that for both types of trading activities relevant to the AMLA (own account and third-party account), only **circulating coins and banknotes at market value** may be traded. Circulating coins are coins created for the purposes of payment transactions that are issued and accepted by the state at face value. 142

With regard to **coins**, they are not subject to the Act if they are traded at a premium of more than 5 percent above their face value. This is particularly relevant for coins in circulation with special numismatic characteristics (e.g., with a misprint), commemorative coins and investment coins, medals, and small bars intended for use as jewelry. South African Krugerrand coins are not considered precious metal investment coins due to their low fineness. However, they are legal tender in South Africa, even though they do not have a face value stamped on them. For this reason, professional trading in these coins is subject to reporting requirements based on Art. 5 para. 1 lit. b AMLO. 143

Banknotes in circulation are official legal tender and must be accepted by everyone. They are issued by a state-authorized institution, generally the central bank, and are redeemed at their face value. Banknotes that have been taken out of circulation are excluded.

3. Foreign exchange trading (book money)

14 5 According to Art. 5 para. 1 lit. a AMLO, the purchase and sale of foreign exchange on behalf of third parties is considered a **trading activity** subject to the AMLA. Proprietary trading in this area is not subject to the AMLA. **Foreign exchange** is defined as monetary claims denominated in foreign currencies and payable abroad (e.g., in the form of bank balances, checks, or bills of exchange).

14 6 In practice, there are many different types of financial intermediaries active in the **foreign exchange business**. These can basically be divided into four groups, although Art. 2 para. 3 AMLA is only relevant for the first group (customer foreign exchange dealers):

1. Customer foreign exchange dealers: These "typical" foreign exchange dealers accept customers' money in a collective account held in their name. Customers place trading orders with the foreign exchange dealer (either themselves or through their asset manager). The customer foreign exchange dealer is the counterparty to these transactions, which it then executes via its various currency accounts held in its name. If the customer foreign exchange dealer is not already subject to the Banking Act and thus to Art. 2 para. 2 lit. a AMLA, it is subject to Art. 2 para. 3 lit. c AMLA if it carries out this activity on a professional basis.
2. Foreign exchange asset manager: The foreign exchange asset manager does not carry out foreign exchange trading transactions in its own name, but manages foreign exchange by means of limited power of attorney. Customers have an account in their name with a bank or broker engaged in foreign exchange trading, or with a customer foreign exchange trader.
3. Foreign exchange trading funds: This group also accepts money from investors in a collective account in their name, but does not individualize it for clients. Instead, investors only receive a claim to their proportional share of the capital. As a result, the CISA or FinIA is generally applicable and subordination occurs in accordance with Art. 2 para. 2 AMLA.
4. Intermediaries: The intermediary accepts investors' funds in a collective account held in its name. It does not engage in foreign exchange trading itself, but forwards the funds to a third party's account. The accounts with this third party are in the name of the intermediary – usually with the customer's name as a sub-designation. This generally constitutes an activity

subject to the Banking Act, which means that the intermediary is already subject to Art. 2 para. 2 lit. a AMLA.

4. Trading in bank precious metals (gold, silver, platinum, palladium)

Trading in **bank precious metals** is covered by both Art. 5 para. 1 lit. a AMLO ("purchase and sale on behalf of third parties") and Art. 5 para. 1 lit. e AMLO ("trading on own account"). 147

Precious metals include gold, silver, platinum, and palladium. In addition to the definition in Art. 1 para. 1 of the Precious Metals Control Act (EMKG), the Precious Metals Control Ordinance (EMKV) defines the form and fineness required for a metal to be considered a precious metal. According to Art. 178 EMKV, bank precious metals are defined as gold bars and granules with a minimum fineness of 995 thousandths (lit. a), bars and granules of silver with a minimum fineness of 999 thousandths (lit. b), and bars and sponges of platinum and palladium with a minimum fineness of 999.5 thousandths (lit. c). 148

Trading in **investment coins** made of these materials is subject to regulation if they are traded at a premium of less than 5 percent above their face value. 149

It is irrelevant whether trading takes place through the purchase and sale of bank precious metal or through the purchase of **smelting material**, which the trader has processed into bank precious metal for subsequent sale. If trading takes place via precious metal accounts, the requirement for a banking license (or the possible applicability of the settlement account exemption pursuant to Art. 5 para. 3 lit. c BankV) must be examined. The maintenance of weight accounts is not a criterion for subordination. If precious metal weight accounts are maintained exclusively within the scope of an industrial activity and for accounting purposes, then this is not a subordinate activity. 150

Trading in (unprocessed) melt material, precious metal goods, semi-finished products, plated and substitute goods, as well as direct purchases by manufacturing companies or the sale of bank precious metals to manufacturing companies for the purpose of producing such goods, is **not subject** to regulation. The provisions on goods trading may apply to these forms of trading. 151

The **gold trade** occupies a prominent position in Switzerland. Gold imports into Switzerland are mostly in the form of raw gold (mined gold or red gold), non-monetary gold (gold powder) or gold scrap. Gold refineries located in 152

Switzerland process raw gold or melt down existing gold goods. In contrast to the trade in other valuable materials via Switzerland, gold traded and refined in Switzerland is actually physically delivered via Switzerland. The money laundering risk here lies, on the one hand, in the fact that valuable materials may have been acquired by criminal means (e.g., through corruption, theft, or other criminal offenses). On the other hand, valuable materials can be used directly for money laundering or as a vehicle for financing other criminal offenses. In addition to the requirements of the EMKV, most financial intermediaries in the precious metals business have voluntarily subjected themselves to additional international standards of due diligence. The controls provided for by these standards go beyond the requirements of the AMLA with regard to knowledge and monitoring of business relationships, thereby reducing the susceptibility to money laundering.

15 3 Trading in physical valuables (including precious metals) on the **blockchain** is also considered a regulated trading activity. Trading in tokens linked to bank precious metals may therefore also be subject to Art. 2 para. 3 lit. c AMLA, unless it is already subject to prudential regulation under Art. 2 para. 2 AMLA through the acceptance of public deposits or the formation of a collective investment scheme.

15 4 Furthermore, the purchase and sale of **old gold** (i.e., second-hand gold such as teeth, crowns, or other gold-containing objects, as well as gold waste from manufacturing) does not fall under Art. 2 para. 3 lit. c AMLA. These transactions differ from trading in raw gold or commodities such as gold bars and the individual control measures applicable to them. Since 2009, the volume of old gold sold by private individuals in Switzerland has increased significantly. Sales are mostly made in cash.

5. Currency exchange

15 5 Art. 5 para. 1 lit. a AMLA also classifies **currency exchange** on behalf of third parties as a trading activity.

15 6 Currency exchange is defined as the direct **exchange of** an amount in one currency for the equivalent amount in another currency. In contrast to money transfer business, currency exchange involves a clearly defined two-party relationship, i.e., the purchase and sale are made from the parties' own holdings. Compliance with the two-party relationship is not considered to be unequiv-

ocally guaranteed if, for example, the financial intermediary cannot (technically) ensure that a user of an SBB ticket machine does not transfer Bitcoin to the wallet of a third party.

Money exchange also includes the purchase and sale of virtual currencies (payment tokens) against official currencies ("FIAT") or other virtual currencies. Although these are not "money" in the traditional sense, they fulfill the central characteristics of money. Currency exchange is therefore also carried out by crypto exchange offices and **cryptocurrency traders** acting on behalf of customers. Cryptocurrency trading is not subject to the BankG, but is subject to the AMLA as a currency exchange activity if the payment tokens purchased with pooled funds as part of token purchase orders are always transferred directly to the individualized blockchain addresses of the respective customer, or if the purchased payment tokens within the meaning of Art. 16 no. 1bis lit. a BankG. In the area of decentralized finance, liquidity providers may be considered money changers if they make virtual currencies available as liquidity in a liquidity pool for exchange against other virtual currencies and thereby benefit from a share of the exchange fees generated. 15 7

Payment for goods or services in one currency with change in another currency is not generally subject to the AMLA, as long as the focus is on the purchase of goods or services. If there is an obvious discrepancy between the amount of money paid and the actual price, a **circumventing transaction** is assumed and, in fact, a money exchange activity subject to the AMLA is present. 15 8

If a company conducts currency exchange **accessorily** to its main activity, this is not considered a trading activity under Art. 5 para. 3 AMLO and is therefore not subject to the AMLA. However, currency exchange is no longer considered ancillary if the financial intermediary carries out or is prepared to carry out individual or multiple related currency exchange transactions in excess of CHF 5,000, or if the gross profit from currency exchange exceeds 10 percent of the company's profit per calendar year. 15 9

6. Trading in commodities (on and off the exchange)

Art. 5 para. 1 lit. c. and d AMLO regulate trading in **commodities** on behalf of third parties. A person who carries out transactions in the field of commodity trading is therefore only considered a financial intermediary under Art. 2 para. 16 0

3 lit. c AMLA if they act on behalf of and for the account of a third party. However, if a person conducts a transaction in this area in their own name and at their own risk and then resells the goods, this does not constitute financial intermediation. Proprietary trading is therefore not subject to regulation. However, this only applies to "genuine" proprietary trading, i.e. when the transaction is concluded in the trader's own name, exclusively with their own assets and in their own interest, and at their own risk. However, if the trade is carried out on commission, i.e., in one's own name but on behalf of a third party, it is subject to taxation.

16 1 Commodities are defined as **unprocessed raw materials** that usually originate from mining or agriculture or can be attributed to the energy sector, such as crude oil, natural gas, metals, ores, and coffee. On the other hand, wheat flour, soybean oil, soybean meal, raw sugar, and white sugar are not included, as these are not unprocessed raw materials within the meaning of FINMA Circular 2011/1. Precious stones are not considered commodities due to their lack of association with the financial sector, but are included in the definition of goods.

16 2 A distinction is made between **exchange-traded** (lit. c) and **over-the-counter** (lit. d) trading in commodities, whereby the latter must, according to Art. 5 para. 1 lit. d AMLO, have such a high degree of standardization that they can be liquidated at any time. The possibility of selling at any time should refer to normal market conditions and not to situations in which, for example, there is temporary illiquidity in the market for political or economic reasons. A stock exchange is defined as an institution for the multilateral trading of securities, at which securities are listed and which aims to facilitate the simultaneous exchange of offers between several participants and the conclusion of contracts according to non-discretionary rules (Art. 26 para. 1 lit. b FinMIA). However, securities trading on a stock exchange is only open to regulated participants who are already subject to the AMLA pursuant to Art. 2 para. 2.

16 3 **Commodity derivatives** are generally considered securities and are therefore subject to the exemption provision of Art. 5 para. 2 AMLO. Even in the case of trading in standardized commodity derivatives, trading is therefore only considered a trading activity if a license is required under FinIA.

In this case, the activity is subject to Art. 2 para. 2 AMLA. If the trading activity with commodity derivatives does not fall under FinIA due to a lack of securities quality, it is not subject to AMLA (subject to Art. 6 AMLO).

7. Securities trading

According to Art. 5 para. 2 AMLO, trading in securities is only considered a trading activity subject to the AMLA if it requires a **license** under the FinIA. In these cases, however, trading is already subject to the AMLA under Art. 2 para. 2 lit. d AMLA (lex specialis). If, on the other hand, no authorization is required because, for example, the commercial nature of the activity is not achieved under FinIA, the trading is not considered relevant from an AMLA perspective. It is therefore not covered by Art. 2 para. 3 AMLA in any constellation (neither by the general clause nor by the special provisions), and the provision of Art. 5 para. 2 is thus redundant. 164

Securities are defined as standardized securities suitable for mass trading, rights to securities, in particular simple rights to securities and registered rights to securities, as well as derivatives and book-entry securities (Art. 2 lit. b FinMIA). Securities are considered standardized and suitable for mass trading if they are offered to the public in the same structure and denomination or placed with more than 20 customers, provided that they are not created specifically for individual counterparties (Art. 2 para. 1 FinfraV). The term "securities" also includes units in collective investment schemes. 165

Derivatives qualify as securities if they are standardized and suitable for mass trading (Art. 2 lit. b FinMIA). Standardized precious metal derivatives therefore fall under Art. 5 para. 2 AMLO, and their trading is only covered by the law if it is subject to authorization under FinIA. Derivatives are not standardized if they are tailored to the needs of the individual parties (customized forward contracts and swaps). Derivatives are financial contracts whose price is derived from an underlying asset, namely (lit. a) assets such as shares, bonds, commodities, and precious metals or (lit. b) reference values such as currencies, interest rates, and indices (Art. 2 para. 2 FinfraV), and which do not constitute spot transactions within the meaning of Art. 2 para. 4 FinfraV (Art. 2 lit. c FinMIA). Derivatives typically include a time value and/or leverage component. Financial futures relate to the future delivery of an item and usually have completely standardized terms and conditions, which means that these derivatives are generally considered securities. The term "securities" 166

also includes other standardized derivatives suitable for mass trading, such as exchange-traded derivatives (ETDs), warrants, and structured products, including ETPs (umbrella term for secured exchange-traded commodities (ETCs) or exchange-traded notes (ETNs)).

16 7 In the **blockchain sector**, DLT securities are defined as securities in the form of registered rights (Art. 973d CO) or other rights held in distributed electronic registers which, by means of technical procedures, confer power of disposal over the right on the creditors but not on the debtor (Art. 2 b^{bis} FinMIA). Furthermore, FINMA treats investment tokens as securities if, for example, they represent a book-entry security and the tokens are standardized and suitable for mass trading. Depending on their structure, stablecoins may also qualify as securities. Derivatives offered in standardized form on crypto trading platforms in the form of perpetual futures may also qualify as securities, provided that the product desired by the user can be compiled and automatically priced on the basis of a limited number of predefined variables defined by a limited number of modifiable parameters.

8. Money market instruments

16 8 According to the wording of Art. 2 para. 3 lit. c AMLA, trading in **money market instruments** is also subject to regulation. This provision is not specified in detail either at the ordinance level or in FINMA's practice. This is likely due to the fact that liquidity is traditionally obtained through money market instruments almost exclusively between financial intermediaries, thus posing a low risk of money laundering.

16 9 **Money market instruments** are financial instruments that, due to their maturity of less than twelve months and their issuer and investor base, are attributable to the money market and are intended to raise liquidity. Tradable money market instruments include, in particular: money market book receivables from the federal government, cantons, the National Bank, and large companies; money market (investment) funds; money market derivatives; and domestic and foreign money market securities (such as treasury bills, certificates of deposit, etc.). Money market instruments are generally securities, which means that Art. 5 para. 2 AMLO applies.

E. Making investments as an investment advisor (lit. f)

Art. 2 para. 3 lit. f AMLA subjects investment advisors who make investments on behalf of third parties to the Anti-Money Laundering Act. According to Art. 6 para. 1 lit. b AMO, this refers to the execution of **investment orders** for third parties. In accordance with the materials, FINMA specifies that pure investment advice *e contrario* does not fall under the AMLA, but only cases in which investments are made on the basis of a corresponding power of attorney in individual cases, such as by placing an order with the client's asset manager or custodian bank. Simply forwarding the instructions given by the client (e.g., client order as a PDF document attached to an email from the client) does not constitute a power of attorney. 17 0

An **investment advisor** generally provides the client with personal recommendations regarding investment decisions relating to transactions in financial instruments (Art. 3 lit. c no. 4 FIDLEG). Unlike asset managers, investment advisors do not have power of attorney over their clients' assets. The transaction recommended by the investment advisor is initiated by the client themselves. The client can either conclude the transaction themselves or have it concluded by the investment advisor by means of a special power of attorney for one or more clearly defined transactions. If the investment advisor acts as the client's representative in individual cases on the basis of such an order, there is a risk, according to the dispatch, that the investment advisor's services will be misused for money laundering purposes. For this reason, investment advisors who do not limit themselves to purely advisory activities but also develop investment activities for their clients are subject to the law. 17 1

Regardless of possible AMLA subordination with affiliation to an SRO (or in parallel thereto), investment advisors are required to register in an **advisor register** (Art. 22 para. 2 and Art. 28 para. 1 FINIG). This obligation applies to natural persons who provide investment advisory services themselves or on behalf of a financial service provider (Art. 3 lit. e FIDLEG), but not to client advisors of supervised financial service providers such as banks, where investment advisory services are part of the supervised activity for their clients. 17 2

In contrast to investment advisors, **asset managers** are authorized and also in fact able to dispose of client assets independently (discretionary asset management by means of a power of attorney with the custodian bank). The decisive factors here are the commercial nature of the activity and the fact that it 17 3

is carried out in the name and on behalf of the client. In principle, asset managers do not make payments on behalf of their clients and therefore do not have general power of attorney or power of disposal.

17 4 The application of Art. 2 para. 3 lit. f AMLA is not limited to traditional investment advisory services, but may also apply to operators of **crowd investing platforms** if they make investments based on individual powers of attorney from investors.

F. Custody or management of securities (lit. g)

17 5 Anyone who holds or manages securities on behalf of third parties is subject to the Anti-Money Laundering Act pursuant to Art. 2 para. 3 lit. g. According to the message accompanying the AMLA, the intention was to subject those financial intermediaries who hold or manage assets to the Act. **Securities** were expressly mentioned as the primary example.

17 6 In its practice, FINMA refers to the **definition of securities** under the FinMIA.

17 7 However, Art. 6 para. 1 lit. a AMLO clarifies that administration (unlike custody) includes not only securities but also **financial instruments** as such. Administrative acts also include the collection of interest and dividends, the collection of redeemable securities, and the control of lotteries. Relevant constellations are also conceivable in the context of crowd investing.

17 8 **An administrator** is someone who, within the framework of a mandate relationship, has the power of attorney to dispose of third-party assets freely or within the framework of a predetermined investment strategy. The asset manager is therefore the authorized representative and not the person who ultimately carries out the asset management. The subdelegation of asset management tasks therefore has no influence on the obligation of the person authorized to manage assets to report to the authorities. Custody or management is only covered if the activity in question is carried out on behalf of third parties (Art. 6 para. 1 AMLO). The management of own securities does not fall within the scope of the AMLA.

17 9 Since the entry into force of the FinIA and the associated licensing requirement, asset managers who, due to the different criteria for **commercial activity** in the FinIA (Art. 19 FinIA), but who nevertheless manage investments

for their clients on a professional basis within the meaning of Art. 7 AMLO on the basis of a specific or general power of attorney.

Forms of investment that are not subject to the CISA pursuant to Art. 2 para. 2 CISA are also not covered by Art. 2 para. 3 AMLA. This applies to occupational pension institutions (Art. 2 para. 2 lit. a CISA and Art. 2 para. 4 lit. b AMLA), social insurance institutions and compensation funds (Art. 2 para. 2 lit. b CISA) and public-law corporations and institutions (Art. 2 para. 2 lit. c CISA). This also applies to operating companies that carry out business activities (Art. 2 para. 2 lit. d CISA), provided that these are not of a financial intermediary nature. Holding companies (Art. 2 para. 2 lit. e CISA), associations and foundations (Art. 2 para. 2 lit. g CISA) are also not covered by the AMLA, provided that they do not engage in financial intermediation and do not qualify as domiciliary companies. 180

Investment clubs that are excluded from the scope of the CISA pursuant to Art. 2 para. 2 lit. f CISA are also not subject to the AMLA in accordance with FINMA practice, as they do not manage third-party assets. However, a financial intermediary within the meaning of Art. 2 para. 3 AMLA is defined as a non-member and thus a third party who is commissioned to execute the investment decisions made jointly by the members of an investment club and who, in this context, has power of disposal over the assets of an investment club. 181

Limited Qualified Investor Funds (L-QIFs) in the legal form of an investment company with variable capital (SICAV) or a limited partnership for collective investment schemes (KmGK) are also excluded from the scope of the AMLA if the institution responsible for management pursuant to Art. 118*h* para. 1, 2 or 4 CISA, the institution responsible for management assumes responsibility for fulfilling the obligations contained in this Act (Art. 2 para. 4 lit. e AMLA). 182

On the other hand, **investment companies** that are excluded from the scope of the CISA pursuant to Art. 2 para. 3 CISA fall under Art. 2 para. 3 AMLA. Asset managers of foreign collective investment schemes fall under Art. 2 para. 3 AMLA if the foreign collective investment scheme they manage is not subject to Swiss equivalent supervision within the meaning of the CISA (Art. 2 para. 4 lit. d AMLA). 183

Custody is to be understood as possession within the meaning of Art. 919 of the Swiss Civil Code (CC). The term "custody" refers to a custody business 184

and thus to a deposit agreement in accordance with Art. 472 ff. of the Swiss Code of Obligations (CO) or a similar contractual arrangement. In practice, physical custody of securitized securities is still relevant. However, due to the special legal supervision of professional custodians, Art. 2 para. 3 lit. g AMLA only applies in a few constellations in this area, in particular for lawyers, trustees, and escrow agents.

18 5 According to FINMA practice, the custody of **other assets** such as cash, precious metals, or securities that are not of securities quality (Art. 6 para. 1 lit. c AMLA) does not fall under the AMLA pursuant to Art. 2 para. 2 lit. a no. 1 AMLA. In contrast, some legal scholars consider the inclusion of other assets in the context of financial intermediary custody (e.g., cash or securities that are not securities) to be justified under the general clause of Art. 2 para. 3 AMLA. In our opinion, subordination under Art. 2 para. 3 AMLA should be rejected, especially since Art. 2 para. 2 lit. a no. 1 AMO unequivocally excludes the purely physical storage of assets, with the express exception of securities.

18 6 Nor does the provision of individual, lockable (physical) **safe deposit boxes**, which the contractual partner alone has access to and to which the provider generally has no regular access, result in an obligation to report. In this case, the lessor does not acquire any power of disposal over the third-party assets to be stored.

18 7 Today, securities custody and management for third parties is mostly carried out by professional and regulated **custodians** such as banks, securities firms, or central securities depositories. Securities are generally held as book-entry securities, whereby the securities or global certificates are deposited with the custodian or the book-entry securities are entered in the main register at the custodian and credited to one or more securities accounts (Art. 6 para. 1 BEG). Only prudentially supervised companies can be considered as custodians under the BEG (Art. 4 BEG), which is why they are already covered by Art 2 para. 2 AMLA, meaning that Art. 2 para. 3 AMLA is no longer relevant in these cases.

18 8 A commercial **securities business** exists if accounts are maintained or securities are held directly or indirectly for more than 20 clients (Art. 65 para. 1 FINIV). If securities are held for fewer than 20 clients, the custodian is not subject to authorization and is not covered by Art. 2 para. 2 AMLA. Nevertheless, the threshold of professionalism within the meaning of the AMLA (Art. 7

AMLO) may be reached, namely if the securities have a value of more than CHF 5 million (Art. 7 para. 1 lit. c AMLO), in which case the activity falls under the provision of Art. 2 para. 3 lit. g AMLA.

Securities can also be stored in the **blockchain sector**. Art. 2 para. 3 lit. g AMLA applies to custodial wallets offered for the storage of investment tokens where the custodian has power of disposal over the corresponding private key. This is in contrast to non-custodial wallet providers without power of disposal over the customer's private key, where, as a rule, AMLA subordination pursuant to Art. 2 para. 3 lit. b AMLA in conjunction with 4 para. 1 lit. b AMO comes into question as a result of a permanent business relationship, but not the custody of securities. Analogous to the regulation for wallets, Art. 2 para. 3 lit. g AMLA also covers the offering of an administered smart contract that stores investment tokens and thereby grants the financial intermediary storing them as admin control over these investment tokens by controlling the smart contract (using admin keys). 18 9

According to FINMA practice, the custody of securities by an **employer** is expressly not subject to the AMLA if these are issued as part of employee participation programs and constitute a component of salary; nor is the keeping of a share register or stock register without custody of the securities. 19 0

G. Activity as an organ of domiciliary companies

Under the heading “other activities,” Art. 6 para. 1 lit. d AMLO also subjects the function as an organ of **registered companies** to the AMLA. The provision refers to Art. 2 para. 3 lit. f and g AMLA, but there is no explicit legal basis for this subjection in either lit. f or lit. g. In practice and in doctrine, the general clause of Art. 2 para. 3 AMLA is therefore applied. 19 1

The purpose of subjecting the **organ** of a registered office company to the AMLA is to prevent a company from being used as a front for handling third-party assets in order to circumvent the provisions of money laundering law. 19 2

In principle, the **activities of an organ** are not considered to be financial intermediary activities, as legal entities can only act through their organs and, when deciding on the company's assets, these do not dispose of third-party assets. In the case of domiciliary companies, however, the organ activity is considered a financial intermediary activity if it is carried out on the instructions of the beneficial owner (fiduciary). In this case, the organ persons do not 19 3

manage third-party assets legally, but they do manage them economically. Conversely, and as a consequence of this, the beneficial owner who is himself an organ person is not subject to any obligation to submit.

19 4 Art. 6 para. 1 lit. d AMLO is based on a broad **definition of an organ**, which includes formal, material, and de facto organs. According to this, all persons who make decisions reserved for the organs or who are responsible for the actual management of the company and thus have a decisive influence on the company's decision-making process are considered organs. Collective signing authority is sufficient for this. However, according to doctrine, there is a restriction in the sense that, in the case of Swiss domiciliary companies, only organs with their registered office in Switzerland fall within the geographical scope of Swiss money laundering legislation, unless they operate (frequently) in and from Switzerland.

19 5 The definition of a **domiciled company** for the purposes of the Anti-Money Laundering Ordinance and the corresponding exceptions can also be found in Art. 6 AMLO. Accordingly, domiciliary companies are legal entities, companies, institutions, foundations, trusts, fiduciary companies, and similar associations that do not engage in any commercial, manufacturing, or other business conducted in a commercial manner (Art. 6 para. 2 AMLO). As a rule, these are so-called "financial vehicles" that serve solely to manage the assets of the beneficial owner and to generate income or capital gains. Whether the assets held by the company and managed by its organs are attributable to the financial market or consist of real estate, luxury goods, etc. is irrelevant in this context.

19 6 Whether a company is a domiciliary company or an **operating company** must always be clarified on a case-by-case basis. Indicative evidence is used to assess whether the main purpose of a company is to manage the assets of the beneficial owner or to engage in business activities. If, for example, a securities portfolio or other asset represents the dominant balance sheet item of a company and, at the same time, the income statement shows predominantly income or capital gains from the assets reported in the balance sheet, this strongly indicates that the company is a domiciliary company. Further indications of the existence of a domiciliary company include, in particular, the lack of its own business premises, as is the case with a c/o address, a registered office at a lawyer's, a trustee's or a bank's, or the lack of its own staff. In principle, therefore, the same considerations must be applied as those used in the

practice developed by the SDC for determining the beneficial owner of domiciliary companies. In cases where there are indications of both an operating company and a domiciliary company, the dominant indications that determine the main purpose of the company must be determined in the overall context.

An **investment company** may be exempt from the scope of application of the CISA pursuant to Art. 2 para. 3 CISA, but in this case it falls within the scope of application of Art. 2 para. 3 AMLA. This applies to investment companies in the form of stock corporations, provided that they are listed on a Swiss stock exchange or that only qualified shareholders within the meaning of Art. 10 para. 3 or 3 ter CISA are permitted to hold shares and the shares are registered. If the administration is outsourced, it is questionable whether the company is to be regarded as a domiciliary company on the basis of this outsourced administration and whether its organs are therefore subject to the AMLA. The purpose of the company is decisive in distinguishing between an investment company subject to the AMLA (within the meaning of Art. 2 para. 3 CISA) and a real estate domiciliary company. If the purpose of the company is to invest in real estate and offer these investment opportunities to its clients, it constitutes an investment company (at least from the perspective of the AMLA). If, on the other hand, the purpose of the company is to hold real estate in trust for third parties, it is to be assumed that it is a registered office company. Thus, an investment company that meets the criteria of Art. 2 para. 3 CISA will never qualify as a registered office company within the meaning of the AMLA at the same time. 197

Whether the protector of a **trust** is subject to the AMLA depends on its powers. If it can dispose of the assets held by the trust like a trustee and make arrangements that directly affect the trust assets, it is considered a financial intermediary. The power to replace the trustee is not sufficient for subordination. 198

An **exception** to this requirement is defined in Art. 6 para. 3 lit. a AMLO for companies which "aim to protect the interests of their members or beneficiaries through mutual self-help or pursue political, religious, scientific, artistic, charitable, social or similar purposes." According to FINMA practice, this also includes family foundations under Swiss law and operating companies in liquidation. As a rule, these companies are non-profit associations which, due to 199

their lack of profit orientation, usually do not reach the threshold of professionalism required for subordination under the AMLA anyway.

200 More relevant in practice is the exception in Art. 6 para. 3 lit. b AMLO, which also exempts "genuine" **holding companies** from supervision. This covers companies that hold a majority stake in one or more operating companies and whose purpose is not primarily the management of third-party assets. According to FINMA practice, the holding company must actually exercise its management and control powers (known as the management principle). FINMA's practice of only subjecting the governing bodies of subsidiaries to the AMLA when qualifying subsidiaries of the holding company as domiciliary companies is viewed critically in academic circles. Based on the wording of the ordinance provision, such a holding company would not be covered by the exemption, i.e., its governing bodies would also have to be subject to supervision.

H. Insurance intermediaries

201 If a **tied insurance intermediary** (including an agent) is contractually bound to an insurer by an employment contract, they are subject to the regulations applicable to the insurance company. If this insurance company is subject to Art. 2 para. 2 lit. c AMLA because it operates direct life insurance or shares in a collective investment scheme, or Art. 2 para. 3 lit. a AMLA because it offers mortgage loans, the intermediary is also already covered by its subordination and does not have to register as a financial intermediary itself. This applies, for example, to main and general agencies.

202 According to FINMA practice, **unaffiliated intermediary activities** (as a broker or agent) are not subject to the AMLA. An obligation to comply with the AMLA only arises if, in addition to the intermediary activity, an activity subject to Art. 2 para. 3 AMLA is carried out, for example, if the insurance intermediary accepts funds on behalf of a customer (as debtor) and forwards them in accordance with instructions, thereby providing a payment transaction service. However, there is no obligation to comply if the activity consists of **collecting** a due debt.

203 In principle, all transfers and forwarding of funds carried out **on behalf of the debtor** of the service are subject to the AMLA, regardless of whether the debtor compensates the service provider before or after the service provider

has been remunerated by the third party. In insurance brokerage, there are contractual relationships with the insurance company on the one hand and with the insured on the other. The actual **principal of the transfer** must be determined on the basis of circumstantial evidence, with compensation typically being paid by the principal. Civil law relationships are primarily decisive.

In practice, there are cases in which independent insurance intermediaries broker insurance (in particular reinsurance) for clients (as insured persons) on their behalf and also forward the insurance premiums from the insured person to the insurance company. The order to **collect premiums** may come from either side. Although contractual relationships exist in both directions, the insured person is primarily the customer of the independent insurance intermediary, as the intermediary service is provided for the insured person. For this reason, the contractual relationship between the insurance intermediary and the customer as the premium debtor is the main focus. Insurance intermediaries often act as paying agents in Switzerland for foreign insurance companies. A power of attorney from the insurance company does not mean that the contractual relationships between the intermediary and the insurance company take precedence. Therefore, **independent insurance intermediaries** are subject to the AMLA when collecting premiums. Indications that the insured person is considered the actual principal include the broker's negotiation of the contract on behalf of the insured person, the broker's fiduciary relationship with the insured person (Art. 40 para. 2 ISA), and the broker's compensation by the insured person. The insured person also compensates the intermediary if the brokerage fee and other services provided are already included in the insurance premium and are deducted as a percentage when the premium is forwarded, meaning that the insured person also indirectly pays for the forwarding of the insurance premium to the insurance company. From an economic perspective, the intermediary executes payment orders to the insurance company in return for a fee. 20 4

Premium collection is only considered non-regulated **collection** within the meaning of Art. 2 para. 2 lit. a no. 2 AMLO if there is a due claim between the insurance company and the insured person and the independent broker is primarily commissioned by the insurance company (as the creditor) to collect this claim. The forwarding of **claims payments** to the insured person is clearly to be classified as collection within the meaning of Art. 2 para. 2 lit. a 20 5

no. 2 AMLO, as the insurance company is the client commissioning the forwarding of the claims payments.

206 On January 1, 2024, the revised Insurance Supervision Act (ISA) and the revised Supervision Ordinance (SOS) came into force. Since then, independent insurance intermediaries have been required to **register** with FINMA (Art. 41 para. 1 ISA).

I. Attorneys and notaries

207 If **attorneys or notaries** engage in financial intermediary activities, they are also subject to the Anti-Money Laundering Act.

208 However, due to professional secrecy within the meaning of Art. 321 of the SCC (SCC), the following distinction must be observed for these professional groups: According to FINMA practice, activities covered by **attorney-client privilege** do not lead to an obligation to register. However, attorney-client privilege does not protect all activities, but only those specific to the profession in which the legal element outweighs the commercial element. According to FINMA practice, activities that are usually performed by banks, asset managers, or trust companies (in particular the investment of funds) are therefore not covered by attorney-client privilege. These activities are also referred to as ancillary activities of a lawyer or notary. Thus, short-term investments in connection with court cost advances, payments of public law fees, or in connection with the execution of a will or divorce are covered by attorney-client privilege and do not lead to subordination under the AMLA.

209 A lawyer or notary acting as an **escrow agent** is subject to the AMLA if the execution of the *escrow agreement* involves the power of disposal over third-party assets and their legal expertise is not required for the execution, which can generally be assumed if the *escrow* activity is not related to a specific legal mandate. Nevertheless, the specific individual case must always be taken into account; the decision is the responsibility of the lawyer.

210 In the case of **company formations**, the lawyer is (currently) not subject to the AMLA if he or she limits himself or herself to providing advice, drafting contracts, mediating between persons to ensure management, and carrying out the formation without intervening in the necessary payment transactions or holding securities. However, according to FINMA practice, the transfer of

the formation capital by the lawyer to the bank already constitutes a service subject to payment transactions.

However, the transfer of the **purchase price** (including the directly related payment of mortgage debts, brokerage commissions, or taxes) in the context of a real estate sale via the client account of the certifying notary does not constitute an activity subject to supervision, as it is closely related to his or her professional activities. The same applies if the notary redeems mortgage debts from the purchase price or pays government levies or taxes from the real estate transaction from funds transferred to him by one of the contracting parties. The transfer of a brokerage commission to a third party does not constitute a financial intermediary activity subject to supervision either, because this service is related to the notary's professional activities. However, only payments to third parties that are necessary for the smooth handling of the real estate transfer are considered to be specific to the profession. 21 1

The partial revision of the AMLA extends the scope of the law. Certain **consulting services** with an increased risk of money laundering are now explicitly covered by the AMLA. The corresponding amendment to the AMLO specifies the activities covered and defines supplementary supervisory rules. According to Art. 2 para. 3bis E-AMLA, natural and legal persons who professionally assist third parties in **financial transactions**, including the procurement of funds in connection with the following specific legal transactions, are considered **consultants subject to supervision** pursuant to Art. 2 para. 1 lit. c E-AMLA: (a.) Purchase and sale of real estate; (b.) the formation and establishment of non-operational legal entities based in Switzerland or legal entities based abroad; (c.) the management and administration of non-operational legal entities; (d.) deposits and distributions by non-operational legal entities; (e.) the purchase and sale of legal entities, provided that the purchase or sale is carried out by a non-operational legal entity. This also includes natural persons and legal entities who, on a professional basis, provide addresses or premises as a domicile or registered office for legal entities for a period of more than six months (Art. 2 para. 3ter AMLA) as well as public officials in a public-law employment relationship who, in this capacity, assist third parties in financial transactions, including the procurement of funds in connection with specific legal transactions in accordance with para. 3bis lit. a–e (Art. 2 para. 3^{quater} AMLA). 21 2

21 3 **Excluded from the scope of the AMLA are** lawyers and notaries who perform activities in connection with court, criminal, administrative, or arbitration proceedings, including representation in proceedings and advising in connection with the preparation and conduct of proceedings, the clarification of facts, assessing litigation risks, preventing such proceedings and enforcing the results of proceedings (Art. 2 para. 4 E-AMLA), as well as natural persons and legal entities licensed or supervised by the Federal Audit Oversight Authority for their auditing and inspection activities (Art. 2 para. 4bis E-AMLA).

21 4 In view of the **low risk of money laundering and terrorist financing**, the following are excluded from the scope of the AMLA pursuant to Art. 2 para. 4ter E-AMLA: (a.) Transactions relating to real estate and legal entities as a result of family, matrimonial, and matrimonial property law, inheritance law, or gifts, or in which related persons as defined in Art. 2 para. 2 lit. a FinIA are involved; (b.) transfers of real estate and legal entities with a value of less than five million Swiss francs, provided that the purchase price is paid and received exclusively through banks or other financial intermediaries subject to the law; (c.) Purchase of owner-occupied residential properties in Switzerland or purchase of residential properties in Switzerland that serve as replacement properties within the meaning of Art. 12 para. 3 lit. e of the Tax Harmonization Act of December 14, 1990; (d.) Transfer of agricultural businesses or land in accordance with the Federal Act of October 4, 1991, on rural land law to persons who wish to farm them themselves; (e.) Transfer of real estate for the purpose of land consolidation and similar transactions; (f.) Corporate activities for operational legal entities as well as for charitable foundations and operational associations based in Switzerland; (g.) Establishment of foundations upon death; and (h.) Pure notarization without ancillary consulting activities. The Federal Council may provide for further exceptions to Art. 2 para. ^{3bis} and para. ^{3ter} by means of an ordinance (Art. 2 para. 5 E-AMLA).

J. Real estate sector

21 5 The **real estate sector** is not (yet) subject to the Anti-Money Laundering Act in Switzerland, which is criticized due to the "medium-high" risk of money laundering (large amounts, frequent cash transactions, easy under- or over-invoicing due to different valuations, attractive long-term investment, money laundering through fictitious rental agreements, etc.).

Despite the fundamental non-subjection, **special features** must be taken into account in the real estate sector in the following constellations: 216

In **property management**, collection activities are usually carried out in the name, on behalf, and for the account of the property owner (for rent, etc.), which are not subject to the AMLA. If the property manager uses the income received on behalf of the owner (or funds received directly from the owner) to make payments to third parties, these are also not subject to the AMLA if they are directly related to normal property management (e.g., interest and amortization payments on mortgage loans, bills for ongoing expenses such as water, electricity, insurance, gardening, etc.). Outside of these administrative activities, the receipt and transfer of money is subject to the AMLA. This practice applies to the management of condominiums according to the same criteria. 217

If a property is only held by a company and not managed in the above sense, it is classified as a **registered office company** due to its lack of operational activity, and its organs are subject to the AMLA. 218

Pure **brokerage** (brokerage activity) is not subject to the AMLA. Neither is real estate trading on one's own account. However, if the real estate agent transmits the purchase price to the seller on behalf of the buyer, this is considered a professional activity and is subject to the general clause of Art. 2 para. 3 AMLA. If the real estate agent acts on behalf of the seller and is remunerated by the seller, this is considered a collection activity and is not subject to the AMLA. According to Nagel, the same rules also apply to rental agents and corresponding online platforms. 219

Asset transactions carried out in the context of construction are also not generally subject to the AMLA. For example, general contractors who accept payments from the client as a price for work and pass them on to their subcontractors do not have any third-party money. Payment instructions from architects or engineers in the context of construction management are classified as ancillary. However, if the client appoints a construction trustee to handle payment transactions and pay construction invoices, the latter is classified as a financial intermediary, as they are acting on behalf of the debtor. 220

V. GENERAL CLAUSE

A. Structure

22 1 Art. 2 para. 3 AMLA first contains a **general clause** with an abstract definition. According to this, persons who professionally accept or hold third-party assets (alternatively) or help to invest or transfer them are considered financial intermediaries. The terms "asset," "third-party," and "accepting, holding, and assisting in the investment and transfer" must therefore first be defined. It should be noted at the outset that the term "third-party assets" continues to be of great importance, while the activities described in the general clause rarely serve as catch-all provisions in themselves.

B. Third-party assets

22 2 The term "assets" was not defined in the Money Laundering Act. Since it was taken from the wording of Art. 305ter para. 1 SCC and this provision, like the money laundering provision (Art. 305bis SCC), is based on a very **broad definition**, no restriction is to be recognized in the present case either.

22 3 The literature **expressly** mentions monetary claims arising from account management or financing transactions or payment transactions that are relevant in practice, as well as more traditional forms such as banknotes, precious metals, coins, securities, rights, checks, and newer forms of assets such as cryptocurrencies and other types of tokens.

22 4 However, the Money Laundering Act is intended to regulate the **financial sector**, which at least allows the term "assets" to be restricted to those with a corresponding connection to this sector. However, it is not so much the type of asset that matters, but rather the service associated with it. The activities listed in the catalog in Art. 2 para. 3 lit. a-g AMLA can be clearly assigned to the financial sector. This catalog forms the starting point for interpreting the general clause. Activities that are comparable or very similar to the activities expressly mentioned in the list must be examined on a case-by-case basis and, if necessary, made subject to the law via the general clause. The only undisputed distinction is that an item or right must have economic value at present or in the future, otherwise it is not relevant to the financial sector (example: counterfeit money).

The question of the **foreign nature** of the assets is both a legal and an economic one. Firstly, the financial intermediary must not have any claim to the assets. They must not be the owner of the item or the creditor of the claim. And even if, for example, in the case of an executive position in a domiciliary company, the mixing of cash or the fiduciary holding of shares, the assets under management are not third-party assets from a purely legal point of view, they must still be third-party assets from an economic point of view. In other words, only assets that are legally and economically owned by the intermediary are not covered by the general clause of Art. 2 para. 3 AMLA. It should be noted that even this basic rule is partially broken in the special cases under Art. 2 para. 3 lit. a-g AMLA, but only if these special cases are otherwise fulfilled. 225

C. Financial intermediary activity

Acceptance refers to the conscious granting and acceptance of power of disposal over third-party assets. This means that the disposer wishes to grant power of disposal and the acceptor expressly or tacitly accepts this. Neither the materials nor the prevailing doctrine provide any examples of application. It can be assumed that this activity is rarely relevant in its own right in today's practice and that acceptance alone does not constitute financial intermediation. However, this may be initiated if the person concerned is active in the financial sector, as acceptance often takes place with a view to the safekeeping, investment, or transfer of third-party assets. 226

A modern application of the offense of acceptance in the blockchain sector is the custodial staking of virtual currencies. In this case, the staking service provider accepts virtual currencies from customers, locks them at a staking address, and receives staking rewards for the operation of a validator node of a proof-of-stake blockchain, either carried out by itself or delegated. Assumption pursuant to Art. 2 para. 3 AMLA applies if the virtual currencies received are stored on individual blockchain addresses and there is a contractual obligation to keep them available at all times. If, on the other hand, the virtual currencies received are held in collective custody or are not kept available at all times, the staking service requires a banking license, and the financial intermediary is subject to Art. 2 para. 2 lit. a AMLA. 227

The concept of **custody** of third-party assets is of rather limited relevance, as the forms of custody that are significant in practice today are already regulat- 228

ed elsewhere. For example, the physical custody of assets is expressly excluded from the concept of financial intermediation (Art. 2 para. 2 lit. a no. 1 AMLO). This applies to the physical safekeeping of money at least if it is kept separately and not mixed with that of the custodian. If the money is mixed with the custodian's money, the custodian acquires ownership of the money and it is no longer a case of pure safekeeping. The rental of safes and other containers to which only the user has access is not considered storage at all due to the lack of power of disposal. The storage of securities, which is important in practice, is covered by a special provision (lit. g). Accordingly, the general clause generally only covers cases of application of the deposit agreement pursuant to Art. 472 para. 1 of the Swiss Civil Code (CC) that relate to the financial sector and are not already regulated elsewhere.

22 9 However, safekeeping does occur in the blockchain sector in the context of **custodial wallet services**. If the custodian/depositary holds payment tokens individually assigned to customers under a contractual obligation to keep them available at all times, it is exempt from the banking law licensing requirement with regard to the provision of custody services for these crypto-based assets (Art. 1*b* para. 1 lit. a BankG in conjunction with Art. 5*a* para. 1 BankV *e contrario*). However, the custodial wallet provider with sole power of disposal qualifies as a financial intermediary within the meaning of Art. 2 para. 3 AMLA,

whilst in the case of shared power of disposal by means of multi-signature, it provides assistance in transferring the virtual currencies to a third party within the meaning of Art. 2 para. 3 lit. b AMLA in conjunction with Art. 4 para. 1 lit. b AMLO.

23 0 **Assistance with the investment** of third-party assets is provided in the case of a power of attorney or another form of (even limited) power of disposal. The offence therefore also covers cases in which the financial intermediary has the possibility of indirectly issuing instructions regarding assets via third parties. In this case, a one-time granting of a special power of attorney is sufficient if the professional requirement is met. The possibility of co-determination is sufficient for the requirement to apply. The type of assistance is irrelevant. The line is drawn at pure investment advice, which, in the absence of power of disposal, is expressly not subject to the Anti-Money Laundering Act as long as the advisor does not make any investments himself.

With regard to **assistance with transfer**, it is also required that there be some form of power of disposal over the third-party assets. As a rule, this involves assistance with the transfer of ownership or a change of creditor. Assistance with the transfer of third-party assets differs from assistance with investment in that the transfer changes the ownership structure. Here, too, purely physical transfer in the sense of mere transport is again excluded by Art. 2 para. 2 lit. a no. 1 AMLO due to the lack of power of disposal. This fourth description of activities is also of little practical significance, as assistance with the transfer of third-party assets will generally fulfill the special conditions of Art. 2 para. 3 lit. b AMLA (services for payment transactions). 23 1

A comprehensive assessment of the financial intermediary activity can be made if various **group companies** within a group or individuals, regardless of the existence of a formal group, make a significant contribution to fulfilling the criteria of Art. 2 para. 3 AMLA in an overall plan. According to Federal Supreme Court case law, it should not be possible to circumvent the licensing requirement and financial market supervision by individual companies or the persons behind them not fulfilling all the requirements for an activity to be subject to supervision on their own, but nevertheless carrying out such an activity jointly. Such a uniform (economic) approach is applied if there are close economic (or financial/business), organizational, and personnel links between the individual persons and/or companies and if, reasonably, only an overall assessment does justice to the factual circumstances and the objectives of financial market supervision. Group action may be deemed to exist in particular if the parties involved present themselves to the outside world as a single entity or if, due to the circumstances (blurring of the legal and accounting boundaries between the parties involved; de facto identical place of business; economically unjustified, intertwined shareholdings; intermediary trust structures) it can be assumed that – explicitly or tacitly, based on a division of labor and specific objectives – a *coordinated*, joint activity is being carried out in the regulatory sense. 23 2

VI. PROFESSIONALISM

A. Fundamentals

In the non-banking sector, the AMLA applies exclusively to financial intermediaries who carry out their activities "**professionally**." The AMLA does not 23 3

apply to those who carry out financial intermediary activities only occasionally. It is irrelevant whether this is a main activity or merely a lucrative sideline. By limiting the scope of application of Art. 2 para. 3 AMLA to the professional provision of financial services, the legislative process took into account the principle of proportionality under Art. 5 para. 2 FC.

23 4 In addition to the general criteria for the existence of professional activity under Art. 7 AMLO, which apply both to the general clause and to certain catalogued cases, the Ordinance provides for **special provisions** for credit transactions in Art. 8 AMLO, for money or value transfer transactions in Art. 9 AMLO, and for trading activities in Art. 10 AMLO.

23 5 If a person **switches** from a non-professional **to a professional activity**, the rules of Art. 11 AMLO apply.

B. General criteria (Art. 7 AMLO)

23 6 A financial intermediary always carries out its main or secondary activity on a professional basis if *alternatively* one of the following quantitative **criteria** is met:

- **Gross proceeds** of more than CHF 50,000 (lit. a): This provision is intended to prevent, for example, asset management for relatives from becoming subject to the Act. According to FINMA practice, gross proceeds consist of all income generated by activities subject to the Act – without deduction of any reductions in proceeds. The reason for the income is irrelevant. If a financial intermediary provides services that are subject to the AMLA and services that are not subject to the AMLA, only the income from the activity subject to the AMLA is relevant. This requires a clear and clean accounting separation between income from activities subject to the AMLA and activities not subject to the AMLA. If FINMA is unable to determine the distribution of income from the two activities with reasonable effort, it will base its assessment of professionalism on the total income from all business activities. The financial intermediary must charge the subject activities at rates that correspond to its actual expenses and usual prices.
- **Business relationships** with more than 20 contracting parties for the relevant activity per calendar year that are not limited to a one-off activity (lit. b): However, it is sufficient if 20 business relationships are established in a calendar year, even if they are terminated again in the same year. If a fi-

nancial intermediary that acts on behalf of financial intermediaries pursuant to Art. 2 para. 2 AMLA and is therefore subject to the exception in Art. 2 para. 4 lit. d AMLA has more than 20 other contracting parties within the scope of Art. 2 para. 3 AMLA, it is subject to the AMLA for all of its activities. In this case, only customer relationships with contractual partners are relevant for assessing whether the activity is carried out on a professional basis. Traditional cash transactions are not counted.

- **Unlimited power of disposal** over third-party assets exceeding CHF 5 million at any given time (lit. c): In the case of an executive function in a domiciliary company, the balance sheet assets are used as "assets under management" to determine the extent of the third-party assets.
- **Transactions** whose total volume exceeds CHF 2 million per calendar year (lit. d): According to Art. 7 para. 2 AMLO, inflows of assets and reallocations within the same custody account are not to be taken into account when calculating the transaction volume, and in the case of mutually binding contracts, only the performance provided by the counterparty is to be taken into account. According to FINMA practice, a transaction is generally understood to mean any form of conversion or transfer of assets. Furthermore, the execution of a single isolated transaction is not considered a professional activity, even if it exceeds CHF 2 million. According to FINMA, professional activity is assumed from the second transaction onwards if the total volume exceeds CHF 2 million.

Activities for **third parties** that are not subject to the AMLA pursuant to Art. 2 para. 4 AMLA (Swiss National Bank, tax-exempt occupational pension institutions, certain other financial intermediaries, and selected types of funds) are not taken into account when assessing professional activity (Art. 7 para. 3 AMLO). 23 7

Pursuant to Art. 7 para. 4 AMLO, financial intermediary activities for **related persons** are only taken into account for the assessment of professional activity if they generate gross proceeds of more than CHF 50,000 in the calendar year. According to Art. 7 para. 5 AMLO, related persons are defined as direct relatives and relatives by marriage in the direct line, and relatives up to the third degree in the collateral line. In addition to spouses, registered partnerships and long-term cohabiting couples, as well as co-heirs until the division of the estate, reversionary heirs and reversionary legatees, are also covered by the exception. 23 8

239 The **threshold values** for commercial or professional activity – and consequently for the requirement to obtain a license – for asset managers and trustees are essentially based on the provisions of Art. 7 AMLO. However, a significant difference is that the criterion of a transaction volume of CHF 2 million per calendar year from the AMLO is not provided for in Art. 19 para. 1 FINIV. There are also differences in the exceptions (see Art. 4 FinIA), which may result in an asset manager or trustee not falling within the scope of the FinIA (and thus Art. 2 para. 2 AMLA), but being subject to the AMLA as an other financial intermediary under Art. 2 para. 3 AMLA.

240 The thresholds for professional activity can also be reached by means of **group formation**, which requires a group assessment. In such a case, the individual contributions (e.g., the number of client relationships and gross revenues) of the group members must be added together within the framework of a criterion of Art. 7 AMLO to determine professional activity. A group assessment means that the regulatory consequences (in particular the obligation to join an SRO in accordance with Art. 14 para. 1 AMLA) apply to all group members, even if not all of the criteria are met when considering individual members in isolation.

C. Credit business (Art. 8 AMO)

241 Professional activity is defined individually for **credit transactions**. According to Art. 8 para. 1 AMLO, such transactions are only considered to be carried out on a professional basis if they generate gross proceeds of more than CHF 250,000 in a calendar year and (cumulatively) a credit volume of more than CHF 5 million is granted at any given time. Gross proceeds are defined as all income from credit transactions less the portion used to repay the credit (Art. 8 para. 2 AMLO). If a person engages in both credit transactions and another activity that qualifies them as a financial intermediary, the professional nature of both activities must be determined separately. If professional activity is established in one area, the activity in both areas is considered professional (Art. 8 para. 3 AMLO).

242 FINMA Circular 2011/1 clarifies this provision with reference to **leasing contracts**: the total volume of all installments payable under the contract is relevant. Professional activity in the leasing business therefore exists if the total value of all leasing contracts exceeds the threshold of CHF 5 million, with each leasing contract being recorded at the total volume of all installments to

be paid, and if the proceeds from the interest portion of the leasing installment exceed CHF 250,000.

D. Money and value transfer business (Art. 9 AMLO)

According to Art. 9 AMLO, money or value transfer business is always considered professional and is therefore subject to the AMLA regardless of whether a threshold value is reached. A threshold of CHF 50,000 gross proceeds only applies if the activity is carried out for a related person within the meaning of Art. 7 para. 5 AMLO. 24 3

E. Trading business (Art. 10 AMLO)

According to Art. 10 AMLO, for the purpose of assessing the professional nature of **trading activities**, the criterion within the meaning of Art. 7 para. 1 lit. a AMLO is based on gross profit rather than gross proceeds/gross turnover. 24 4

According to FINMA practice, this applies to **trading companies** that use the gross method to prepare their income statements. 24 5

VII. CONSEQUENCES OF THE OBLIGATION TO COMPLY

A. SRO affiliation

Persons who carry out a professional activity in accordance with Art. 2 para. 3 AMLA are subject to the AMLA and must join a **self-regulatory organization** (SRO) in accordance with Art. 14 para. 1 AMLA. The SROs specify the due diligence obligations under the AMLA for their affiliated financial intermediaries in a set of regulations and monitor compliance with these obligations. The SROs are themselves subject to supervision by FINMA, which approves and monitors them. FINMA bases its decisions on the parameters set out in the GwV-FINMA when approving SRO regulations in accordance with Art. 25 AMLA and recognizing SRO regulations as minimum standards in accordance with Art. 17 AMLA (Art. 1 para. 2 AMLA-FINMA). The self-regulatory organizations can therefore limit themselves to regulating deviations from the GwV-FINMA. In any case, however, the deviations must be indicated (Art. 1 para. 3 GwV-FIMA). Currently, 11 SROs are recognized by FINMA. 24 6

A financial intermediary is generally **entitled to** join an SRO if it meets the requirements of Art. 14 para. 2 AMLA. However, according to Art. 14 para. 3 24 7

AMLA, individual SROs are free to supervise only certain industries and areas of activity (e.g., lawyers, leasing companies, insurance companies, etc.). There are currently several SROs in Switzerland that accept all types of financial intermediaries as members. Without such affiliation, the financial intermediary is engaging in an unauthorized activity within the scope of the AMLA, which has supervisory and criminal law consequences.

248 According to Art. 11 para. 1 AMLO, a financial intermediary within the meaning of Art. 2 para. 3 AMLA must, upon **changing** from a non-professional to a professional activity, immediately comply with the due diligence, reporting, and organizational obligations within the meaning of Art. 3-11 AMLA (lit. a) and submit an application for membership to an SRO within two months (lit. b). Until a decision on membership has been made, such a financial intermediary is prohibited from taking any action that goes beyond what is strictly necessary to preserve the assets (Art. 11 para. 2 AMLO).

249 Art. 12 AMLO stipulates that a financial intermediary who withdraws from an SRO or is excluded from one and wishes to continue to operate as a financial intermediary on a professional basis must submit an application for membership to another SRO within two months of **withdrawal** or of the legally binding **exclusion** (para. 1). Until a decision on the application has been made, the financial intermediary may only continue to carry out its activities within the scope of existing business relationships (para. 2). If the financial intermediary has not submitted an application to SROs within the prescribed period or if its application for membership is rejected, it is prohibited from continuing to operate as a financial intermediary (para. 3).

250 If the financial intermediary has been excluded from an SRO for violating supervisory provisions, FINMA may prevent it from continuing its activities by ordering supervisory measures; in extreme cases, the financial intermediary may be liquidated in accordance with Art. 20 AMLA in conjunction with Art 37 FINMASA. If a company to be liquidated is a financial intermediary, it remains subject to the AMLA for as long as the company **in liquidation** continues to maintain business relationships that are subject to the AMLA on a professional basis.

B. Supervisory and criminal consequences of non-compliance

Pursuant to Art. 2 para. 3, supervision of compliance with the obligations under Chapter 2 of the AMLA for financial intermediaries is the responsibility of the recognized SROs (Art. 24 AMLA), which in turn are supervised by FINMA (Art. 18 para. 1 lit. b AMLA). If a person who is not subject to Art. 2 para. 2 of (indirect or direct) supervision of FINMA, without being affiliated with an SRO, within the scope of the AMLA within the meaning of Art. 2 para. 3 AMLA, FINMA may, pursuant to Art. 20 para. 1 AMLA, apply the **supervisory instruments** pursuant to Art. 29-37 FINMASA analogously to these persons as well. Pursuant to Art. 20 para. 2 AMLA, it may, as a last resort, order the dissolution of legal entities and collective and limited partnerships or the deletion of sole proprietorships from the commercial register. Depending on the severity of the case, FINMA shall publish the measure on its website and in the commercial register in accordance with Art. 34 FINMASA, appoint a liquidator and determine his or her duties. These supervisory measures supplement the criminal provisions for financial intermediaries who operate unlawfully on the financial markets (Art. 44 FINMASA). They serve to restore order and ensure a level playing field on the financial markets. 25 1

In 2024, **FINMA** processed over 1,833 reports and complaints from the public concerning unlicensed financial operators who had often falsely claimed to have a presence in Switzerland or a FINMA license. FINMA's investigations into these reports often lead to enforcement proceedings or entries in the warning list. 25 2

If a person intentionally carries out an activity that requires authorization, recognition, approval, or registration under financial market laws without such authorization, recognition, approval, or registration, they shall be **punished** with imprisonment of up to three years or a fine in accordance with Art. 44 para. 1 FINMASA. In the case of negligence, a fine of up to CHF 250,000 may be imposed in accordance with Art. 44 para. 2 FINMASA. The same applies if the status is not applied for within the statutory period when changing to professional status or as a result of leaving or being excluded from an SRO (Art. 11 and 12 AMLO). 25 3

According to Art. 50 para. 1 FINMASA, the Legal Service of the General Secretariat of the **Federal Department of Finance** (FDF) is responsible for criminal prosecution. It initiates administrative criminal proceedings if it 25 4

learns of a situation through a criminal complaint or in any other way that indicates, in the sense of an initial suspicion, that a possible criminal offense has been committed. As a rule, such a criminal complaint is filed by FINMA.

25 According to the latest **statistics** from FINMA, in 2024 it concluded 232 in-
5 vestigations and 9 enforcement proceedings in the (generally) unauthorized area under the heading "Financial intermediary without a license / SRO affiliation / Fintech business models." In eight cases, FINMA filed criminal charges with the FDF's criminal law service under the heading "Financial intermediary AMLA without authorization/SRO affiliation."

This publication reflects solely the personal opinion of the authors and is not binding on FINMA.

BIBLIOGRAPHY

Ackermann Jürg-Beat/Zehnder Stephanie, Kommentierung zu Art. 305bis StGB, in: Ackermann Jürg-Beat (Hrsg.), Kommentar Kriminelles Vermögen – Kriminelle Organisationen, 2 Bd., Zürich 2018.

Andreotti Fabio, Dezentrale Handelsplattformen im Schweizer Finanzmarktrecht, Zürich 2024.

Andreotti Fabio/Zimmermann Stephan/Prantl Florian, Custodial Staking, GesKR 3 (2023), S. 333 ff.

Bachelard My Chau/Hess Martin, Kommentierung zu Art. 2 Abs. 3 lit. b GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Bahar Rashid, Kommentierung Art. 2 lit. c FinfraG, Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

Baumann Simone, Crowdinvesting im Finanzmarktrecht, SSFM 117, Zürich et al. 2014.

Breuleux Raoul/Gmünder Eliane, Kommentierung zu Art. 7a GwG, in: Graf Damian K./Hutzler Doris, Onlinekommentar, Geldwäschereigesetz, Zürich 2025, https://onlinekommentar.ch/de/kommentare/gwg7a.

Cornelia Stengel/Luca Bianchi, Geldwäscherei und Terrorismusfinanzierung, in: Rolf H. Weber/Hans Kuhn (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Zürich 2021, S. 225 ff.

Daeniker Daniel/Waller Stefan, Kommentierung Art. 2 lit. b FinfraG, Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

De Capitani Werner, in: De Capitani, Schmid Niklaus/Bernasconi Paolo/de Capitani Werner (Hrsg.), Kommentar Einziehung - Organisiertes Verbrechen - Geldwäscherei, Band II, Zürich 2002.

FINMA, Aufsichtsmitteilung 02/2019, Zahlungsverkehr auf der Blockchain, vom 26.8.2019.

FINMA, Ergänzung der Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs) vom 11.9.2019.

FINMA, Jahresbericht 2020, abrufbar unter: 20200325-finma-jahresbericht-2020.pdf, besucht am 11.4.2025.

FINMA, Jahresbericht 2021, abrufbar unter: 20220405-finma_jahresbericht_2021.pdf, besucht am 11.4.2025.

FINMA, Jahresbericht 2022, abrufbar unter: https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/geschaeftsbericht/20230328-finma-jb22.pdf, besucht am 11.4.2025.

FINMA, Jahresbericht 2023, abrufbar unter: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/geschaeftsbericht/20240320_finma_jb2023.pdf, besucht am 11.4.2025.

FINMA, Jahresbericht 2024, abrufbar unter: 20250408-finma_jb24.pdf, besucht am 11.4.2025.

FINMA, Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs) vom 16. Februar 2018.

Frigo Patrick/Jain Vivien, Kommentierung zu Art. 14 GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Fritschi Mirjam Eva, Crowdfunding aus zivilrechtlicher Perspektive, Zürich/St. Gallen 2018.

Glarner Andreas/Ganzoni Romedi/Hepp Sebastian, Erweiterter Geltungsbereich des Geldwäschereigesetzes im DLT-Bereich, AJP 9 (2023), S. 1091 ff.

Graf Crystel, Le commerce de bijoux d'occasion et d'or, EF 1-2/18, S. 84 ff.

Greter Alexander, Kommentierung zu Art. 2 Abs. 3 lit. a GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Grunder Regula/Lienhard Stephan, Kommentierung zu Art. 2 Abs. 3 lit. c GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Heim Kathrin/Wettstein Tamara, Praxiskommentar zur Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken, 4. Aufl., Zürich 2019.

Hess Nico, Geltungsbereich der bewilligungspflichtigen Tätigkeiten im Bankenrecht de lege lata und de lege ferenda, SSFM 142, Zürich et al. 2023.

Hsu Peter Ch./Bahar Rashid/Flühmann Daniel, in: Watter Rolf/Bahar Rashid (Hrsg.), Kommentierung zu Art. 34 FINMAG, Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., 2019.

Humbel Claude/Eckert Fabrice, Decentralized Exchanges: Grundlagen, Risiken und ausgewählte aufsichtsrechtliche Aspekte, SZW 1 (2023), S. 10 ff.

Hutzler Doris, Kommentierung zu Art. 9 GwG, in: Ackermann Jürg-Beat (Hrsg.), Kommentar Kriminelles Vermögen – Kriminelle Organisationen, 2 Bd., Zürich 2018.

Interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT), National Risk Assessment (NRA), Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz, Juni 2015.

Interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT), National Risk Assessment (NRA), Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets, Januar 2024.

Etienne Joane, Kommentierung zu Art. 2 Abs. 2 GwG, in: Graf Damian K./Hutzler Doris, Onlinekommentar, Geldwäschereigesetz, im Erscheinen.

Jutzi Thomas/Abbühl Andri, Fintech und DLT, Privat- und finanzmarktrechtliche Grundlagen in der Schweiz, Bern 2023.

Kindler, Kommentierung zu Art. 14 GwG, in: Graf Damian K./Hutzler Doris, Onlinekommentar, Geldwäschereigesetz, Zürich 2025, https://onlinekommentar.ch/de/kommentare/gwg14.

Kontrollstelle für die Bekämpfung der Geldwäscherei, Unterstellungskommentar, Geldwäschereigesetz, 29.10.2008.

Meirich David, Regulatorische Einordnung von Decentralized Finance, SSFM 144, Zürich et al. 2023.

Meyer Stephan D., Dezentrale autonome Organisationen (DAOs) und das Gesellschaftsrecht der Zukunft, AJP 3 (2023), S. 319 ff.

Nagel Thomas, Der persönliche und sachliche Geltungsbereich des schweizerischen Geldwäschereigesetzes (GwG), SSFM 132, Bern 2020 (zit. Nagel, GwG).

Nagel Thomas, Dienstleistungen für den Zahlungsverkehr unter dem Geldwäschereigesetz: Abgrenzungen und ausgewählte Praxisfragen, GesKR 1 (2023), S. 72 ff. (zit. Nagel, GesKR).

Peyer, Kommentierung zu Art. 2 Abs. 4 GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Schären Simon, Kommentierung zu Art. 2 GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar zum Geldwäschereigesetz, Bern 2017.

Schott Ansgar/Kessler Martina A., Kommentierung zu Art. 8a GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar zum Geldwäschereigesetz, Bern 2017.

Schwob/Wohlers, Kommentierung zu Art. 50 FINMAG, Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

Sethe Rolf/Aggteleky Tobias, in: Sethe Rolf/Bösch René/Favre Olivier/Kramer Stefan/Schott Ansgar (Hrsg.), Kommentar zum Finanzdienstleistungsgesetz, Zürich et al. 2021.

Staatssekretariat für internationale Finanzfragen, Bundesrat eröffnet Vernehmlassung zu Verordnungen über die Transparenz juristischer Personen und die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Medienmitteilung vom 15.2025, abrufbar unter https://www.sif.admin.ch/de/geldwaeschereigesetz-gwg, besucht am 17.10.2025.

Stengel Conrrnelia/Glarner Andreas, Anwendung des GwG auf Tokens, in: Blockchain Taskforce, Positionspaper zur rechtlichen Einordnung von ICOs, April 2018, S. 17–23.

Stengel Cornelia, Wirtschaftliche Berechtigung an digitalen Werten, in: Jusletter 22. August 2022.

Stengel Cornelia/Ruckstuhl Lea, in: Stengel Cornelia/Weber Rolf H. (Hrsg.), Digitale und mobile Zahlungssysteme, Kredit- und Debitkarten, Wallets, virtuelle Währungen und Kryptowerte, 2. Aufl., Zürich et al. 2024.

Stengel Cornelia/Wirthensohn Gino/Stäuble Luca, Regulierung von künstlicher Intelligenz für FinTech-Anwendungen, SZW 4 (2021), S. 395 ff.

Thelesklaf Daniel/Wyss Ralph, Kommentierung zu Art. 20 GwG, Orell Füssli Kommentar, Schweizerisches Geldwäschereigesetz mit weiteren Erlassen, 3. Aufl. Zürich 2019.

Weber Rolf H., Versicherungsvermittlung – Quo vadis Rechtsauslegung?, SJZ 120/20 (2024), S. 939 ff.

Wyss Ralph, Kommentierung zu Art. 2 GwG, Orell Füssli Kommentar, Schweizerisches Geldwäschereigesetz mit weiteren Erlassen, 3. Aufl., Zürich 2019.

Zysset Pascal/Nagel Thomas, Der räumliche Geltungsbereich des Geldwäschereigesetzes, GesKR 2 (2018), S. 140 ff.

MATERIALS

Änderung des GwG vom 26.9.2025, BBl 2025 2899, abrufbar unter https://www.fedlex.admin.ch/eli/fga/2025/2899/de, besucht am 17.10.25.

Anhörungsbericht zum FINMA-Rundschreiben 2011/1 vom 26.11.2010, abrufbar unter https://www.finma.ch/de/~/media/finma/importiertedokumente/regulierung/anhoerungen/26-rundschreiben-finanzintermediation-nach-gwg/br-rs-finanzintermediation-gwg.pdf?sc_lang=de&hash=06D20A8E19BBBA06D2CB3255C7977A1E, besucht am 30.7.2025.

Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070) vom 25.6.2014, abrufbar unter https://www.news.admin.ch/NSBSubscriber/message/attachments/35361.pdf, besucht am 30.7.2025.

Botschaft zum Bundesgesetz über die Eidgenössische Finanzmarktaufsicht vom 1.2.2006, BBl 2006 2887, abrufbar unter https://www.fedlex.admin.ch/eli/fga/2006/303/de, besucht am 30.7.2025.

Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG) vom 17.6.1996, BBl 1996 III 1101, abrufbar unter https://www.fedlex.admin.ch/eli/fga/1996/3_1101_1057_993/de, besucht am 30.7.2025.

Botschaft zum Bundesgesetz über die Transparenz juristischer Personen und die Identifikation der wirtschaftlich berechtigten Personen vom 22.5.2024, BBl 2024 1607, abrufbar unter https://www.fedlex.admin.ch/eli/fga/2024/1607/de, besucht am 29.7.2025.

Botschaft zum Finanzdienstleistungsgesetz (FIDLEG) und zum Finanzinstitutsgesetz (FINIG) vom 4.11.2015, BBl 2015 8901, abrufbar unter https://www.fedlex.admin.ch/eli/fga/2015/2141/de, besucht am 30.7.2025.

Botschaft zum Finanzmarktinfrastrukturgesetz (FinfraG) vom 14.10.2014, BBl 2014 7483, abrufbar unter https://www.fedlex.admin.ch/eli/fga/2014/1633/de, besucht am 30.7.2025.

Bericht des Bundesrates zu den rechtlichen Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz vom 14.12.2018, abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/55150.pdf, besucht am 30.7.2025.

Erläuterungen zur Verordnung des Bundesrates zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register

vom 18.6.2021, abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/67150.pdf, besucht am 30.7.2025.

Erläuterungsbericht der EBK zur Revision der Bankenverordnung (Devisenhändler) vom 19.11.2007, abrufbar unter https://www.finma.ch/FinmaArchiv/ebk/d/regulier/konsultationen/20071119_04_d.pdf, besucht am 30.7.2025.

Erläuterungsbericht zur Geldwäschereiverordnung vom 11.11.2015, abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/41723.pdf, besucht am 30.7.2025.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 3 AMLA

A commentary by Robert Iliev / André Tanner

SUGGESTED CITATION

Robert Iliev/André Tanner, Commentary of art. 3 AMLA, in: Damian K. Graf/ Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Iliev/Tanner, art. 3 AMLA N. XXX.

Chapter 2 Duties

Section 1 Financial Intermediaries Duty of Due Diligence

Art. 3 Verification of the identity of the customer

[1] When establishing a business relationship, the financial intermediary must verify the identity of the customer on the basis of a document of evidentiary value. Where the customer is a legal entity, the financial intermediary must acknowledge the provisions regulating the power to bind the legal entity, and verify the identity of the persons who enter into the business relationship on behalf of the legal entity.

[2] In the case of cash transactions with a customer whose identity has not yet been identified, the duty to verify identity applies only if one transaction, or two or more transactions that appear to be connected, involve a considerable financial value.

[3] Insurance institutions must verify the identity of the customer if the amount of a single premium, the regular premium or the total of the premiums involves a considerable financial value.

[4] If in cases under paragraphs 2 or 3 there is any suspicion of money laundering or terrorist financing, the identity of the customer must be verified even if the relevant amounts have not been reached.

[5] FINMA, the Federal Gaming Board (FGB), the Federal Department of Justice and Police (FDJP), the Federal Office for Customs and Border Security (FOCBS) and the self-regulatory organisations shall determine what constitutes a considerable financial value within the meaning of paragraphs 2 and 3 in their respective fields and adjust such values as required.

CONTENT

I. Preliminary remarks ... 155
II. Art. 3 para. 1 AMLA – Identity of the contracting party ... 156
A. Entering into a business relationship ... 156
1. Business relationship ... 156
2. Time ... 157
3. Contracting party ... 159
4. General provisions ... 161
a. Evidentiary value ... 161
b. Validity ... 161
c. Information to be documented ... 162
d. Internal documentation ... 163
5. Irregularities in identification ... 164
a. Substantive verification of the information and documents? ... 164
b. Missing identification documents ... 165
c. Doubts during identification ... 165
d. Failure of identification ... 166
B. Identifying natural persons ... 167
1. In the event of a personal meeting ... 167
2. By correspondence ... 167
3. Issuers of confirmations of authenticity ... 169
4. Special forms ... 170
a. Minors ... 170
b. Sole proprietorship ... 170
c. Communities of heirs ... 170
d. Joint accounts ... 171
e. Collective accounts ... 171
f. Usufruct ... 171
g. Condominium and co-ownership associations ... 171
h. Tenant deposit account ... 172
i. Life insurance contracts ... 172
C. Identification of legal entities and partnerships ... 172
1. When registering ... 172
2. Without entry in the register ... 173
3. Identity of persons establishing the business relationship ... 173
4. Power of attorney ... 174
5. Special forms ... 175
a. Simple partnership ... 175
b. Widely known company and authority ... 176
c. Trust ... 176
d. Company in formation ... 177

D. Delegation ... 177
1. General provisions ... 177
2. Types of delegation ... 178
a. Delegation with written agreement ... 178
b. Delegation without written agreement ... 178
E. FINMA-RS 2016/7 ... 179
1. General ... 179
2. Video identification ... 180
3. Online identification ... 181
4. Involvement of third parties ... 183
III. Art. 3 para. 2 AMLA – cash transactions ... 184
A. Definitions ... 184
1. AMLO-FINMA / CDB 20 ... 184
2. AMLO-SFBC ... 184
3. AMLO-FDJP ... 185
4. AMLO-BAZG ... 185
B. Significant threshold ... 186
C. Lack of prior identification ... 186
IV. Art. 3 para. 3 AMLA – Insurance premiums ... 186
V. Art. 3 para. 4 AMLA – suspicion of money laundering ... 187
VI. Art. 3 para. 5 AMLA – Authorities defining the threshold ... 189
A. FINMA ... 189
B. SBA ... 190
C. SRO - Example SRO-SIA ... 190
D. ESBK ... 190
E. FDJP ... 190
F. BAZG ... 191
VII. Sanctioning of violations of the identification requirement ... 191
A. FINMASA, AMLA, AMLO-FINMA ... 191
B. CDB ... 193
C. SRO – example SRO-SIA ... 195
D. External asset managers and trustees ... 195
Bibliography ... 196
Materials ... 199

I. PRELIMINARY REMARKS

The **beginnings of** customer due diligence date back to the very first agreement on the duty of care in the acceptance of funds and the handling of banking secrecy from July 1, 1977. In the years that followed, the Swiss Bankers Association increased the level of detail of the rules in connection with customer due diligence. In 1998, following various parliamentary initiatives and growing pressure from abroad, the duty to verify the identity of the contracting party was enshrined in law and extended to the non-banking sector. Since then, only marginal adjustments have been made to the legal text, which has been supplemented by various implementing provisions at the ordinance and sector-specific self-regulation level. 1

The identification of the contracting party is part of the catalog of duties defined in the AMLA that is intended to ensure due diligence in financial transactions. It is a central cornerstone in the fight against money laundering and terrorist financing. The particular **purpose of** identifying the contracting party is to reduce anonymity and increase transparency in financial transactions. Incriminated assets can be more clearly assigned to a person or persons, and the individual movements of assets can be better traced. In conjunction with the other due diligence requirements, the documentary basis is created that not only helps the authorities to locate and confiscate incriminated assets, but also to identify and potentially prosecute the persons responsible for money laundering. Financial intermediaries and traders are supported in identifying the contracting party with a better understanding of their customers ("Know Your Customer"). The granularity of the understanding of the customer has an impact on the economic component of a financial intermediary or trader. The more detailed the knowledge of a customer, the more profitably the range of services can be tailored to that customer. 2

The application and scope of the identification of the contracting party is based on the activity performed as a financial intermediary or dealer, the legal form of the contracting party, the type, duration and value of the assets of a business relationship in connection with financial transactions or the existence of special circumstances. For reasons of clarity and relevance of the following financial intermediaries for the Swiss financial center, this commentary focuses on the implementing provisions for **banks** (Art. 2 para. 2 let. a AMLA in conjunction with Art. 35 AMLO-FINMA and Art. 4–19 CDB 20), **in-** 3

surance institutions (Art. 2 para. 2 let. c AMLA in conjunction Art. 42 f. AMLO-FINMA and Art. 3–8 R SRO-SVV) and **external asset managers** (Art. 2 para. 2 let. a^{bis} AMLA in conjunction with Art. 44–55 AMLO-FINMA).

II. ART. 3 PARA. 1 AMLA – IDENTITY OF THE CONTRACTING PARTY

A. Entering into a business relationship

1. Business relationship

4 When entering into a business relationship, a financial intermediary is obliged under Art. 3 para. 1 AMLA to identify the contracting party on the basis of a probative document. AMLA does not provide a legal definition of the term "business relationship". A business relationship within the meaning of Art. 3 para. 1 AMLA exists when a **contractual relationship under private or administrative law** exists between a financial intermediary and another party in connection with a **financial transaction**. The individual implementing provisions define what constitutes a relevant financial transaction with regard to the identification of the contracting party for financial intermediaries within the meaning of Art. 2, para. 2 AMLA that are subject to the licensing requirements under special legislation. Financial intermediaries without special licensing requirements are obliged to identify the contracting party if they carry out, in particular, any of the financial transactions listed in Art. 2 para. 3 let. a–g AMLA on a professional basis. The financial transactions that fall under Art. 2, para. 3, let. a–g AMLA or are explicitly excluded from it are set out in the implementing provisions. For certain financial transactions, the duty to verify the identity of the contracting party only arises when a threshold value is reached and/or exceeded.

5 The **banking sector** itself regulates the following financial transactions in particular: opening accounts, savings books or securities accounts; conducting fiduciary transactions; renting safe-deposit boxes; accepting instructions to manage assets held by third parties; executing trading transactions involving securities, foreign exchange, precious metals and other commodities as well as cash transactions involving amounts in excess of CHF 15,000. For decades, banks have also been obliged to verify the identity of their contractual partners in credit relationships. The list of financial transactions provided for in

CDB 20 is therefore not exhaustive. It is supplemented by a ban on opening new bearer savings books.

Of the **insurance institutions**, those that offer or distribute units in collective investment schemes, operate direct life insurance or grant mortgage loans fall within the scope of the AMLA. In addition, a monetary threshold must be met for most of these financial transactions in order for the duty to identify the contracting party to take effect. Financial transactions that are not considered relevant to the AMLA include, in particular, pillar 2 and 3a insurance contracts, pure risk insurance (so-called insurance without a savings component), and the activities in connection with (mortgage) lending business that are explicitly excluded in Article 3 AMLO. Consequently, insurance institutions are not covered by the scope of the AMLA when operating a (tax-exempt) pillar 2 or 3a pension fund. 6

An **external asset manager** within the meaning of the AMLA is a person who, on a commercial basis, is able to dispose of assets on behalf of clients in the context of a financial transaction in accordance with Art. 3 let. c no. 1–4 of the FIDLEG. Financial transactions include all financial services to be provided for clients in connection with financial instruments in the areas of execution only, investment advice and asset management. In addition, any activity directed at specific customers that specifically aims at the purchase or sale of a financial instrument is to be regarded as a financial transaction; currency exchange transactions of CHF 5,000 or more; cash transactions of CHF 15,000 or more; transactions with virtual currency of CHF 1,000 or more, provided that these do not constitute money and value transfers and these transactions do not constitute a long-term business relationship within the meaning of Art. 2 let. d AMLO-FINMA; transfers of funds and assets from Switzerland abroad; transfers of funds and assets from abroad to Switzerland in excess of CHF 1,000. 7

2. Time

Pursuant to Art. 3 para. 1 AMLA, the financial intermediary must identify the contracting party **when entering into the business relationship**. A business relationship is deemed to have been entered into when the customer can use the contractually agreed services of the financial intermediary in connection with a relevant financial transaction. The contracting party must be identified before or at the latest upon the commencement of the business rela- 8

tionship. It is recommended that the contracting party be identified as part of the due diligence and thus before the business relationship is established, which is also how financial intermediaries usually do it. The main reasons for this are the ability to correct identification errors as part of the "multiple-eye" approval/control process and the associated avoidance of self-regulatory sanctions that could potentially be imposed in the event of a breach of due diligence.

9 According to Art. 4 para. 1 CDB 20, **banks** are obliged to verify the identity of the contracting party when entering into a business relationship. Art. 45 para. 1 CDB 20 clarifies that an account may only be used once the documentation required for the identification of the contracting party is complete and in the proper form. An account is deemed to be usable if it is technically possible to make bookings on the account. If only the account number is reserved internally within the bank or the account is blocked for inflows and/or outflows, the criterion of usability is not met. Potential customers (prospects) recorded in the system are only to be identified when the business relationship is established. In exceptional cases, an account may be used if only individual details and/or documents are missing or individual documents are not available in the proper form, sufficient information is available on the identity of the contracting party and the controlling person and/or beneficial owner and the application of this exception appears appropriate based on a risk-based assessment. The satisfaction of the cumulative conditions must be documented in a manner comprehensible to a knowledgeable third party. The missing information and/or documents must be obtained no later than 30 days after the business relationship is established. Art. 45 para. 3 in conjunction with para. 4 CDB 20 cannot be invoked if no identification documents are available at all or if the documents are inadequate, unclear or contradictory. One of the main cases in which the exception is applied in practice is when the bank has all the information and documents in full, but one of the identification documents is only available as a scan and not yet in the original.

10 **Insurance institutions** must have completed the identification of the contracting party completely and properly at the time of delivery of the policy, in the case of mortgage transactions before disbursement of the loan and in the area of collective investment schemes before the services are exchanged (i.e. acceptance of assets vs. posting of financial instruments to the client portfolio). There is no apparent obligation for insurance institutions to identify po-

tential customers, especially since the duty of care can be carried out in all cases even after the contract has been concluded. The self-regulation of the insurance sector is silent on an analogous exception to the banking sector, namely the ability to provide missing information and/or documents after the business relationship has commenced, within a specified period of time.

External asset managers are obliged to carry out the identification of the contracting party when entering into a business relationship. Art. 55 para. 1 AMLO-FINMA specifies that all the documents and information required to identify the contracting party must be available in full before any transactions are carried out within the framework of a business relationship. As part of their self-regulation, a supervisory organization may impose stricter provisions than those of AMLO-FINMA and require its members to carry out the complete and proper identification of the contracting party at an earlier stage. The AMLO-FINMA and the self-regulation of the supervisory organizations do not provide for the possibility of subsequently documenting individual missing details and/or documents within a period of time after the execution of the first transaction or receipt of the power of disposition over the client assets. 11

3. Contracting party

A contracting party is any person **deemed to be a legal entity under the locally applicable civil or public law** that enters into a contractual relationship of a private or administrative nature with a financial intermediary in connection with a financial transaction. This includes all natural persons, legal entities or partnerships, public-law institutions, corporations, foundations and administrative units at the national, regional or municipal level in Switzerland or abroad. Public-sector entities are grouped together as “authorities” in CDB 20 and AMLO-FINMA, while self-regulation in the insurance sector (with the same interpretation content) refers to public-sector companies/corporations. The contracting party does not have to consist of only one legal entity, but can in principle be made up of several identifiable parties. If a financial intermediary's systems and/or the nature of the financial transaction do not provide for any restrictions, there is basically no limit to the number of parties that can make up a contracting party. 12

From Art. 3 para. 1 sentence 1 AMLA e contrario, it can be concluded that persons with whom the financial intermediary does not enter into **a contrac-** 13

tual relationship of a private or administrative nature in connection with a financial transaction do not have to be identified. However, if a legal entity or partnership is a contracting party, since 2009 all financial intermediaries have been legally obliged to take note of the power of attorney of a contracting party and to verify the identity of the person who enters into the business relationship on behalf of the contracting party (the so-called opener). In practice, a more in-depth implementation of Art. 3 para. 1 sentence 2 AMLA is observed in particular with regard to banks and external asset managers. For reasons relating to liability risks and the duty to verify the identity of the beneficial owner as provided for in Art. 4, para. 1, sentence 1 AMLA, a simple copy of the identification document is also obtained from authorized agents and beneficial owners or controlling owners and checked for plausibility as part of the due diligence of a business relationship.

14 If a legal entity has **already been identified** in an existing business relationship, the financial intermediary shall not carry out a new identification of the entity when the business relationship is extended. A legal entity shall be deemed to have already been identified if, when the business relationship was originally established, the identification was carried out in accordance with the implementing provisions in force at that time or, alternatively, with the currently applicable implementing provisions (so-called lex mitior). In practice, it has been observed that, for liability reasons, banks in particular only refrain from re-identifying a legal entity when expanding an existing business relationship if a qualitatively adequate copy of an identification document from the previous identification is available. Some financial intermediaries are even stricter and stipulate in their internal guidelines that they only accept copies of valid identification documents. When a business relationship is expanded, attention should be paid to the currency of the identification document in order to prevent the risk of violating one's own guidelines. The option of waiving re-identification is limited only to the legal entity that has already been identified and has no effect on other, previously unidentified legal entities within the framework of a multiparty agreement. The reasons for waiving a new identification are not to be documented on record. Rather, it is sufficient if it can be seen from the physical or electronic documentation that the legal entity has already been correctly identified.

4. General provisions

a. Evidentiary value

The financial intermediary must identify the contracting party in accordance with Art. 3, para. 1, first sentence AMLA on the basis of a conclusive document. In the 1996 Message, examples of **conclusive documents** for natural persons include official proof of identity such as a passport or ID card, and for legal entities, an extract from the commercial register or an equivalent document (certificate of incorporation). The question of when a document meets the requirements of conclusiveness is defined in the individual implementing provisions or according to civil or public law aspects. 15

b. Validity

Whether an identification document must be valid and how long it is considered valid is a key question for a financial intermediary when carrying out his due diligence. The regulations for the banking and insurance sectors and AMLO-FINMA do not explicitly stipulate a validity requirement for the identification document of a **natural person**. It is therefore left to the competence and discretion of the individual banks, insurance institutions and external asset managers to determine in their internal guidelines whether invalid identification documents are permitted when identifying natural persons, and if so, only in exceptional cases or not at all. If the identification document is no longer valid, it is assumed that there is no doubt about the identity of the natural person to whom it was issued and that there is no reason to believe that it no longer reflects the current circumstances (e.g. change of name due to marriage). If a financial intermediary decides to accept expired identification documents in general or in exceptional situations, he runs the risk that a knowledgeable third party (e.g. an audit firm or self-regulatory/supervisory organization) may assess the question of the admissibility of the identification document differently in individual cases. When choosing one of these approaches, it is recommended that at least the most important key points for dealing with invalid identification documents be defined in the internal guidelines. In particular, it would be necessary to determine under which conditions an expired identification document may be accepted, how the validity of the identification document is to be periodically verified and under which circumstances it is to be updated. If a financial intermediary decides to accept only valid identification documents, he is depriving himself of the flexibility to 16

react to exceptional situations, increases his monitoring and updating efforts for the duration of the business relationship and runs a greater risk of violating his internal guidelines. It is therefore recommended that the processes and controls in connection with the validity of the identification documents be set out in the internal guidelines if this approach is chosen.

17 The document used to identify the contracting party, which is a **legal entity or partnership**, must not be older than twelve months and must reflect the current circumstances. An exception to this deadline is planned for banks, insurance institutions and external asset managers with regard to a specific type of association. An association that is not entered in the commercial register and is not subject to audit can only be identified by means of (usually older) statutes or other association documents. Depending on the date of establishment, such a contracting party would be unable to provide the financial intermediary with a conclusive identification document that was issued less than twelve months previously. It would therefore be impractical to adhere to the twelve-month period for an association that is not entered in the commercial register and is not subject to auditing requirements.

18 The date of issue of the identification document and the time at which the financial intermediary identifies the contracting party on the basis of the identification document presented to him and documents the performance of the identification for knowledgeable third parties are decisive for the **calculation of the deadline**. In doing so, the financial intermediary must carry out the identification of the contracting party with a view to establishing the business relationship in a timely manner and must not do so "in advance" with a view to meeting the deadline. It is therefore not unusual for a considerable period of time to elapse between the time of identification and the establishment of the business relationship.

c. Information to be documented

19 Financial intermediaries must record and retain the **essential information** obtained through the identification of the contracting party (see Art. 7, para. 1 AMLA). In the case of multiparty contracts, this must be done for each individual legal entity that makes up the contracting party.

20 In the case of **natural persons**, the financial intermediary must record and document the person's surname, first name, date of birth, domicile address

and nationality. In accordance with Art. 23, para. 1 CC, domicile is the place where the natural person resides with the intention of remaining there permanently. Even though the dispatch and the individual implementing provisions speak of one nationality, it is advisable to clarify with the contracting party and document any further nationalities. This is due less to the duty of care in identifying the contracting party and more to the assessment of the risks of a business relationship in the areas of money laundering and terrorist financing, sanctions or taxes.

If the natural person comes from a country in which **dates of birth or residential addresses are not used**, this information is not to be recorded or kept. However, the background to such cases is to be recorded in writing (e.g. in the form of a memo). 21

In the case of **legal entities or partnerships**, the financial intermediary must record and retain the company name and registered address. When determining the registered address, the identification documents obtained (e.g. an extract from the commercial register) may be used as a primary source. 22

d. Internal documentation

In addition to recording and retaining the essential information from the identification of the contracting party, a financial intermediary must also record the means by which the identity was verified. Consequently, he is obliged to keep on his files a simple or certified copy of the document(s) on the basis of which the contracting party was identified. Internal files and thus the information and documents obtained, as well as clarifications carried out internally in connection with the identification of the contracting party, must be created, organized and stored in such a way that an **expert third party** can form a reliable opinion on compliance with due diligence within a reasonable period of time. In practice, it can be observed that banks and insurance institutions in particular store their documentation associated with the identification of the contracting party both physically and electronically in systems specifically designed for this purpose. In order to make them easier to find, they label the identification documents with specific titles/codes. External asset managers shall store the internal documentation associated with the due diligence commented on here mainly physically, i.e. in a separate section of the physical folder/file, and/or the files thereof at a separate location within the framework of a simple electronic folder structure. 23

5. Irregularities in identification

a. Substantive verification of the information and documents?

24 In the case of natural persons, the financial intermediary must **examine the identification document** and check the photograph to see whether the person appearing is the person indicated. If the contracting party is a legal entity or a partnership, a financial intermediary must check the identification documents in particular to see whether it exists and to see who represents it and to what extent. If no personal meeting takes place between the financial intermediary and the contracting party in the context of the identification, the confirmation of authenticity to be consulted by the financial intermediary shall confirm that the contracting party and the person on the identification document are one and the same.

25 A financial intermediary must also **verify that** the information documented corresponds to that on the identification document(s). With regard to the address of domicile and registered office, the financial intermediary may, in principle, rely on the information provided by the contracting party, since the address of domicile, in particular, is rarely reflected in an identification document. In line with a risk-based approach, the financial intermediary has further duties of clarification if there are indications (e.g. contrary information in the course of due diligence) that the information provided by the contracting party may not be correct (any longer). When opening an account by correspondence, banks and external asset managers must always verify the domicile address by postal delivery or other equivalent means. The implementing provisions for the insurance sector explicitly exclude this.

26 The implementing provisions require that, when a business relationship is established, the identification documents reflect the **current circumstances** of a legal entity or partnership. A financial intermediary should be able to rely on the information provided by the contracting party with regard to the up-to-dateness of the circumstances. If, in the course of the due diligence, there are indications that the identification documents do not reflect the current circumstances of the contracting party, the financial intermediary is obliged to obtain a more up-to-date version.

27 The financial intermediary must check the plausibility of the identification document with **reasonable effort** with respect to its authenticity. To do this,

the financial intermediary must know the main characteristics of the identification documents of a country from which he wishes to accept contracting parties.

b. Missing identification documents

If a contracting party has no identification document within the meaning of the implementing provisions, a financial intermediary may, exceptionally, establish the identity on the basis of **conclusive substitute documents**. This approach applies in particular to natural persons without identification documents or public-law legal entities with no obligation to be entered in the commercial register and to have corresponding company documents. What is considered to be a substitute document of evidentiary value in such special cases depends on the legal nature of the contracting party, the legal circumstances and documentation standards of the country or countries concerned. The exceptional situation must be explained in writing and attached to the contracting party's complete documentation together with the substitute document of evidentiary value. The reasons for the absence of a corresponding identification document and the choice of alternative probative document should be clearly stated. 28

c. Doubts during identification

If a financial intermediary has doubts concerning the information provided on the identity of the contracting party when entering into or during the business relationship, he shall take appropriate **measures,** such as carrying out clarifications and/or repeating the identification. There is doubt if there are indications that the information on the identity of the contracting party is not or is no longer correct. It is recommended that measures be taken immediately if there are such indications. If the financial intermediary is able to dispel his doubts by taking the measures, the background and the result of the measures taken must be recorded in writing and attached to the overall documentation of the contracting party. If, despite the measures taken, the doubts cannot be removed (within the deadline) or if the financial intermediary suspects that the contracting party has knowingly provided false information regarding his identity or has provided forged documents, the identification shall be deemed to have failed. 29

30 In practice, doubts regarding the identity of the contracting party arise less frequently than regarding the beneficial owner, both at the outset and during the course of a business relationship. In particular, the **heavy focus on formal aspects** of Art. 3 AMLA in conjunction with the individual implementing provisions, the personal or written interaction between the contracting party or their representative(s) and the financial intermediary, the standardization and the fundamentally "official nature" of the documents to be obtained make it difficult for customers to consciously or unconsciously influence the identification process. In practice, doubts about the information originally provided by the contracting party regarding their identity only arise in the course of a business relationship. The most common reasons will be relocation, marriage in connection with a change of name, death or naturalization.

d. Failure of identification

31 An identification is deemed to have failed at the start of or during a business relationship if the requested **information and/or documents** from the contracting party as part of the identification process are **not provided (in a timely manner)**, the financial intermediary's **doubts** about the information and/or documents regarding the identity of the contracting party are **not dispelled in a timely manner** despite measures taken, or there is a suspicion that the contracting party has **deliberately provided false information** and/or has provided **forged documents**. If the identification of a contracting party fails, the establishment of a new business relationship must be refused or the continuation of an existing business relationship must be discontinued in compliance with Art. 9 et seq. AMLA in conjunction with Art. 12a et seq AMLO. If requested, the business relationship must be blocked for inflows and outflows. The AMLA and its implementing provisions do not define how quickly a business relationship is to be rejected or terminated in cases of failed identification without any suspicion of possible money laundering or terrorist financing. For the banking sector, this is to be done as quickly as possible without committing a breach of contract. Insurance institutions and external asset managers are also recommended to reject the new business relationship or terminate the existing one as quickly as possible in such cases. In addition, in the event of failed identifications, they should also document the background, the result of the measures taken and the fact of the rejection or termination itself, including the exact time, and attach this to the overall documentation of the (potential) contracting party. If identification fails, it must

be assumed that all the business relationships in which the contracting party is involved have been "contaminated". For this reason, in such cases all (potential) business relationships must be rejected and/or existing business relationships must be terminated that one intends to conduct or conducts with the contracting party.

B. Identifying natural persons

1. In the event of a personal meeting

During the personal meeting, **physical contact** takes place. In the process, a representative of the financial intermediary views and makes a copy of a probative document belonging to the contracting party and files it. The client file should show when and where this physical contact took place. The regulations do not specify where and for how long the meeting should take place. It does not necessarily have to be on the business premises of the financial intermediary. If a copy of the probative document is only made after the personal meeting, the provisions on identification when establishing a business relationship by correspondence apply. 32

An **evidentiary document** is an official document with a photograph, such as a passport, an ID card or a driver's license. The CDB does not provide an exhaustive list. In line with the risk-based approach, it is up to the financial intermediary to decide which documents are acceptable. On the other hand, for insurance companies, Art. 4 R SRO-SVV definitively regulates the permissible probative documents for natural persons. For external asset managers, Art. 45 Para. 3 AMLO-FINMA stipulates that those identification documents are permissible that are provided with a photograph and have been issued by a Swiss or foreign authority. 33

The **copy of** the document does not necessarily have to be photocopied, but can also be scanned or photographed. In addition to the identification data and the signature, the photograph of the contracting party must also be recognizable on the copy. Reasons for which it is technically impossible to make a recognizable copy of the photograph remain reserved. 34

2. By correspondence

When entering into a business relationship **by correspondence**, the financial intermediary must verify the domicile address of the contracting party by 35

postal delivery or by another equivalent means and file a certified copy of the probative document.

36 The term "by correspondence" is too narrowly defined, as it includes not only the opening of the business relationship by letter, but also by telephone, via the internet or by other electronic means, such as online identification in accordance with FINMA Circular 2016/7. The case in which a third party who is not authorized to represent and is not is not considered to be a contracting party, personally delivers the account-opening documents signed by the contracting party to the financial intermediary, as in such cases there is no personal meeting with the contracting party. It would therefore be more precise to use the wording of Art. 45 para. 2 AMLO-FINMA: "Establishment of the business relationship '**without personal meeting**'".

37 The financial intermediary must **verify the domicile address** by postal delivery or another equivalent method. According to CDB 20, delivery by ordinary mail (A or B mail) is sufficient. In particular, the provision of an official confirmation of domicile is deemed to be equivalent. The provision of so-called *utility bills* (electricity, water or telephone bills) and tax or other official bills is also common.

38 In the case of **insurance companies**, the domicile address does not have to be verified. In addition, Art. 4 Para. 1 lit. c R SRO-SVV allows a further procedure for this sector: "Instead of identification in accordance with lit. a [in person] and b [by correspondence], it is sufficient in both cases to deliver the insurance policy or the confirmation of the opening of the premium account by a domestic or foreign post office by registered letter with return receipt or by courier service with receipt, provided that delivery is made personally to the person to be identified and that the person is identified on the basis of an official identification document in accordance with lit. a. The insurance company must keep the return receipt/receipt and a simple copy of the identification document on file."

39 From a practical point of view, the following should also be noted. According to Art. 13 para. 2 lit. c AMLO-FINMA, the absence of personal contact with the contracting party is also a possible **criterion for a business relationship with increased risks (GmeR)**. Establishing a business relationship by correspondence may thus have an impact on the risk calculation of the business relationship. The internal risk score will be increased if this is taken into ac-

count or may even lead to the business relationship being classified as a higher-risk business relationship. Furthermore, it should be noted that actively avoiding personal contact is a **clue to money laundering** in accordance with no. 3.4.1 of the AMLO-FINMA appendix.

3. Issuers of confirmations of authenticity

When the business relationship is established without a personal meeting, the financial intermediary receives a copy of the required probative document instead of the original. It is therefore necessary to confirm the **authenticity of the copy**. 40

The confirmation of the authenticity of the copy of the probative document may be **issued by** a notary or a public office which usually issues such confirmations of authenticity; a financial intermediary in accordance with Art. 2, para. 2 or 3 AMLA with domicile or registered office in Switzerland; an attorney licensed in Switzerland; a financial intermediary domiciled or based abroad that carries out an activity in accordance with Art. 2 para. 2 or 3 AMLA, provided that it is subject to equivalent supervision and regulation with regard to combating money laundering and terrorist financing. 41

What is meant by "**equivalent supervision and regulation**" in relation to combating money laundering and terrorist financing? The Anti-Money Laundering Control Authority (AMLCA), one of the three predecessor authorities of FINMA, had already stated in its practice regarding Article 2 para. 3 AMLA that equivalence cannot be verified in the abstract. It therefore left the clarifications to the individual financial intermediaries and did not maintain a list of the supervisory authorities recognized as equivalent. FINMA also does not publish such a list. The CDB also states that "equivalent" or "appropriate" must be assessed on a case-by-case basis. Possible criteria include the FATF country list or the assessments of Transparency International and other non-governmental organizations (NGOs). However, the assessment in each individual case remains decisive. In this process, it must be ensured that, on the one hand, the equivalent "supervision" and, on the other hand, the equivalent "regulation" or "supervision" must be assessed. 42

Regarding the term **attorney-at-law**, the CDB 20 Commentary and the R SRO-SVV Commentary state that public bodies within the meaning of Art. 11 para. 1 let. c CDB 20 and Art. 4 para. 2 let. b R SRO-SVV can also include at- 43

torneys-at-law licensed abroad. However, they must be authorized for this function by the foreign law. In practice, there is often uncertainty when the issuer of the certificate of authenticity does not identify themselves with the most common term "lawyer" or "attorney-at-law", but rather as "advocate", "solicitor", "lawyer", "solicitor", "lawyer" or "barrister". With regard to the correct interpretation of the term "lawyer", it is not the terminology used that is decisive, but the possession of a lawyer's patent. On the basis of this additional qualification, licensed lawyers enjoy greater credibility than simple lawyers.

44 In order to take account of the growing use of digital technology, an alternative to the authentication of copies of the documents required as evidence is provided for. The financial intermediary may also obtain a copy of an identity document from the **database of a recognized certification service provider** in accordance with the Federal Act on Electronic Signatures (ZertES). The contracting party is authenticated electronically. The technical procedure of the electronic signature can be used to verify the authenticity of a document, an electronic message and the identity of the signatory.

4. Special forms

a. Minors

45 When a business relationship in the name of a minor is opened by a third party, the **opening adult person** must be identified. However, if the **(sane) minor** opens a business relationship in person, it is the minor (and not his legal representative) who must be identified.

b. Sole proprietorship

46 When entering into a business relationship with the owner of a sole proprietorship, the financial intermediary shall comply with the **requirements for natural persons**. Banks and insurance companies may also proceed in accordance with the rules **applicable to legal entities and partnerships** for sole proprietorships registered in the commercial register.

c. Communities of heirs

47 If the financial intermediary's contracting party dies, the community of heirs shall succeed to the business relationship by universal succession, and shall become the new contracting party. In civil law, communities of heirs are to be

qualified as **simple partnerships**. Therefore, when a new business relationship is established, the provisions of Art. 46 para. 1 AMLO-FINMA, Art. 16 para. 1 CDB 20 or Art. 4 para. 5 R SRO-SVV apply. If the **deceased person** has already been properly identified in the context of an existing business relationship, re-identification can be waived.

d. Joint accounts

Unless an exception applies, **all account holders** must be identified for joint accounts (including so-called *joint accounts*). This has been repeatedly confirmed by the CDB supervisory board. It must also apply by analogy to external asset managers. If a life insurance contract is concluded by several policyholders, all policyholders must also be identified. 48

e. Collective accounts

As long as the ownership rights are held in a collective account or collective deposit account in the name of the company, **only the company** must be identified for collective accounts or collective deposit accounts used to manage employee ownership plans. 49

f. Usufruct

If both the **capital owner** and the **usufructuary** each establish a business relationship with the financial intermediary, both must be individually identified. The same applies if the capital owner and the usufructuary can only dispose of the property jointly. By a contrario, only the legal entity that can dispose of the property would have to be identified if it is not both of them but they establish a business relationship together. 50

g. Condominium and co-ownership associations

According to the CDB, both condominium and co-ownership associations must be identified by an entry in the land register based on an **excerpt from the land register**. If the excerpt from the protocol shows that the manager is authorized to manage the account, identification can also be based on the **excerpt from the protocol** together with a simple copy of the **regulations**. 51

h. Tenant deposit account

52 A tenant deposit account is opened by the landlord in the tenant's name for the purpose of **depositing a rent deposit**. The tenant does not have sole power of disposal over the assets deposited; he requires the landlord's consent.

53 This special form is in fact only relevant for banks. According to the CDB, the contracting party of a tenant deposit account for a rental property **in Switzerland** does not need to be identified. E contrario, for rental properties abroad, a corresponding identification must be carried out in accordance with the rules of Art. 4 CDB 20.

i. Life insurance contracts

54 In the case of insurance contracts, the person requesting the contract must be identified. If a life insurance contract is concluded by several policyholders, **all policyholders** must be identified as contracting parties. The representative, the insured person or the beneficiary is not considered to be a contracting party or a policyholder.

C. Identification of legal entities and partnerships

1. When registering

55 When the contracting party is a legal entity or a partnership, no distinction is made between the establishment of a business relationship with and without a personal meeting. Whether the persons who **opened the account were personally present** is only relevant to the way in which the identity of the persons who opened the account is verified.

56 Legal entities or partnerships registered in the **Swiss commercial register** or in an **equivalent foreign register** are to be identified by means of a register extract issued by the registrar, a written extract from a database maintained by the registry authority or a written extract from privately managed directories and databases (provided these are trustworthy).

57 For **insurance companies**, the R SRO-SVV Commentary lists the sources that are deemed equivalent to an extract from the commercial register: Publications in the Swiss Official Gazette of Commerce (SOGC), in the central business name index of the federal government (ZEFIX), a current Teledata/

Creditreform/Bisnode D&B-Print, publications and confirmations of the supervisory authorities (e.g. listing of the contracting party on the FINMA website) or confirmations of the auditors (audit certificate).

The requirements regarding the **quality of identification documents** are not the same for external asset managers, insurance companies and banks. Pursuant to Art. 48 para. 1 AMLO-FINMA, the relevant documentation must be submitted to the financial intermediary in the original or as a certified copy. Pursuant to Art. 5 R SRO-SVV, insurance companies are obliged to identify the contracting party on the basis of conclusive original documents. For banks, however, a simple copy of the identification document of legal entities and partnerships is sufficient. These statements also apply to contracting parties without an entry in the register, in accordance with the following chapter. 58

Regarding the **current validity** of the respective identification documents, we refer to our comments in Chapter II.A.4.b. (see above, N. 16 et seq.). 59

2. Without entry in the register

Legal entities and partnerships not entered in the Swiss commercial register or **an equivalent foreign register** must be identified on the basis of the articles of association, the formation documents or the formation agreement, a confirmation from the auditors, an official authorization to carry out the activity or an equivalent document; or a written extract from privately administered directories and databases (provided these are trustworthy) . 60

The financial intermediary must identify the **public authority** as a contracting party on the basis of a suitable statute or decision or on the basis of other equivalent documents or sources. 61

Regarding the **current validity** of the relevant identification documents, we refer to our comments in Chapter II.A.4.b. (see above, N. 16 ff.). 62

3. Identity of persons establishing the business relationship

If the contracting party is a legal entity or partnership, the identity of the persons who establish the business relationship on behalf of the legal entity must be verified. 63

64 The persons authorized to represent and actually acting at the time of opening the business relationship and signing the opening documents are deemed to be the **persons opening** the account. The focus here is on the natural persons who sign the documentation underlying the contractual relationship. The other persons authorized to sign for a contracting party are not to be identified, even if they are authorized to represent the contracting party vis-à-vis a financial intermediary in the context of the business relationship.

65 Compared with opening relationships with natural persons, the verification of the identity of the persons opening the account involves a **simplified form of identification**. According to the R SRO-SVV, the persons opening the account may themselves make a copy of the identification document and send it by post or electronically. According to the CDB, the actual residential address of the persons opening the account does not have to be noted or verified. Furthermore, the essential information from the identification of the persons opening the account in accordance with Art. 7, para. 1 CDB 20 does not have to be recorded and documented separately. In practice, however, financial intermediaries often do record this information anyway, particularly because the persons opening the account usually also act as authorized agents within the framework of the business relationship. If the persons establishing the business relationship should at a later date become a contracting party, they must be identified in accordance with the rules for natural persons, provided this has not already been done.

4. Power of attorney

66 If the contracting party is a legal entity, the power of attorney provisions of the legal entity are to be noted only **for the record**. This means that when the business relationship is established, the bank must inspect a list of the persons with a power of attorney or power of representation. Such a list must be copied and kept on file. The type of signing authority must also be documented, i.e. whether it is an individual or collective signing authority.

67 Art. 15 para. 3 CDB 20 only mentions "**legal entities**" and omits "partnerships", which are explicitly mentioned in para. 1. This is intentional. Para. 3 does not apply to differently organized contracting parties such as simple partnerships, general partnerships, limited partnerships or trusts.

Art. 44, para. 3 AMLO-FINMA and Art. 5, para. 3 R SRO-SVV refer to the "legal entity" or **"partnership"** as the contracting party. The requirements for external asset managers and insurance companies are therefore deliberately more extensive. 68

Persons who are authorized to act on behalf of the financial intermediary are considered to be authorized representatives. In addition to the persons opening the account, the **identity of the other** authorized representatives listed in the corresponding proof of representation does not have to be verified. 69

Typically, the provisions of the power of attorney are taken from an **extract from the commercial register** or an equivalent register. **Alternatively,** powers of attorney granted by corporate bodies to other persons, extracts from corresponding internal regulations, signature books, *certificates of incumbency* and similar documents may also be accepted, provided that they provide sufficient information about the power of attorney. This also applies to the provision of a simple copy of the relevant corporate documents (such as statutes, association regulations, minutes of the general assembly and board of directors). 70

In the case of a "**chain of representation**", all the links in the chain must be checked and documented, in particular in the case of a substitute power of attorney or if the legal entity itself is the authorized representative. 71

5. Special forms

a. Simple partnership

Simple partnerships have no legal personality, are not capable of acting, litigating or enforcing, and are not entered in the Commercial Register. 72

When a **insurance company** identifies a simple partnership, it must always identify the partners who sign the contract. 73

When entering into a business relationship with a simple partnership, **banks** and **external asset managers** may choose to identify all the partners or at least one partner, as well as the persons authorized to sign for the financial intermediary. 74

For so-called "**exclusively charitable companies**", i.e. simple partnerships whose purpose is to safeguard the interests of their members or their benefi- 75

ciaries in joint self-help or which exclusively pursue political, religious, scientific, artistic, charitable, social or similar purposes, such as Jass clubs, Guggenmusik and class funds, the CDB provides for a relaxation for banks. Only the persons authorized to sign for the bank must be identified. The charitable status and its exclusivity must be documented in a manner comprehensible to third parties, whether by means of an excerpt from the internal regulations, a meaningful website, a tax exemption certificate or similar plausible evidence.

b. Widely known company and authority

76 The financial intermediary may **refrain from** identification in the case of a widely known legal entity or partnership or an authority and instead record the fact that the identity of the contracting party is widely known.

77 Widely known companies are in particular **public limited companies** or companies directly or indirectly associated with such.

78 Swiss public-law entities are only deemed to be **public authorities** if they have a legal basis and carry out public duties. These include, in particular, federal, cantonal and municipal authorities, together with their institutions and public-law corporations. The foreign concept of authority is determined by the respective foreign law.

79 The **reasons for waiving** identification must be documented by the financial intermediary in the file in a manner comprehensible to an independent third party. There are no further formal requirements in this regard. In practice, a memorandum is drawn up and the stock exchange listing of the public company or the proof concerning the legal basis of the authority is printed out or saved.

c. Trust

80 The Swiss legal system does not have a specific substantive law of trusts. The trust has **no legal personality of its own** but is, according to the Swiss interpretation of the law, a contract between the trustee and the beneficiaries.

81 In the case of business relationships with a trust, the financial intermediary must identify the **trustee** as the contracting party, either according to the requirements for natural persons or for legal entities or partnerships. In addition, the trustee must confirm in writing that he is authorized to open a business relationship for the trust. In the case of banks, this is typically done by

means of Form T. As an alternative to this written confirmation, a so-called "**legal opinion**" is also permissible. There are no precise formal requirements here. This is usually provided by a lawyer and contains at least the same information as Form T.

In practice, the business relationship is not only opened by trustees but also by so-called "**underlying companies**". This is a domiciliary company held by a trust, the shares of which are in the trust assets. In these cases, the domiciliary companies are the contracting parties of the financial intermediary. 82

d. Company in formation

When a company, in particular an AG or GmbH, is being formed, a confirmation of the deposited share capital must be available for entry in the commercial register. In practice, the corresponding capital is deposited in a **capital contribution** or **payment account** at a bank. The account must be in the name of the company being formed and must initially be blocked. The capital may only be made available once the governing bodies have been appointed and evidence of this provided. 83

The bank must identify the **persons opening** an account for companies that are being formed. 84

After the company has been established it must be identified in accordance with the provisions for legal entities and partnerships (Art. 12 ff. VSB 20) if it becomes a contracting party of the financial intermediary. In practice, as a rule no new account is opened; instead the existing account is renamed, e.g. by deleting the suffix "in Gründung". 85

D. Delegation

1. General provisions

A financial intermediary may delegate the identification of the contracting party to third parties. This approach is of interest to the financial intermediary in practice in particular where the **third party involved (e.g. external asset manager or broker)** knows the prospective client better and therefore has more familiar access to him or has greater expertise in a geographical region. The natural person or legal entity or partnership entrusted by the financial intermediary with the identification of the contracting party, domiciled or es- 86

tablished in Switzerland or abroad, may not, as a general rule, call upon any other third parties. After the identification has been carried out by the mandated person, the financial intermediary must keep a copy of the identification documents for his records and must obtain written confirmation that the copies provided to him correspond to the originals. With regard to the identification documents received, the financial intermediary carries out a subsequent check to ensure that the third party has duly fulfilled the duties of due diligence. He checks the plausibility of the results of any additional clarifications, for example if there are doubts about the information provided regarding the identity of the contracting party. Regardless of the type of delegation, a financial intermediary remains responsible under supervisory law in all cases for the proper performance of the tasks for which he has involved the third party.

2. Types of delegation

a. Delegation with written agreement

87 A financial intermediary may, by means of a written agreement, mandate a third party to carry out the identification of the contracting party, provided that he **carefully selects** the mandated person, **instructs** the latter on his duties regarding the due identification and **monitors** the third party's compliance with the duties of due diligence during the contractual relationship. The implementing provisions do not define the criteria for careful selection. In practice, the following are checked in particular before a person is commissioned: their integrity (e.g. background check in a screening system purchased from an external provider and/or obtaining an extract from the criminal records), specialist knowledge (e.g. obtaining training certificates and/or CVs) and the possible fulfillment of specific supervisory requirements (e.g. entry in a register). In the written agreement, the financial intermediary and the mandated third party shall set out the rights and obligations underlying the delegation of identification.

b. Delegation without written agreement

88 The financial intermediary shall not be required to conclude a written agreement when delegating the identification of the contracting party provided the person appointed is an office within a **group or a group** and applies an equivalent standard of due diligence. Delegation to **other financial interme-**

diaries is also covered by this exception, provided that they are subject to equivalent regulation and supervision in relation to combating money laundering and terrorist financing and have taken measures to perform the due diligence in an equivalent manner. The client file should make it clear to an expert third party why the identification of the contracting party was carried out by an authorized person without a written agreement.

E. FINMA-RS 2016/7

1. General

The rules issued by FINMA should be as **technology-neutral** as possible to ensure fair competition between all financial market players and to avoid competitive disadvantages. 89

In order to take digital regulation into account in the fight against money laundering and terrorist financing, particularly with regard to the identification of the contracting party and the establishment of the beneficial owner when entering into a business relationship, FINMA Circular 2016/7 "Video and online identification" came into force on March 18, 2016. The objective is to interpret the duties of due diligence under AMLA and the corresponding implementing provisions, namely AMLO-FINMA, the CDB and the SRO-SIA regulations, with regard to a digital environment, with a focus on **establishing business relationships via electronic channels**. 90

FINMA-Circ. 2016/7 is directly **applied to** financial intermediaries in accordance with Art. 2 para. 2 AMLA. Where the circular makes reference to AMLO-FINMA, this also includes the analogous provisions of the CDB and the SRO-SIA regulations. FINMA Circular 2016/7 applies indirectly to financial intermediaries in accordance with Art. 2 para. 3 AMLA by reference to this circular in the corresponding SRO or AO regulations. 91

In order to avoid competitive disadvantages for Swiss financial intermediaries, enabling digital account opening is certainly to be welcomed in view of a competitive international environment. On the other hand, a purely digital process of video and online identification increases the **risk of** using falsified or counterfeit identification documents, for example. In addition, a specific infrastructure and corresponding expertise is required, which can be associated with high costs, as this is usually purchased externally. 92

93 In **practical terms**, video and online identification is a key aspect of financial services solutions that are fully digitized and are mostly offered by so-called smartphone or neobanks. Retail banks usually have video and online identification as a supplement to their range of services. For private banks, these electronic channels tend to be the exception, since the focus is on the exchange between the client advisor and the client.

2. Video identification

94 Video identification refers to the identification of the contracting party by means of **video transmission**. Such identification is equivalent to identification in the case of a personal interview, provided that the conditions set out in margin no. 6 et seq. of FINMA Circular 2016/7 are met, regardless of whether the contracting party is a natural person, a legal entity or a partnership, or whether there are several contracting parties.

95 Video transmission refers to **audiovisual communication in real time** (i.e. a live connection). The financial intermediary must use suitable technical aids for this purpose. These must, on the one hand, provide secure transmission and suitable image and audio quality. On the other hand, they must ensure that information in the machine-readable zone (MRZ) on the identification document can be read and decrypted.

96 From an **organizational point of view**, the financial intermediary must establish a process for conducting the identification meeting and draw up a discussion guide. The employees entrusted with the video identification must be trained accordingly. The meeting with the contracting party must be audio-recorded in its entirety. The recordings must be checked for quality on a random basis and stored internally in such a way that an expert third party can form a reliable judgment within a reasonable period of time.

97 The video identification of **natural persons** is governed by margin nos. 5–22 of FINMA-Circ. 2016/7. In order to verify the authenticity of the identification document, the financial intermediary must, on the one hand, electronically read and decode the information in the MRZ. On the other hand, a visually variable security feature and another randomly selected security feature must be examined. This can also be done by means of a visual check, such as tilting the ID. It follows from this that, unlike identification in the case of a personal (physical) meeting, in the case of video identification only official identifica-

tion documents can be provided that have both an MRZ and optical security features.

If there is any doubt regarding the authenticity of the identification document or the identity of the contracting party, or if the image and/or audio quality does not allow for proper identification, the video identification process will be **aborted**. In this case, the conventional identification process by means of a personal interview or by correspondence remains possible. 98

The video identification of **legal entities and partnerships** is governed by margin nos. 23–26 of FINMA-RS 2016/7, in addition to margin nos. 5–22 of FINMA-RS 2016/7, which also apply. As with conventional identification, video identification also requires an extract from a database maintained by the relevant registry authority or from a trustworthy, privately managed directory, but in electronic form. The contracting party's authorization provisions must also be acknowledged in electronic form. The identity of the persons opening the account must be verified in accordance with the requirements in margin no. 5-22 FINMA-RS 2016/7. 99

Video identification must be carried out for each contracting party individually and in accordance with the respective rules (margin nos. 5–22 FINMA-RS 2016/7 for natural persons; margin nos. 5–26 FINMA-RS 2016/7 for legal entities and partnerships), provided that a **business relationship is entered into with several contracting parties**. 100

3. Online identification

Online identification involves obtaining identification documents by **digital correspondence** and the conditions under which the identification documents obtained digitally may be treated the same as those obtained by conventional means. 101

A photocopy of the identification document produced by the contracting party is treated the same as a **simple copy of the identification document**. In order for the financial intermediary to be able to keep the photograph in its files, the contracting party sends it electronically. The main application of such an uncertified photograph of the identification document is in the simplified due diligence requirements pursuant to Article 12, para. 2 AMLO-FINMA. 102

10 3 For **equivalence with the authenticated ID copy**, FINMA Circular 2016/7 provides for three possible procedures. In all three, only official identification documents that have an MRZ and optical security features may be accepted.

10 4 The first procedure according to margin no. 32 et seq. of FINMA-Circ. 2016/7 concerns the **electronic copy of the identification document with authentication by the financial intermediary**. In this case, the financial intermediary must obtain photographs of all the relevant sides of the identification document and of the contracting party itself. These photographs must be compared with each other accordingly. Furthermore, the digitally decoded information must be checked for consistency with the remaining information on the ID card and with the data provided by the contracting party when the business relationship was established. The authenticity of the identification document must be assessed on the basis of at least two randomly selected security features. The financial intermediary shall also have the contracting party transfer money from an account held in the contracting party's name. The financial intermediary may dispense with this under the conditions set out in margin no. 33.1 of FINMA Circular 2016/7. Finally, the financial intermediary must also verify the contracting party's residential address as part of the initial procedure. The financial intermediary can do this on the basis of a tax or other official invoice, an energy, water or telephone bill (*utility bill*), a postal delivery, a public register, a database or directory maintained by a trustworthy private individual, or geolocalization.

10 5 The second procedure according to margin no. 38 f. of FINMA-Circ. 2016/7 concerns the **electronic copy of an identification document with a qualified electronic signature**. In this case, the financial intermediary must obtain an electronic copy of all the relevant pages of the identification document via an electronic channel. This image of the identification document provided by the contracting party must be provided with a qualified electronic signature in accordance with the ZertES issued by a certification service provider recognized in Switzerland. The information on the ID must be checked by the financial intermediary for consistency with that of the qualified electronic signature.

10 6 The third procedure according to margin no. 40 f. FINMA-Circ. 2016/7 concerns the **digital certificate of authenticity**. This may be created by the issuer of certificates of authenticity in accordance with Art. 49 AMLO-FINMA and sent to the financial intermediary by electronic means. If the issuer of the

confirmation of authenticity carries out the confirmation of authenticity at the address provided by the contracting party in the account opening process as their residential address, the confirmation of authenticity issued in this way simultaneously provides the confirmation of residence in accordance with Art. 45 para. 2 AMLO-FINMA. The fact that the confirmation of authenticity is carried out at this address must be evident from the documentation.

For **legal entities and partnerships**, the photographs of the person establishing the business relationship must be verified in accordance with the requirements in margin no. 32 of FINMA Circular 2016/7. In addition, margin no. 43 of FINMA Circular 2016/7 states that the financial intermediary must have the contracting party transfer money from an account held in the contracting party's name. Finally, an extract in accordance with margin no. 24 of FINMA Circular 2016/7 and the contracting party's power of attorney must be obtained. 10 7

4. Involvement of third parties

Taking **into account Articles 28 and 29 AMLO-FINMA**, the financial intermediary may mandate third parties to carry out the video and online identification. The circular emphasizes that these third parties or companies must in particular have the technical knowledge and technical means with regard to the identity documents of the countries concerned. They must provide the financial intermediary with the photographs, electronic copies, audio recordings, declarations and documentation they have created (including by electronic means) for it to keep on its files. In any case, the financial intermediary itself remains responsible under supervisory law for the proper performance of the tasks of the third parties involved. 10 8

According to Art. 28 para. 3 AMLO-FINMA, third parties called in may not in turn call in any further persons or companies. With only this wording, the frequent constellation in which a financial intermediary commissions another financial intermediary to identify the contracting party would only be possible in the analog environment. Since this would not be in line with the spirit of technology neutrality, the following explanation of Art. 28 para. 3 AMLO-FINMA was added to the table on technology neutrality under margin no. 53 of FINMA-Circ. 2016/7 as of June 1, 2021: “If a financial intermediary involves another financial intermediary and the latter carries out the video and online identification through directly commissioned service providers, the latter are 10 9

not considered to be additional persons or companies and there is no prohibited **sub-delegation**."

III. ART. 3 PARA. 2 AMLA – CASH TRANSACTIONS

11 5 A distinction must be made between (long-term) business relationships within the meaning of Art. 3 para. 1 AMLA and **one-off financial transactions**, known as cash transactions. Pursuant to Art. 3, para. 2 AMLA, financial intermediaries are only required to verify the identity of the contracting party in the case of a cash transaction if it reaches a significant threshold and the contracting party has not already been identified. The contracting party is generally the legal entity that carries out the cash transaction with the financial intermediary.

A. Definitions

1. AMLO-FINMA / CDB 20

11 6 Pursuant to Art. 2 let. b AMLO-FINMA, a cash transaction is deemed to be any **cash transaction**, in particular currency exchange, the purchase and sale of precious metals, the sale of traveler's checks, the cash payment of bearer instruments, cash and bond bonds and the cash redemption of checks, provided that no lasting business relationship is associated with these transactions. The determining factor in individual cases is not the cash settlement in the sense of a physical receipt or delivery of an asset. Rather, the execution of the one-off financial transaction must not be carried out via an existing account and must not result in any further relationship between the contracting party and the financial intermediary.

2. AMLO-SFBC

11 7 The implementing provisions for the licensed casinos sector distinguish between **land-based and online games**. In connection with both types of games, occasional financial transactions may arise that require the licensed casino to identify the player and thus its contracting party when a significant threshold is reached. The following are considered relevant one-off financial transactions in the case of land-based games: the purchase and sale of tokens to the casino; the payment of winnings from automated gambling machines; the issuing and cashing of checks; the exchange of currency and banknotes;

and in the case of online games, the deposit of funds into a player's own account in accordance with Art. 50 para. 1 VGS and the transfer of winnings and credit balances to a player's own payment account in accordance with Art. 50 para. 2 DDO.

3. AMLO-FDJP

According to Art. 2 let. b AMLO-FDJP, a cash transaction in the large-scale gambling sector includes all **cash transactions with players**, in particular the payment of gambling winnings in cash, as well as the payment of gambling winnings by bank or postal transfer, provided that no long-term business relationship is associated with these transactions. The AMLO-FDJP differentiates between cash transactions for online and non-online major games. For non-online major games, an organizer must identify the player if a payout of winnings reaches one of the specified significant thresholds. In the case of major games played online, the identification requirement applies if a player makes deposits into their own player account or transfers a significant amount from the player account to their own payment account. According to Art. 2 let. c AMLO-FDJP, a lasting business relationship exists if the organizer of the major game provides the player with an account for game credits. In the case of major games conducted online, the organizer basically provides the player with an account for game credits. Participation in a major game conducted online basically requires an account for game credits provided by the organizer. As a rule, a player account for game credits requires registration and identification of the player. Consequently, the financial transactions required under Art. 4, para. 1 AMLO-FDJP for the identification of the contracting party do not qualify as spot transactions in the strict sense. 11 8

4. AMLO-BAZG

In the banking precious metals trade, the spot transaction is the **purchase and sale of precious metals in cash**, provided that no long-term business relationship is associated with these transactions. A lasting business relationship within the meaning of the Ordinance exists if a customer relationship exists between the contracting party and a Swiss trade assay office or a Swiss group company in accordance with Art. 42bis EMKG, which is not limited to a one-time activity subject to the Ordinance. 11 9

B. Significant threshold

120 The substantial threshold values provided for in Art. 3 para. 5 AMLA in conjunction with the implementing provisions (see below, Chapter VI, N. 134 ff.) can be reached or exceeded by **one or more related transactions**. The conclusion of several spot transactions just below the substantial threshold (so-called **smurfing**) is regarded as an indication of money laundering.

C. Lack of prior identification

121 A contracting party is considered to be not already identified in a cash transaction if he **does not** have a (long-term) **business relationship** with the financial intermediary **or** has not already been properly **identified** in the case of certain **previous cash transactions**. Even if no new identification is to be carried out, the financial intermediary shall check the existing identification documentation to ensure that it is in order and to ensure that the contracting party is the person who has already been identified. In any case, however, the beneficial owners must be identified.

IV. ART. 3 PARA. 3 AMLA – INSURANCE PREMIUMS

122 Art. 3 para. 3 AMLA requires insurance institutions to verify the identity of their contracting party only if, as with cash transactions within the meaning of Art. 3 para. 2 AMLA, a significant threshold is reached or exceeded. When calculating the significant threshold, any premium deductions/surcharges must be taken into account. The basis for this calculation is either the amount of the one-time premium or, in the case of periodic premiums, the total **premium volume, including taxes**, that is owed **according to the policy**.

123 If the insurance institution suspects that the identification requirement is to be circumvented by concluding several insurance contracts or premium accounts with premium payments below the minimum limit (so-called **smurfing**), it must nevertheless identify the contracting party. Such suspicion exists if, taking into account all the circumstances, there are no identifiable legitimate reasons for taking out several life insurance policies or premium accounts.

Insurance institutions are also not required to re-identify a contracting party that has already been identified in an existing business relationship when the **scope of the business relationship** is **expanded**. 12 4

V. ART. 3 PARA. 4 AMLA – SUSPICION OF MONEY LAUNDERING

Article 3 para. 4 AMLA states that, in the cases mentioned in paras. 2 and 3, if there are **suspicious circumstances** regarding possible money laundering or terrorist financing, the contracting party must be identified even if the relevant thresholds are not reached. The risk of money laundering or terrorist financing also exists for financial transactions below the respective thresholds. 12 5

For external asset managers, this rule is explicitly **implemented in** Art. 51 para. 3 AMLO-FINMA, for banks in Art. 6 para. 2 CDB 20, and for insurance companies in Art. 3 para. 2 R SRO-SIA. AMLO-SFBC and AMLO-FDJP do not contain any explicit implementation provisions, but Art. 3 para. 4 AMLA must also be applied by casinos and organizers of major games. AMLO-BAZG explicitly states that the contracting party must be identified in any case if there are suspicions of possible money laundering or terrorist financing. 12 6

If there are grounds for suspecting money laundering or terrorist financing, the second sentence of Article 52 para. 2 AMLO-FINMA also requires the **recipient of a transfer of funds and assets** (from abroad to Switzerland) to be identified in every case. 12 7

Suspicious facts within the meaning of Article 3 para. 4 AMLA are understood to mean **concrete indications** of money laundering. These do not have to reach the level of seriousness of "well-founded suspicion" within the meaning of Article 9 para. 1quater AMLA. The materials on the right to report under Art. 305ter para. 2 SCC and the duty to report under Art. 9 para. 1 AMLA should therefore be consulted. 12 8

For the **right to report**, subordination or vague impressions are not sufficient. Indicative evidence that points to incriminated assets may be reported as "perceptions". Even one piece of evidence is enough to trigger a report; certainty is not required. In its most recent case law, the Federal Supreme Court stated the following regarding the **reporting requirement**: "If, in the context of background clarifications pursuant to Art. 6 para. 2 AMLA [...] the suspicion 12 9

cannot be dispelled, it is automatically deemed to be well-founded." In its judgment of January 11, 2021, the Federal Supreme Court also referred to the 1996 dispatch on the AMLA. It was already stipulated there that suspicions that cannot be dispelled must be reported, which is in line with the logic of the AMLA and the purpose of this law.

13 0 Art. 3, para. 4 AMLA must be considered in this context. If there is a concrete indication of money laundering, the contracting party must be identified in any case. Based on the existing suspicion, the financial intermediary must carry out appropriate background checks in accordance with **Art. 6, para. 2 AMLA**. Only if the suspicion that the assets are of criminal origin cannot be refuted, must the business relationship be reported to the Money Laundering Reporting Office. The mere existence of a suspicious fact does not directly lead to a report under Art. 9 para. 1 AMLA. The initial identification of the contracting party is intended to ensure that such a report could be made in the first place.

13 1 The **Annex to AMLO-FINMA** lists possible indications of money laundering. The list is not exhaustive and contains the following specific indications for cash transactions in nos. 3.1.1 to 3.1.8: Exchanging a large amount of banknotes (foreign and domestic) with a small nominal value for those with a large nominal value; exchanging a significant amount of money without posting it to a customer account; cashing large amounts of checks, including traveler's checks; buying or selling large quantities of precious metals on an over-the-counter basis; buying a significant amount of bank checks on an over-the-counter basis customers; transfer orders to foreign countries by walk-in customers without any apparent legitimate reason; repeated conclusion of spot transactions just below the identification limit; acquisition of bearer securities by physical delivery.

13 2 According to the **commentary R SRO-SVV**, indications of unusual activity and thus possible suspicions of money laundering may also arise during the term of the contract. This is the case, for example, if the contracting party wishes to pay in an amount of more than CHF 15,000 in cash; the economic environment or the knowledge and experience of the customer cannot be or can no longer be reconciled with the contract; the construction of the contract indicates that a criminal purpose is to be achieved; the purpose of the contract conclusion is not recognizable or appears to be economically nonsensical; the contracting party, in addition to the insurance policy; a business

relationship is entered into with asset holding entities for which no specific person is the beneficial owner, or in the case of business relationships with partnerships, trusts and domiciliary companies; or the conclusion otherwise appears unusual, unless it is recognizable as being lawful.

There are numerous indications of money laundering. The ones we know of today should not be considered exhaustive. On the contrary, new ones will constantly be added, for example, with regard to the ongoing digitalization of the business with virtual assets. According to Wyss, any suspicion of possible money laundering or terrorist financing must be taken into account. This is to be agreed. **In case of doubt**, the financial intermediary must decide in favor of the identification of the contracting party. 13 3

VI. ART. 3 PARA. 5 AMLA – AUTHORITIES DEFINING THE THRESHOLD

By introducing thresholds, the legislator is pursuing the aim of keeping the clarification and documentation effort of the financial intermediaries for certain types of financial transactions within reasonable limits. This emanation of the **principle of proportionality** is based on the assumption that the risk of money laundering is considered to be low for small sums. In accordance with Art. 3 para. 5 AMLA, the FINMA, the SROs, the SFGB, the Federal Office of Justice and Police and the FOC are responsible for determining the threshold values and their relevance in connection with Art. 3 para. 2 (cash transactions) and para. 3 AMLA (insurance premiums). 13 4

A. FINMA

Within the scope of its authority, FINMA has set the following significant thresholds: **CHF 15,000** or more for cash transactions; **CHF 5,000** or more for currency exchange transactions; **CHF 1,000** or more for occasional financial transactions with virtual currencies; **CHF 1,000** or more for transfers of funds and assets from abroad into Switzerland; and **CHF 0** if funds or assets are transferred from Switzerland out of the country. The ordinance does not provide for a period of time for calculating several interrelated transactions for the purpose of reaching the stated thresholds. 13 5

B. SBA

13 The SBA is not mentioned in Art. 3 para. 5 AMLA and is not considered a self-
6 regulatory organization within the meaning of Art. 24 et seq. AMLA. However, based on Art. 7 para. 3 FINMASA, FINMA recognizes the self-regulation of the banking sector as a minimum standard. According to Art. 4 para. 2 lit. g CDB 20, banks must identify the contracting party in the case of cash transactions involving amounts in excess of **CHF 15,000**. CDB 20 does not define a period for calculating several interrelated transactions for the purpose of reaching the threshold value.

C. SRO - Example SRO-SIA

13 The SRO-SVV is a recognized self-regulatory organization within the meaning
7 of Art. 24 et seq. AMLA. In Art. 3 para. 1 R SRO-SVV, it therefore states that, for the predominant financial transactions, a premium payment(s) of more than **CHF 15,000** triggers the identification of the contracting party. For the calculation of premiums for conventional life insurance policies with savings components and unit-linked life insurance policies, a period of five years applies to reach the stated threshold per contract.

D. ESBK

13 With regard to the identification of the contracting party, the ESBK provides
8 for a substantial threshold of **CHF 4,000** or more for various isolated financial transactions, which a player must reach within 24 hours. In the case of land-based games, the licensed casinos are free to identify and register all players, regardless of a threshold. The reasons for such a procedure in practice are in particular the relief of the transaction monitoring (e.g. elimination of the verification of thresholds or of "smurfing" to circumvent possible identification measures) as well as the implementation of social protection measures (e.g. gambling addiction or avoidance of the participation of minors).

E. FDJP

13 For **non-online major games**, the level of the substantial thresholds is gen-
9 erally based on the method of participation in the major game. The FDJP therefore defines the significant thresholds for cash transactions for **non-online major games** as follows: prize payments of CHF 5,000 or more for elec-

tronic tickets, CHF 10,000 or more for printed tickets, and CHF 15,000/25,000 or more for all other non-online major games. The same thresholds apply to large-scale online games over a thirty-day calculation period, even though the financial transactions that identify the contracting party do not usually constitute cash transactions in the strict sense. The amount of the significant thresholds for major games played online varies depending on the type of transaction (incoming vs. outgoing payments from the player account), the percentage of stakes in a period of 30 days in major games with a certain payout ratio or the circumstance of whether the winnings are game winnings or not.

F. BAZG

The BAZG set the thresholds as follows within the scope of its competence: **CHF 15,000** or more for cash transactions; **CHF 5,000** or more for foreign exchange transactions; **CHF 1,000** or more for virtual currency transactions, provided that these are not asset transfers and are not associated with a lasting business relationship; **CHF 1,000** or more for asset transfers from abroad to Switzerland; and **CHF 0** if asset transfers are made from Switzerland abroad. The ordinance does not provide for a period of time for calculating several related transactions for the purpose of reaching the significant thresholds mentioned. 140

VII. SANCTIONING OF VIOLATIONS OF THE IDENTIFICATION REQUIREMENT

A. FINMASA, AMLA, AMLO-FINMA

The supervisory authorities under special legislation fulfil their tasks by imposing sanctions and also pursue their supervisory and strategic objectives. Combating money laundering is one of **FINMA's** strategic objectives. 141

If there are indications of irregularities or violations of the law, FINMA first conducts informal **preliminary clarifications**. Such indications may arise from FINMA's supervisory activities (e.g. its own on-site inspections or audit reports by audit firms). Reports from third-party authorities, complaints from clients or media reports may also trigger preliminary clarifications. In addition, supervised institutions and audit firms must immediately report to FIN- 142

MA any incidents that are of material significance for supervision. In connection with the duty of identification under Article 3 AMLA, it should also be noted that the CDB Supervisory Board and the respective AOs and SROs report violations and decisions to FINMA.

14 3 If there are indications of violations of supervisory law, FINMA will open **enforcement proceedings**. These are conducted in accordance with the APA, which regulates both the first-instance proceedings before FINMA and the appeal proceedings before the Federal Administrative Court. Enforcement contributes to the achievement of supervisory and strategic objectives and aims to eliminate abuses, restore compliance with the law and sanction violations in a way that also acts as a deterrent. It is used in a targeted manner for serious violations of supervisory law.

14 4 A **serious violation of supervisory law** with regard to Article 3 AMLA is determined according to the criteria for the opening of enforcement proceedings and FINMA Circular 2013/3. The assessment of the severity of the violation of Article 3 AMLA can be divided into the case groups "systematic errors" and "individual cases". A systematic violation of Art. 3 AMLA constitutes a serious violation of a regulatory provision. This may include, for example, the circumstance that video identifications carried out over a period of months are no longer traceable or no longer available due to poor data quality or other IT problems. In contrast, a one-time, isolated and minor violation of financial market obligations is generally not sufficient to open enforcement proceedings. However, a one-time violation of a central obligation, such as the duty to provide information in accordance with Art. 29 FINMASA, can result in enforcement proceedings. The duty to identify in accordance with Art. 3 AMLA also represents such a central due diligence obligation. For example, failure to carry out identification in the case of a cash transaction despite obvious suspicions of possible money laundering or terrorist financing. Or consciously ignoring doubts about the identity of the contracting party and not clarifying them further. In individual cases, the intensity of the breach of duty and the significance of the disregarded duties are taken into account. Ultimately, FINMA uses its discretion to decide whether a serious violation has occurred. This allows it to define this vague legal term.

14 5 Art. 30 et seq. FINMASA lists the following **supervisory instruments** that FINMA can use to address violations of the obligations under the AMLA: restoration of a proper state of affairs in accordance with Art. 31 FINMASA;

determination of serious violations of supervisory law by means of a ruling and substitute performance in accordance with Art. 32 FINMASA; professional ban of up to five years in accordance with Art. 33 FINMASA; temporary or permanent ban on activities in accordance with Art. 33a FINMASA; publication of the legally binding final ruling, stating personal data in accordance with Art. 34 FINMASA; confiscation of unlawfully obtained gains or avoided losses in accordance with Art. 35 FINMASA; appointment of an independent and expert investigating agent in accordance with Art. 36 FINMASA; and withdrawal of the license, recognition, admission or registration in accordance with Art. 37 FINMASA. Any violation of the law is sufficient only for the "restoration of the proper state of affairs"; otherwise, all of the above-mentioned supervisory instruments require a serious violation of supervisory provisions.

The only violations of the **AMLA** that are penalized are the violation of the reporting requirement in accordance with Art. 9 in conjunction with Art. 37 AMLA and the violation of the duty of inspection by dealers in accordance with Art. 15 in conjunction with Art. 38 AMLA. Violations of the other due diligence and conduct requirements under Article 3 et seq. AMLA are not penalized. 146

Under Article 9 para. 1 AMLO-FINMA, a violation of the provisions of the **AMLO-FINMA** may call into question the guarantee of proper business conduct required of the financial intermediary. For financial intermediaries subject to prudential supervision by FINMA, this possibility of sanction already arises from the general licensing requirements; see Art. 3 para. 2 let. c BankG for banks and Art. 14 para. 1 VAG for insurance companies. Serious violations can, according to Art. 9 para. 2 AMLO-FINMA, result in a ban from the profession under Art. 33 FINMASA and the confiscation of the profits gained from the violations under Art. 35 FINMASA. Regarding the ban from the profession, it should be noted that the "person responsible for the violation" can be banned from "an activity in a leading position". The person concerned is not therefore required to have held a management position at the time of their misconduct. 147

B. CDB

If banks domiciled in Switzerland sign up to the CDB, they are subject not only to the supervisory sanctions system under Art. 30 et seq. FINMASA, they 148

are also subject to the **monetary sanctions system** set out in Art. 58 ff. CDB 20. This is a civil law system.

149 If breaches of contract are suspected, the CDB **investigating agent** conducts the necessary investigations and submits a proposal to the CDB supervisory board for the instigation of sanctions proceedings or for the full or partial dismissal of the proceedings. In straightforward cases, the bank can request an abbreviated procedure by means of a **self-report**. To do this, it must submit the complete files and a report from the audit firm, in which case the investigation procedure is omitted and only the sanction procedure is carried out.

150 The **CDB Supervisory Commission** is responsible for investigating and punishing violations of the code of conduct. It determines the appropriate penalty in the sanctioning procedure or dismisses the procedure in whole or in part.

151 The CDB sanctioning provisions distinguish between minor cases and non-minor cases of violations of the code of conduct. A case is generally deemed to be a **minor case** if the CDB's anti-money laundering purpose has been achieved despite formal deficiencies. Art. 63 CDB 20 lists some non-exhaustive examples. If the case is a minor one, the proceedings against the bank at fault are to be closed without sanction.

152 A systemic failure on the part of the bank does not constitute a trivial case. A breach of the code of conduct may also be a matter of a merely different interpretation of the relevant CDB provision(s). In the event of a breach of the code of conduct, the bank at fault may be subject to a **contractual penalty** of up to ten million francs. The following must be taken into account when calculating the penalty: the severity of the violation of the CDB provision(s), the degree of fault, the financial situation of the bank and the measures imposed by other instances in the same case. Art. 68 CDB 20 provides for arbitration in the event of non-payment of the imposed penalty. The decisions of the court of arbitration may be appealed under Art. 389 et seq. CPC.

153 The CDB Supervisory Board informs **FINMA** of its decisions. The audit firm must also report to FINMA any violations of the CDB rules of professional conduct that are not to be classified as minor cases (as well as to the CDB Supervisory Board). The facts reported to FINMA may include not only violations of the provisions of the CDB but also violations of other supervisory and criminal law provisions.

C. SRO – example SRO-SIA

The SRO-SIA has the task of ensuring that the affiliated insurance companies comply with the statutory and regulatory due diligence requirements. To this end, it issues a special **KPS SRO-SVV** based on Art. 10 of its own statutes and in consultation with FINMA, in which it defines the necessary internal and external control procedures, the system of sanctions and the legal remedies. The obligation to issue corresponding regulations arises from Art. 25 AMLA. 15 4

In the event of a breach of the duties under the AMLA and/or the SRO-SIA regulations, the SRO-SIA board is obliged to take the necessary measures to **restore compliance with the law**. The offending insurance company is given a legal hearing before such a decision is made. 15 5

In addition, the SRO-SIA board may decide on sanctions. It may issue a **written warning** or impose a **fine** of up to one million francs. Such fines are collected and may be donated in whole or in part to charitable organizations. SRO-SIA sanctions are private in nature and may be challenged in arbitration. The legal remedies set out in Art. 389 et seq. of the Swiss Code of Civil Procedure (CPC) apply to the decisions of the arbitral tribunal. 15 6

D. External asset managers and trustees

With the FinIA, which came into force on January 1, 2020, external asset managers and trustees must be licensed by FINMA and join a **supervisory organization (SO)** approved by FINMA. They are considered prudentially supervised financial intermediaries in accordance with Art. 2 para. 2 lit. a^{bis} AMLA. With the prudential supervision, the AO also assumes the monitoring tasks in accordance with AMLA. 15 8

Violations of laws, ordinances and regulations by the affiliated are primarily clarified and investigated by the AO. The AO can order appropriate **measures**, such as setting deadlines for the restoration of compliance with the law and regulations, sending a request for a supervisory meeting, imposing conditions of a personnel or organizational nature, setting deadlines for regular reporting on certain events or facts. A report is made to FINMA if the measures ordered by the AO are disregarded by the affiliates (deadlines pass unused, the supervisory meeting is refused, etc.). Serious violations are reported immediately to FINMA. 15 9

160 However, the **sanctioning authority** remains with FINMA. If the AO discovers violations of supervisory law in the course of its ongoing supervision, FINMA imposes sanctions in accordance with the supervisory instruments available to it pursuant to Art. 30 et seq. FINMASA. An appeal against a FINMA ruling may be lodged with the Federal Administrative Court in accordance with APA.

The comments presented here only reflect the interpretations and views of the authors. No conclusions can be drawn regarding the practices of the authors employers.

BIBLIOGRAPHY

Basse-Simonsohn Detlev Michael, Geldwäschereibekämpfung und organisiertes Verbrechen, Berner Bankrechtliche Abhandlungen Band 11, Bern 2002.

Blattner-Schmutz Nadine/Meyer Patrick K., Vorbemerkungen zu Art. 3 GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Brunner Genevieve, Der Tod des Bankkunden, Zürich 2011.

Cincelli Roman, Der Common Law Trust – Grundlagen, rechtvergleichende Entwicklung und Rezeptionsmöglichkeiten aus Sicht der Schweiz, Diss., Zürich 2017.

De Capitani Werner, Geldwäschereigesetz (GwG), Einleitung zu Kapitel 2: Die Pflichten der Finanzintermediäre, in: Schmid Niklaus (Hrsg.), Kommentar Einziehung, Organisiertes Verbrechen, Geldwäscherei, Band II, Zürich 2002 (zitiert: OK-II-De Capitani, GwG Einl. 2. Kap. N. X).

De Capitani Werner, Geldwäschereigesetz (GwG), Kommentierung zu Art. 3 GwG, in: Schmid Niklaus (Hrsg.), Kommentar Einziehung, Organisiertes Verbrechen, Geldwäscherei, Band II, Zürich 2002 (zitiert: OK II-De Capitani, GwG 3 N X).

Dobrauz-Saldapenna Günther/Derungs Corsin, Kommentierung zu Art. 3 GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Geldwäschereigesetz (GwG), Stämpflis Handkommentar, Bern 2017.

Eymann Patric, V. Enforcementverfahren der FINMA / 26. Eröffnung des Verfahrens und Kriterien dazu, in: Zulauf Urs/Wyss David (Hrsg.), Finanzmarktenforcement - Verfahren zur Durchsetzung des Schweizer Finanzmarktrechts, 3. Aufl., Bern 2022, S. 105–107.

Graber Christoph K., Kommentierung zu Art. 3 GwG, in: Graber Christoph K./ Oberholzer Dominik (Hrsg.), Das Neue Geldwäschereigesetz, Gesetzesausgabe mit englischer Übersetzung, Ausführungserlassen und Anmerkungen, 3. Aufl., Zürich et al. 2009.

Heim Kathrin/Wettstein Tamara, VSB 2020, Praxiskommentar zur Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken, 4. Aufl., Zürich 2019.

Hsu Peter Ch./Bahar Rashid/Flühmann Daniel, Kommentierung zu Art. 33 FINMAG, in: Watter Rolf/ Bahar Rashid (Hrsg.), Finanzmarktaufsichtsgesetz/ Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

Kuhn Christoph, Das Berufsverbot nach Art. 33 FINMAG, Zürich 2015 (zitiert: Kuhn, Berufsverbot, S. X).

Kuhn Christoph, XIV. Massnahmen der FINMA, in: Zulauf Urs/Wyss David (Hrsg.), Finanzmarktenforcement - Verfahren zur Durchsetzung des Schweizer Finanzmarktrechts, 3. Aufl., Bern 2022, S. 370–403 (zitiert: Kuhn, Finanzmarktenforcement, S. X).

Kuhn Christoph/Wyss David, XIV. Massnahmen der FINMA, in: Zulauf Urs/ Wyss David (Hrsg.), Finanzmarktenforcement - Verfahren zur Durchsetzung des Schweizer Finanzmarktrechts, 3. Aufl., Bern 2022, S. 351–359.

Kuster Matthias, Zur Abgrenzung des Melderechts nach Art. 305er Abs. 2 StGB von der Meldepflicht nach Art. 9 GwG, in: Jusletter 26.6.2017.

Landolt Kaspar/Gemperli Dominique Lea, Kommentierung zu Art. 3 GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar zum Geldwäschereigesetz, Basel 2021.

Meier-Hayoz Arthur/Forstmoser Peter, Schweizerisches Gesellschaftsrecht - Mit neuem Aktien- und Handelsregisterrecht, 13. Aufl., Bern 2023.

Müller Thomas / Lötscher Matthias, Kommentierung zu Art. 6 GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar zum Geldwäschereigesetz, Basel 2021.

Rayroux François/du Pasquier Shelby, Kommentierung zu Art. 22 FINMAG, in: Watter Rolf/Bahar Rashid (Hrsg.), Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

Schönknecht Florian, IV. Vorabklärungen im FINMA-Enforcement, in: Zulauf Urs/Wyss David (Hrsg.), Finanzmarktenforcement - Verfahren zur Durchsetzung des Schweizer Finanzmarktrechts, 3. Aufl., Bern 2022, S. 65–92.

Strasser Othmar, Die Delegation von Sorgfaltspflichten gemäss Geldwäschereigesetz durch eine Bank, in: Waldburger Robert/Baer Charlotte M./Nobel Ursula/Bernet Benno (Hrsg.), Wirtschaftsrecht zu Beginn des 21. Jahrhunderts, Festschrift für Peter Nobel zum 60. Geburtstag, Bern 2005, S. 651–680.

Taube Tamara, Entstehung, Bedeutung und Umfang der Sorgfaltspflichten der Schweizer Banken bei der Geldwäschereiprävention im Bankenalltag, St. Galler Schriften zum Finanzmarktrecht Band 9, Zürich/St. Gallen 2013.

Tanner André, Der bankinterne Compliance Officer, in: Jusletter 30.9.2019 (zitiert: Tanner, Compliance Officer, S. X).

Tanner Kathrin, XIX. Rechtsmittel gegen Verfügungen der FINMA, in: Zulauf Urs/Wyss David (Hrsg.), Finanzmarktenforcement - Verfahren zur Durchsetzung des Schweizer Finanzmarktrechts, 3. Aufl., Bern 2022, S. 528–541 (zitiert: Tanner, Finanzmarktenforcement, S. X).

Wyss Ralph, Kommentierung zu Art. 3 GwG, in: Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), GwG Kommentar (AMLA Commentary), Schweizerisches Geldwäschereigesetz mit weiteren Erlassen (Swiss Anti-Money Laundering Act with other Laws), 3. Aufl., Zürich 2019.

Zulauf Urs/Wyss David, III. Finanzmarktenforcement der FINMA – Übersicht / 11. Enforcementverfahren als Verwaltungsverfahren, in: Zulauf Urs/Wyss David (Hrsg.), Finanzmarktenforcement - Verfahren zur Durchsetzung des Schweizer Finanzmarktrechts, 3. Aufl., Bern 2022, S. 33–36.

Zulauf Urs, Gläubigerschutz und Vertrauensschutz: zur Sorgfaltspflicht der Bank im öffentlichen Recht der Schweiz, in: Zeitschrift für schweizerisches

Recht, 1994, S. 359–535 (zitiert: Zulauf, Gläubiger- und Vertrauensschutz, S. X).

Zulauf Urs, II. Grundlagen des Finanzmarktenforcement, in: Zulauf Urs/Wyss David (Hrsg.), Finanzmarktenforcement - Verfahren zur Durchsetzung des Schweizer Finanzmarktrechts, 3. Aufl., Bern 2022, S. 13–29 (zitiert: Zulauf, Finanzmarktenforcement, S. X).

MATERIALS

Aufsichtskommission VSB, Tätigkeitsbericht der Aufsichtskommission zur Sorgfaltspflicht der Banken 1990–1992, abrufbar unter https://www.swissbanking.ch/de/themen/regulierung-compliance/geldwaeschereibekaempfung, besucht am 4.9.2024.

Aufsichtskommission VSB, Tätigkeitsbericht der Aufsichtskommission zur Sorgfaltspflicht der Banken 1992–1994, abrufbar unter https://www.swissbanking.ch/de/themen/regulierung-compliance/geldwaeschereibekaempfung, besucht am 4.9.2024.

Aufsichtskommission VSB, Tätigkeitsbericht der Aufsichtskommission zur Sorgfaltspflicht der Banken 1995–1997, abrufbar unter https://www.swissbanking.ch/de/themen/regulierung-compliance/geldwaeschereibekaempfung, besucht am 4.9.2024.

Aufsichtskommission VSB, Tätigkeitsbericht der Aufsichtskommission zur Sorgfaltspflicht der Banken 1998–2001, abrufbar unter https://www.swissbanking.ch/de/themen/regulierung-compliance/geldwaeschereibekaempfung, besucht am 4.9.2024.

Aufsichtskommission VSB, Tätigkeitsbericht der Aufsichtskommission zur Sorgfaltspflicht der Banken 2005–2010, abrufbar unter https://www.swissbanking.ch/de/themen/regulierung-compliance/geldwaeschereibekaempfung, besucht am 4.9.2024.

Aufsichtskommission VSB, Tätigkeitsbericht der Aufsichtskommission zur Sorgfaltspflicht der Banken 2011–2016, abrufbar unter https://www.swissbanking.ch/de/themen/regulierung-compliance/geldwaeschereibekaempfung, besucht am 4.9.2024.

Aufsichtskommission VSB, Praxis der Aufsichtskommission zur Sorgfaltspflicht der Banken, 1.1.–30.6.2017, abrufbar unter https://www.swissbanking.ch/de/themen/regulierung-compliance/geldwaeschereibekaempfung, besucht am 4.9.2024.

Aufsichtskommission VSB, Praxis der Aufsichtskommission zur Sorgfaltspflicht der Banken, 1.1.–30.6.2018, abrufbar unter https://www.swissbanking.ch/de/themen/regulierung-compliance/geldwaeschereibekaempfung, besucht am 4.9.2024.

Aufsichtskommission VSB, Praxis der Aufsichtskommission zur Sorgfaltspflicht der Banken, 1.7.–31.12.2018, abrufbar unter https://www.swissbanking.ch/de/themen/regulierung-compliance/geldwaeschereibekaempfung, besucht am 4.9.2024.

Aufsichtskommission VSB, Praxis der Aufsichtskommission zur Sorgfaltspflicht der Banken, 1.1.–30.6.2019, abrufbar unter https://www.swissbanking.ch/de/themen/regulierung-compliance/geldwaeschereibekaempfung, besucht am 4.9.2024.

Aufsichtskommission VSB, Praxis der Aufsichtskommission zur Sorgfaltspflicht der Banken, 1.7.–31.12.2020, abrufbar unter https://www.swissbanking.ch/de/themen/regulierung-compliance/geldwaeschereibekaempfung, besucht am 4.9.2024.

Aufsichtskommission VSB, Praxis der Aufsichtskommission zur Sorgfaltspflicht der Banken, 1.1.–30.6.2021, abrufbar unter https://www.swissbanking.ch/de/themen/regulierung-compliance/geldwaeschereibekaempfung, besucht am 4.9.2024.

Aufsichtskommission VSB, Praxis der Aufsichtskommission zur Sorgfaltspflicht der Banken, 1.7.–31.12.2022, abrufbar unter https://www.swissbanking.ch/de/themen/regulierung-compliance/geldwaeschereibekaempfung, besucht am 4.9.2024.

Aufsichtskommission VSB, Praxis der Aufsichtskommission zur Sorgfaltspflicht der Banken, 1.1.–30.6.2023, abrufbar unter https://www.swissbanking.ch/de/themen/regulierung-compliance/geldwaeschereibekaempfung, besucht am 4.9.2024.

Aufsichtsorganisation AOOS - Schweizerische Aktiengesellschaft für Aufsicht, Reglement der Aufsichtsorganisation nach Finanzinstituts- und Finanzmarktaufsichtsgesetz vom 1.1.2023, abrufbar unter www.aoos.ch/dataset/file/7653-20230306-aoos-ao-reglement-pdf, besucht am 4.9.2024.

Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor vom 17.6.1996, BBI 1996 III S. 1101 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1996/3_1101_1057_993/de, besucht am 4.9.2024.

Botschaft zur Umsetzung der revidierten Empfehlungen der Group d'action financière (GAFI) vom 15.6.2007, BBI 2007 S. 6269 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2007/938/de, besucht am 4.9.2024.

Botschaft über die Änderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes (Revision des Einziehungsrechts, Strafbarkeit der kriminellen Organisation, Melderecht des Financiers) vom 30.6.1993, BBl 1993 III 277 ff., abrufbar unter www.fedlex.admin.ch/eli/fga/1993/3_277_269_193/de, besucht am 4.9.2024.

Botschaft zum Finanzdienstleistungsgesetz (FIDLEG) und zum Finanzinstitutsgesetz (FINIG) vom 4.11.2015, BBl 2015 8901 ff., abrufbar unter www.fedlex.admin.ch/eli/fga/2015/2141/de, besucht am 4.9.2024.

Casino Zürichsee AG, Allgemeine Geschäftsbedingungen für die Nutzung des Spielangebots auf der Spielplattform, abrufbar unter: https://online.swisscasinos.ch/agb, besucht am 4.9.2024.

EJPD, Erläuterungsbericht des Eidgenössischen Justiz- und Polizeidepartements zu den Verordnungen zum Geldspielgesetz (VGS, SPBVEJPD, GwV-EJPD) vom 22.10.2018, abrufbar unter www.esbk.admin.ch/esbk/de/home/rechtsgrundlagen/gesetzgebung.html, besucht am 4.9.2024.

ESBK, Tätigkeitsbericht 2022 vom 6.2023, abrufbar unter: https://www.esbk.admin.ch/esbk/de/home/publiservice/publikationen.html, besucht am 4.9.2024.

FATF, Anti-money laundering and counter-terrorist financing measures - Switzerland, Fourth Round Mutual Evaluation Report, 2016, Paris, abrufbar unter https://www.fatf-gafi.org/content/dam/fatf-gafi/images/mer/mer-switzerland-2016.pdf.coredownload.inline.pdf, besucht am 4.9.2024.

FINMA, Erläuterungsbericht zur Zusammenführung der Geldwäschereiverordnungen der FINMA vom 8.6.2010, abrufbar unter https://www.finma.ch/de/dokumentation/archiv/abgeschlossene-anhoerungen/2010/, besucht am 4.9.2024.

FINMA, Erläuterungsbericht zur Totalrevision der GwV-FINMA vom 11.2.2015, abrufbar unter https://www.finma.ch/de/dokumentation/archiv/abgeschlossene-anhoerungen/2015/, besucht am 4.9.2024.

FINMA, Erläuterungsbericht zur Teilrevision der GwV-FINMA vom 8.3.2022, abrufbar unter https://www.finma.ch/de/dokumentation/archiv/abgeschlossene-anhoerungen/2022/, besucht am 4.9.2024.

FINMA, Erläuterungsbericht zum Rundschreiben 2016/7 «Video- und Online-Identifizierung» vom 21.12.2015, abrufbar unter www.finma.ch/de/dokumentation/archiv/abgeschlossene-anhoerungen/2016/, besucht am 4.9.2024.

FINMA, Erläuterungsbericht zum Rundschreiben 2016/7 «Video- und Online-Identifizierung» vom 13.2.2018, abrufbar unter www.finma.ch/de/dokumentation/archiv/abgeschlossene-anhoerungen/2018/, besucht am 4.9.2024.

FINMA, Erläuterungsbericht zum Rundschreiben 2016/7 «Video- und Online-Identifizierung» vom 16.11.2020, abrufbar unter www.finma.ch/de/dokumentation/archiv/abgeschlossene-anhoerungen/2020/, besucht am 4.9.2024.

FINMA, Jahresbericht 2017, abrufbar unter https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/geschaeftsbericht/20180327-jahresbericht-2017.pdf, besucht am 4.9.2024.

FINMA, Leitlinien zum Enforcement vom 25.9.2014, abrufbar unter www.finma.ch/de/finma/taetigkeiten/leitlinien/, besucht am 4.9.2024.

FINMA, Liste der aktuell anerkannten Selbstregulierungen, abrufbar unter: https://www.finma.ch/de/dokumentation/selbstregulierung/anerkannte-selbstregulierung/, besucht am 4.9.2024.

FINMA, Liste der aktuell bewilligten Selbstregulierungsorganisationen, abrufbar unter: https://www.finma.ch/de/bewilligung/selbstregulierungsorganisationen-sro/, besucht am 4.9.2024.

FINMA, Strategische Ziele 2021 bis 2024, abrufbar unter www.finma.ch/de/finma/ziele/strategische-ziele/, besucht am 4.9.2024.

Grand Casino Kursaal Bern AG, Allgemeine Geschäftsbedingungen, abrufbar unter: https://www.grandcasino-bern.ch/de/uebersicht-komponenten/startseite/agb, besucht am 4.9.2024.

Kontrollstelle für die Bekämpfung der Geldwäscherei, Praxis zu Art. 2 Abs. 3 GwG vom 29. Oktober 2008, abrufbar unter: www.finma.ch/FinmaArchiv/gwg/d/dokumentationen/publikationen/gwg_auslegung/pdf/59402.pdf, besucht am 4.9.2024.

Motion 86.956 vom 10.10.1986, Leuenberger Moritz, Bankengesetz. Priorität für Teilrevision, abrufbar unter: https://entscheidsuche.ch/docs/CH_VB/CH_VB_001_86-956_1987-03-20.pdf, besucht am 4.9.2024.

Rundschreiben 2011/1, Tätigkeit als Finanzintermediär nach GwG, Ausführungen zur Geldwäschereiverordnung (GwV), siehe online unter: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2011-01-01-01-2017.pdf?sc_lang=de&hash=C13E76F1B7CE20DFB9B822526B383187, besucht am 4.9.2024.

Rundschreiben 2013/3, Prüfwesen, siehe online unter: www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2013-03-20221207.pdf, besucht am 4.9.2024.

Rundschreiben 2016/7, Video- und Online-Identifizierung, Sorgfaltspflichten bei der Aufnahme von Geschäftsbeziehungen über digitale Kanäle, siehe online unter: www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2016-07-20210506.pdf, besucht am 4.9.2024.

Schweizerische Bankiervereinigung, Kommentar zur Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken (VSB 20) vom 13.6.2018, abrufbar unter https://www.swissbanking.ch/de/downloads, besucht am 4.9.2024.

Schweizerischer Versicherungsverband, Kommentar zum Reglement der Selbstregulierungsorganisation zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung vom 12.2019, abrufbar unter https://www.sro-svv.ch/de/regelwerk/kommentar-zum-reglement-sro-svv, besucht am 18.12.2024.

Schweizerischer Versicherungsverband, Kontroll-, Prüf und Sanktionsreglement der SRO-SVV vom 1.1.2017, abrufbar unter https://www.sro-svv.ch/images/pdf/de_regelwerk/KPS_SRO-SVV.pdf, besucht am 4.9.2024.

Schweizerischer Versicherungsverband, Statuten SRO-SVV vom 21.8.2020, abrufbar unter https://www.sro-svv.ch/images/pdf/de_regelwerk/Statuten_SRO-SVV.pdf, besucht am 4.9.2024.

Swisslos Interkantonale Landeslotterie, Bedingungen für die Online-Teilnahme vom 13.1.2025, abrufbar unter: https://www.swisslos.ch/media/de/swisslos/teilnahmebedingungen/bedingungen-f%C3%BCr-die-online-teilnahme.pdf, besucht am 4.9.2024.

Tanner André/von Rotz Madeleine, Kommentierung zu Art. 305ter StGB, in: Lehmkuhl Marianne Johanna/Wenk Jan (Hrsg.), Onlinekommentar zum Schweizerischen Strafgesetzbuch – Version: 13.08.2024: https://onlinekommentar.ch/de/kommentare/stgb305ter, besucht am 4.9.2024, DOI: 10.17176/20240813-190118-0.

Zentralamt für Edelmetallkontrolle, Richtlinie R-249, Weisungen zur Geldwäschereiverordnung-BAZG inkl. Prüfanweisungen vom 1.5.2024, abrufbar unter: www.bazg.admin.ch/bazg/de/home/dokumentation/richtlinien/r-249_weisungen_geldwaeschereiverordnung-bazg.html, besucht am 4.9.2024.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 7 AMLA

A commentary by Martin Peyer / Orlando Battaglia

SUGGESTED CITATION

Martin Peyer/Orlando Battaglia, Commentary of art. 7 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Peyer/Battaglia, art. 7 AMLA N. XXX

Art. 7 Duty to keep records

[1] The financial intermediary must keep records of transactions carried out and of clarifications required under this Act in such a manner that other specially qualified persons are able to make a reliable assessment of the transactions and business relationships and of compliance with the provisions of this Act.

[1bis] The financial intermediary must periodically check the required records to ensure that they are up to date, and update them if need be. The periodicity, scope and type of checking and updating are based on the risk posed by the customer.

[2] The financial intermediary must retain the records in such a manner as to be able to respond within a reasonable time to any requests made by the prosecution authorities for information or for the seizure of assets.

[3] After the termination of the business relationship or after completion of the transaction, the financial intermediary must retain the records for a minimum of ten years.

CONTENT

I. INTRODUCTION 208
A. Purpose of the provision 208
B. History 208
C. Specification of the documentation requirement in other enactments 209
II. DOCUMENTATION OBLIGATION (PARAS. 1) 209
A. Preliminary remarks 209
B. Addressees 210
C. Subject matter and scope of the documentation requirement 210
D. Supporting documents 211
E. Comprehensibility by knowledgeable third parties 213
F. Point in time 213
III. PERIODIC REVIEW AND UPDATING (PARAS. 1BIS) 214
A. Criticism by the FATF as the reason for the insertion 214
B. Regular updating obligation 215
C. Risk-based approach 216
1. Basic principle 216
2. Scope 216
3. Frequency 217
4. Type of review 218
D. Event-driven updating obligation 218
IV. READINESS TO PROVIDE INFORMATION AND HAND OVER DOCUMENTS (PAR. 2) 218
A. Preliminary remarks 218
B. Requests for information and seizure by criminal prosecution authorities 219
C. Compliance within a reasonable period of time 221
D. Requirements for storage 221
V. RETENTION PERIOD (PAR. 3) 222
VI. APPLICATION ISSUES 223
A. Possibility and limits of delegation 223
B. Compliance with the documentation requirement for AI applications 224
VII. LEGAL CONSEQUENCES OF A VIOLATION 224
A. Preliminary remarks 224
B. Supervisory consequences 224
C. Criminal law consequences 225
D. Civil law consequences 226
VIII. Outlook 226
Bibliography 227
Materials 228

I. INTRODUCTION

A. Purpose of the provision

1 The documentation requirement under Art. 7 para. 1 AMLA is one of the provisions of the Act that governs the due diligence obligations of financial intermediaries. The documentation requirement, which applies to all financial intermediaries (see Art. 8a para. 1 lit. c AMLA in relation to dealers), **has several purposes**. Firstly, it is intended to create a basis on which the supervisory authorities and external auditors can verify whether financial intermediaries are fulfilling their due diligence obligations and thus complying with the provisions of the AMLA. Second, the documentation requirement helps law enforcement agencies investigate potentially criminal acts related to money laundering by giving them access, if needed, to the information that financial intermediaries have gathered from transactions and investigations. And thirdly, it serves the obligated financial intermediaries themselves, enabling them to defend themselves against any allegations of negligence under Art. 305ter para. 1 SCC. Furthermore, the documentation requirement also compels financial intermediaries to create the necessary written documentation to enable them to make well-founded and justified decisions even in the case of risky transactions.

2 The **relevance of the documentation requirement in practice** is also evident from the annual reports published by MROS. In connection with the clarification of what constitutes "evidence" (see below, n. 13 ff.), MROS emphasizes, for example, that it is difficult or impossible for it to fulfill its duty to analyze incoming suspicious activity reports and investigate the reported transactions if the documentation provided by financial intermediaries is inadequate. However, if financial intermediaries comply with their documentation requirements, this makes the MROS's work "considerably easier."

B. History

3 With the exception of para. 1bis, Art. 7 AMLA was already included in the law with the same wording when it **came into force in 1998**. Para. 1bis was added as part of the revision of the AMLA to implement the most important recommendations from the fourth country report of the FATF in order to remedy what the FATF had identified as a significant deficiency, namely the lack of a

general and explicit obligation on financial intermediaries to ensure that the information obtained remains accurate and relevant throughout the course of the business relationship. The new para. 1bis (see n. 23 ff. below) entered into force on January 1, 2023.

C. Specification of the documentation requirement in other enactments

As a **framework law**, the AMLA only regulates the documentation obligation in broad terms. Depending on the type of financial intermediary, further regulations exist at the ordinance level (GwV-FINMA, GwV-ESBK, GwV-EJPD and GwV-BAZG; for dealers, the relevant regulations can be found in the GwV), in the VSB and in the regulations of the SROs. In this context, the Federal Supreme Court has explicitly stated, for example in relation to Art. 61 para. 2 GwV-FINMA (in the version of 2010), that this is a (technical) clarification of Art. 7 AMLA. 4

II. DOCUMENTATION OBLIGATION (PARAS. 1)

A. Preliminary remarks

The documentation requirement stipulates that the financial intermediary must prepare documentation on the transactions carried out and on the clarifications required under the AMLA in such a way that knowledgeable third parties can form a reliable opinion on the transactions and business relationships as well as on compliance with the provisions of the AMLA (Art. 7 para. 1 AMLA). In this context, industry- and activity-specific differences arise from the applicable **implementing provisions**. For example, in addition to general requirements in Art. 22 GwV-FINMA, GwV-FINMA also lays down special provisions for banks and securities firms (Art. 35 and 39 GwV-FINMA), fund management companies, CISA investment companies and collective asset managers (Art. 40 para. 3 and 4 and Art. 41 para. 3 GwV-FINMA) as well as for persons pursuant to Article 1b BankG, asset managers and trustees pursuant to Art. 2 para. 1 lit. a and b FinIA and trading systems for DLT securities pursuant to Art. 73a FinMIA (Art. 74 GwV-FINMA). 5

B. Addressees

6 According to the wording, the documentation obligation applies to **financial intermediaries pursuant to Art. 2 para. 2 and 3 AMLA**. **Traders** pursuant to Art. 2 para. 1 lit. b AMLA are also subject to the documentation requirement if they receive more than CHF 100,000 in cash in the course of a commercial transaction (Art. 8a para. 1 lit. c AMLA). However, traders are subject to simplified documentation requirements (see Art. 21 GwV), as they do not typically have a long-term legal relationship with their customers and are therefore generally only subject to the obligation to identify the contracting party (Art. 8a para. 1 lit. a AMLA) and the obligation to determine the beneficial owner (Art. 8a para. 1 lit. b AMLA).

C. Subject matter and scope of the documentation requirement

7 The subject matter of the documentation requirement is, on the one hand, the information on the transactions carried out by the financial intermediary (see n. 8 below) and the clarifications required under the AMLA (see n. 9 below) and, on the other hand, the supporting documents required to prove compliance with the provisions of the AMLA (see n. 10 below).

8 The AMLA does not define the term "**transactions**" in general terms. In connection with Art. 7 para. 1 AMLA, this term refers to all business transactions that are relevant to money laundering. This includes, in particular, activities in connection with the acceptance or safekeeping of third-party assets and assistance in investing or transferring such assets (see Art. 3 para. 3 AMLA).

9 The "**necessary clarifications**" required under the AMLA refer to the due diligence obligations under Art. 3-6 AMLA. Specifically, this means that the clarifications and conclusions regarding the identification of the contracting party (Art. 3), the determination of the beneficial owner (Art. 4), the re-identification or determination of the beneficial owner (Art. 5), and the special due diligence obligations (Art. 6; e.g. the obligation to carry out further clarification in the case of transactions or business relationships that appear unusual) must be documented.

10 In addition to the evidence relating to specific transactions and business relationships, the financial intermediary must also be able to demonstrate how it ensures compliance with the provisions of the AMLA. This means that the financial intermediary must document its **basis for decisions** and assessments

in a manner that is comprehensible to third parties, particularly in the case of discretionary decisions (e.g. on whether a transaction is considered unusual).

Controversial with regard to the subject matter of the documentation requirement is whether it only refers to the due diligence obligations set out in the first part of the provision in accordance with Articles 3–6 AMLA or whether the documentation requirement also covers the other obligations under the AMLA. Due to the systematic integration of the documentation obligation in the section on due diligence obligations and, in particular, due to a grammatical interpretation, we believe that the documentation obligation in Art. 7 AMLA formally refers only to Art. 3–6 AMLA. 11

From a **practical perspective**, however, this does not result in any significant restrictions on the obligation to document transactions relevant under money laundering law. For example, the other obligations under the AMLA (e.g., compliance with the organizational, training, and control obligations under Art. 8 AMLA) must also be documented on the basis of corresponding implementing provisions (see, for example, Art. 26 GwV-FINMA). In addition, pursuant to Art. 34 para. 1 AMLA, financial intermediaries must maintain separate databases and files containing all documents relating to reports to MROS pursuant to Art. 9 AMLA or Art. 305ter para. 2 SCC and to inquiries from MROS pursuant to Art. 11a AMLA. 12

D. Supporting documents

The term "supporting documents" is to be **interpreted broadly** and does not only include supporting documents in the accounting sense pursuant to Art. 957a para. 3 CO, but also the various documents, information and data that must be recorded in the customer profile as part of the due diligence obligations. Copies of identification documents and completed customer forms, as well as handwritten or electronic notes or comments made by the financial intermediary in the customer file, are also considered supporting documents. 13

In its practice, the **MROS** also assumes a broad interpretation of the term and states that it goes beyond traditional documents such as identification documents, documents identifying the beneficial owner, or information relating to transactions carried out in connection with the business relationships concerned. According to federal court rulings, the documentation and retention obligation with regard to any requests for information and seizure by law en- 14

forcement authorities pursuant to Art. 7 para. 2 AMLA extends to all necessary documents, including "internal investigation reports and the underlying structured documentation on extensive bank records and compliance forms."

15 Art. 74 GwV-FINMA also proceeds from such a broad understanding, specifying in concrete terms for persons under Art. 1b BankG, asset managers, trustees, and DLT trading systems, in the sense of a **non-exhaustive list**, which documents these financial intermediaries must retain. According to Art. 74 para. 1 GwV-FINMA, the following must be included in the files:

- a copy of the documents used to identify the contracting party;
- where applicable, a written statement by the contracting party regarding the identity of the controlling owner or the beneficial owner of the assets;
- a written note on the results of applying the criteria for identifying business relationships with increased risks;
- a written note or the documents on the results of the clarifications in the case of business relationships or transactions with increased risks;
- the documents relating to the transactions carried out;
- a copy of any reports pursuant to Art. 9 para. 1 AMLA and Art. 305ter para. 2 SCC;
- a list of AMLA-relevant business relationships maintained.

16 **Similar lists** of documents to be retained can also be found in various **SRO regulations**, e.g. in Art. 51 f. of the SRO SAV/SNV regulations.

17 For practical reasons, supporting documents should generally be drawn up in a **national language or in English**, as the addressees of the supporting documents (supervisory authorities, external auditors, criminal prosecution authorities, etc.; see n. 19 below) are located in Switzerland. However, there is no legal obligation to draw up supporting documents in accordance with Art. 7 AMLA in a national language or in English. The documentation requirement can therefore generally be fulfilled in **any language**. However, restrictions may arise for financial intermediaries subject to SROs from the SRO regulations applicable to them, for example if these require documents relevant to the determination of the facts to be translated.

E. Comprehensibility by knowledgeable third parties

The supporting documents must be **understandable and comprehensible** to knowledgeable third parties. This applies not only to the preparation of the supporting documents themselves, but also to their sensible organization and storage (see Art. 22 para. 1 GwV-FINMA). This primarily serves to relieve the financial intermediary of the burden of having to prepare the supporting documents in such a way that they are understandable to any third party. 18

The individual implementing provisions define who is considered an **expert third party**. According to Art. 22 GwV-FINMA, expert third parties are FINMA, the auditors it engages in accordance with Art. 25 FINMASA, the investigators it appoints in accordance with Art. 36 FINMASA, and the audit companies approved by the audit oversight authority. In the case of casinos, the documentation must be prepared in such a way that the ESBK, the criminal prosecution authority or other authorised bodies can form a reliable opinion (Art. 21 para. 1 GwV-ESKB) and in the case of commercial auditors who trade in bank metals themselves or through a group company (Art. 42bis para. 1 EMKG) and in the case of companies that trade in bankable precious metals on behalf of an auditor to which they belong as part of a group of companies (Art. 42bis para. 3 EMKG), the central office and the auditors and investigators called in must be able to understand the documentation (see Art. 45 para. 5 lit. b GwV-BAZG). 19

The expert third parties must be able to form a reliable opinion on the transactions and business relationships as well as on compliance with the provisions of the AMLA. A reliable opinion requires the ability to objectively assess the relevant transactions on the basis of the supporting documents provided. The documents and supporting evidence must therefore be prepared in such a way that individual **transactions can be reconstructed**, i.e., the documents and supporting evidence prepared must, in themselves, provide a complete and accurate picture of the transactions to be documented. 20

F. Point in time

In principle, the documentation obligation arises when a customer contact actually leads to a **business relationship or the conclusion of a cash transaction** in accordance with Art. 3 para. 2 AMLA. 21

22 Exceptions exist in connection with the reporting obligation under Art. 9 para. 1 lit. b AMLA, according to which a financial intermediary must report to MROS if it breaks off negotiations to establish a business relationship due to a suspicion of money laundering. The financial intermediary can only comply with this **suspicious transaction report** if it documents its findings and clarifications in this regard. In such cases, the financial intermediary is therefore obliged to prepare supporting documents before formally establishing a business relationship or concluding a cash transaction. This is the only way in which it can report the matter to MROS. In other words, the financial intermediary is only exempt from the documentation requirement during the initiation phase if it refrains from entering into a business relationship or cash transaction as a precautionary measure and this does not trigger a reporting obligation under Art. 9 para. 1 lit. b AMLA, i.e. if it breaks off negotiations without reasonable suspicion of criminal conduct within the meaning of Art. 9 para. 1 lit. a AMLA.

III. PERIODIC REVIEW AND UPDATING (PARAS. 1BIS)

A. Criticism by the FATF as the reason for the insertion

23 The obligation to periodically review and, if necessary, update (see n. 26 f.) the documentation prepared in accordance with para. 1 has been in force since January 1, 2023, and originates from FATF Recommendation 10. The FATF considered the previous lack of an explicit obligation to regularly review and update customer data to be a **significant deficiency**, particularly with regard to risk identification and management. Originally, it was planned to implement this FATF requirement by supplementing the GwV-FINMA and the relevant regulations of the SROs. However, for reasons of legal certainty, this was rejected and the provision was incorporated into the AMLA. From the FATF's point of view, the significant deficiency mentioned above was remedied by the entry into force of Art. 7 para. 1bis AMLA.

24 The obligation to (re)verify the identity of the beneficial owner is not a new obligation, but rather a **legal anchoring** of **existing practice and case law**. Even though such an obligation was not explicitly provided for in the law, periodic checks of the information available to the financial intermediary and documented in accordance with Art. 7 para. 1 AMLA had to be carried out to ensure its accuracy even before the entry into force of para. 1bis, in particular

on the basis of Art. 6 para. 1 AMLA. This also applied, for example, to the risk analysis pursuant to Art. 25 para. 2 GwV-FINMA, which also had to be updated periodically.

Financial intermediaries were also required to **regularly update** other information on clients **already in the past**, although this primarily applied to larger clients. In business with small customers, however, there were generally no event-related opportunities (e.g., in the context of periodic customer meetings) to update customer information. In this segment, para. 1bis led to an extension of the obligations of financial intermediaries, whereby the corresponding additional expense for financial intermediaries was offset by the planned risk-based approach (see n. 28 f.). 25

B. Regular updating obligation

According to Art. 7 para. 1bis AMLA, the financial intermediary must periodically check the supporting documents to ensure that they are up to date and update them if necessary. This fundamental obligation applies **regardless of events** and exists for all business relationships, regardless of the associated risk and regardless of whether the business relationship already existed when para. 1bis came into force or is a new business relationship. 26

The data must be updated in accordance with the rules applicable at the time of the update. If the applicable rules change between the time the data was obtained and the time of the update, the update must be carried out in accordance with the new rules and the data must be brought up to date in accordance with these rules. The message does not further explain what is meant by the applicable or "valid rules." This must undoubtedly apply to changes that have a material impact on the documents to be created (such as additional due diligence obligations). If the new rules are merely formal changes that have no material impact, then, in our opinion (in accordance with the ratio legis), no update in line with the new formal requirements is necessary, provided that this has no impact on the financial intermediary's ability to identify and manage risks. Ultimately, the financial intermediary must also decide this question on the basis of a risk-based approach (see n. 28 ff. below) and after weighing up the associated costs (e.g. whether a signed version must be obtained from each customer again when updating a form that has only been formally adapted). 27

C. Risk-based approach

1. Basic principle

28 A **risk-based approach** must be applied with regard to the scope, frequency and type of review and updating of supporting documents (Art. 7 para. 1bis 2nd sentence AMLA).

29 The legislator **has refrained from specifying**, for example, the frequency of reviews, leaving it to the financial intermediaries to define their own approach. The criteria for this must be laid down in an appropriate manner (e.g. in internal guidelines). In addition, the updating or confirmation of the validity must be documented in a manner that is comprehensible to professional third parties (Art. 7 para. 1 AMLA).

2. Scope

30 In principle, **all documents, information, and data** collected in the context of customer due diligence obligations for the customer profile are subject to verification and updating. Unlike Art. 5 para. 1 AMLA, however, the data to be updated is not limited to the identification of the customer or the determination of the beneficial owner. If relevant for the risk classification, the nature and purpose of the business relationship must also be reviewed. However, if, for example, the document used for the original identification of the contracting party (such as an identity card) has expired at the time of the review pursuant to Art. 7 para. 1bis AMLA, this does not necessarily mean that the identification must be renewed, provided that the relevant data relating to the customer's identity has not changed since then. The data that must be updated in each individual case is determined primarily on the basis of its relevance for the risk classification or monitoring of the business relationship.

31 However, documents and records that are requested as part of the documentation of **individual transactions** in accordance with Art. 6 para. 2 AMLA are not covered by the updating obligation, as these obviously do not relate to a permanent situation but to a one-off action. Furthermore, an expired copy of identification used for customer identification does not necessarily have to be obtained again as long as the relevant information on the customer's identity has not changed.

3. Frequency

The financial intermediary also has discretion with regard to the frequency of checks to ensure that information is up to date. The starting point for determining the appropriate frequency is the **risk classification**. Although the obligation to update customer data applies in principle to all customer relationships, business relationships with a higher risk require more frequent checks than those with a low risk due to the risk-based approach. 32

A point of reference for the required frequency of review can sometimes be derived from the obligation to decide annually on the continuation of **business relationships with increased risks** in accordance with Art. 6 para. 2 lit. c AMLA (Art. 19 para. 1 lit. a GwV-FINMA). Since this obligation can only be fulfilled if the documentation relating to the customer relationship is up to date, this interval is likely to represent the maximum period within which the file must be updated in accordance with Art. 7 para. 1bis AMLA for business relationships with increased risks. 33

A longer period should be permissible for **other business relationships**, although it would make sense to differentiate within the individual categories based on the risk classification. Such an approach would also be in line with the approach taken in Germany. According to the BaFin's interpretation and application guidelines on the German Money Laundering Act, a distinction can be made between the classification of business relationships/customers into risk categories when determining the frequency of ongoing monitoring. While for customers subject to enhanced due diligence requirements, the interval between updates of customer information must not exceed one year, for customers who are not subject to enhanced or simplified due diligence requirements, updates may be made at intervals of up to five years. For customers subject to simplified due diligence obligations, there are no specific time requirements from BaFin. Instead, updates must be made in a manner appropriate to the risk. These deadlines were shortened in the latest revision of the interpretation and application guidelines. Until November 2024, it was standard practice to update information at least every two years for high risks, at least every ten years for normal risks, and at least every 15 years for low risks. 34

4. Type of review

35 Measures to review the plausibility of the data must also be based on a risk-based approach. The **sources** may include the bank's own knowledge of the customer profile, public information, and information from an external source. Direct contact with the customer for the purpose of updating is not necessary in every case. If information from the customer is required for verification and updating, this can be obtained in the retail business, for example, via standardized queries using a form in online banking. If a customer does not respond to a request to update their information, further measures must be decided on a risk-based basis.

D. Event-driven updating obligation

36 In addition to periodically reviewing and updating the supporting documents, the financial intermediary must repeat the identification or determination of the beneficial ownership in accordance with Articles 3 et seq. AMLA if **doubts** arise in this regard in the course of the business relationship (Art. 5 para. 1 AMLA). The relevant event-driven clarifications and their results must be documented in accordance with Art. 7 para. 1 AMLA. Under the previous law, financial intermediaries were already required to establish appropriate processes to identify any indications of this in existing business relationships and to act accordingly.

37 Clarifications and changes to the customer profile of a business relationship resulting from the **special** due diligence requirements of Art. 6 AMLA must also be documented.

IV. READINESS TO PROVIDE INFORMATION AND HAND OVER DOCUMENTS (PAR. 2)

A. Preliminary remarks

38 Financial intermediaries must retain the supporting documents in accordance with Art. 7 para. 2 AMLA in such a way that they can comply with any requests for information and seizure by the criminal prosecution authorities within a reasonable period of time. In this context, the question arises, among other things, of how requests for information and seizure can be reconciled with confidentiality obligations such as bank customer secrecy (see N. 39 below)

and what constitutes a reasonable period of time (see N. 44 below). The permissible form of storage and the place of storage must then be clarified (see N. 45 f. below).

B. Requests for information and seizure by criminal prosecution authorities

The purpose of Art. 7 para. 2 AMLA is to enable the procurement of information that is likely to facilitate any criminal investigation into the origin of the assets. Contrary to the wording of Art. 7 para. 2 AMLA, the criminal procedural measure of seizure is not carried out as a request but as an order (Art. 263 para. 2 CrimPC). This also applies to disclosure by means of a disclosure order within the meaning of Art. 265 CrimPC. In contrast, the addressee of a request for information, whereby the criminal prosecution authorities informally request information and documents, is not obliged to comply with this request. This distinction is relevant in practice insofar as banks (see Art. 47 BankG) and financial institutions subject to FinIA (see Art. 69 FinIA) are **prevented from voluntarily disclosing information by client confidentiality**. The disclosure of a secret protected by the aforementioned provisions is therefore only justified if there are federal or cantonal provisions on the duty to provide evidence and information to an authority. 39

From a procedural point of view, the conditions for seizure are governed by Art. 263 para. 1 lit. a CrimPC, according to which only items that are likely to be **used as evidence** may be seized. Since this is a coercive measure, the provisions of Art. 197 para. 1 CrimPC are also relevant, according to which coercive measures may only be taken if they are provided for by law, there is sufficient suspicion of a crime, the objectives sought cannot be achieved by less severe measures, and the significance of the crime justifies the coercive measure. 40

As already explained (see n. 14 above), according to Federal Supreme Court case law, the documentation and retention obligation also extends to internal bank investigation reports and the findings on which they are based. Such investigation reports are often prepared by the financial intermediary's own *second line* legal and/or compliance functions. However, in complex or particularly sensitive cases, financial intermediaries often call on external experts. If these are lawyers, the question arises as to whether these reports are protected by attorney-client privilege and therefore cannot be disclosed. The Federal 41

Supreme Court has addressed this question in various decisions. According to the practice of the Federal Supreme Court, so-called (accessory) "business activities" of lawyers are not protected by professional secrecy. The decisive criterion for the distinction is whether the commercial/operational or the lawyer-specific elements objectively predominate in the services in question. In the case of mixed or global mandates, where lawyer-specific services and ancillary business activities overlap, a decision must be made on a case-by-case basis as to which facts or documents are covered by attorney-client privilege. If a financial intermediary delegates its own statutory compliance and controlling tasks and the associated obligation to document suspicious business transactions appropriately to lawyers, it cannot, according to case law, invoke attorney-client privilege "in its entirety" in the event of criminal investigations in this regard.

42 The Federal Supreme Court has clarified the case law mentioned in the previous paragraph in a recent ruling. In connection with internal investigations by law firms, the Federal Supreme Court held that the investigation of facts (and not merely the examination of the legal situation) also falls within the core area of a lawyer's activities and is therefore protected by attorney-client privilege. However, it is not a typical activity of a lawyer if a lawyer performs compliance tasks in connection with money laundering legislation or internal supervision thereof. The question of whether it seems necessary to get a law firm involved in a specific case isn't relevant to the question of typical lawyer activities, since lawyers are only allowed to work in areas where they have a monopoly (but the protection of lawyer-client privilege isn't limited to these areas). According to the Federal Supreme Court, the decisive factor is rather "whether legally prescribed documentation and retention obligations are circumvented by delegating them to a law firm." In the case in question, the investigation of the facts took place in connection with the provision of advice and representation in relation to existing or impending legal disputes, which qualifies as typical legal work protected by attorney-client privilege. However, the Federal Supreme Court expressly left open the question of whether complex internal investigations and assignments limited to the mere investigation of the facts can generally be classified as activities typical of a lawyer. Finally, in the aforementioned decision, the Federal Supreme Court also addressed the question of whether the "pre-existing" evidence referred to in the investigation report or attached to it is protected by attorney-client privilege and

whether documents considered to be attorney correspondence lose their confidential nature when disclosed to a third party (FINMA).

It should also be noted that financial intermediaries are required to provide information and hand over documents **not only to the criminal prosecution authorities**, but also to MROS (Art. 9 and 11a AMLA), the supervisory authorities responsible for them (Art. 12 AMLA) or SROs and their audit bodies. 43

C. Compliance within a reasonable period of time

Financial intermediaries must comply with requests for information and seizure within a reasonable period of time. Neither the law nor the ordinance specifies what constitutes a "reasonable" period. The law enforcement authorities have an interest in securing evidence as quickly as possible, but financial intermediaries must also be given time to carefully examine the requirements of the request and to provide the relevant documents. A **period of five days** is generally considered reasonable. In the case of seizure orders, the criminal authority usually sets a deadline by which the documents must be made available (Art. 265 para. 3 CrimPC). 44

D. Requirements for storage

The documentation may be kept **in paper form or on an electronic data carrier**. Pursuant to Art. 74 para. 3 GwV-FINMA, which applies to persons under Art. 1b BankG, asset managers, trustees and DLT trading systems, the documents and supporting evidence must be kept in a secure location in Switzerland that is accessible at all times. In line with this provision, various SRO regulations also expressly require storage in Switzerland. The ultimate aim is to ensure that the financial intermediary can comply with any requests for information or seizure by a criminal prosecution authority "within a reasonable period of time" (see n. 44 above). 45

If the documents and supporting documents are stored electronically, the **server must be located in Switzerland**. If, however, the server used is not located in Switzerland or if a cloud solution is used, the financial intermediary must have up-to-date physical or electronic copies of the relevant documents in Switzerland (Art. 74 para. 4 GwV-FINMA). At the same time, the IT solution must also meet the requirements of the Ordinance on Business Records, for 46

example by ensuring that changes or deletions to the stored data can be traced.

V. RETENTION PERIOD (PAR. 3)

47 According to Art. 7 para. 3 AMLA, financial intermediaries must retain supporting documents for **at least ten years** after the termination of the business relationship or after the transaction has been completed. For the start of the aforementioned period, a distinction must therefore be made between transaction-related supporting documents and supporting documents relating to the results of the clarifications pursuant to Art. 3–6 AMLA. In the case of transaction-related documents, the period does not begin on the date on which the transaction document is created, but after the relevant transaction has been completed. In the case of other documents (such as documents identifying the contracting party), the period begins when the business relationship ends or, in the case of cash transactions, when the transaction is completed.

48 The MROS also points out that in cases where financial intermediaries have information that is **more than 10 years old**, it assumes that the financial intermediaries will also make this information available to the MROS (in suspicious transaction reports and in connection with requests from the MROS pursuant to Art. 11a AMLA). According to MROS, this also follows from Art. 11a paras. 1 and 2 AMLA, which stipulates the obligation to disclose information if it is available (the "availability principle").

49 A special feature arising from **data protection considerations** can be found in Art. 34 AMLA. According to para. 4 of this provision, data from reports to MROS must be destroyed five years after the report has been made. However, this obligation to destroy data only applies to data collected in the course of compiling the report and not to the ordinary supporting documents retained in accordance with Art. 7 AMLA. In its 2021 annual report, MROS also pointed out that the deletion obligation under Art. 34 para. 4 AMLA (after five years) only applies to copies that were transmitted in the course of a suspicious activity report or a request for disclosure under Art. 11a AMLA, and not to the originals.

VI. APPLICATION ISSUES

A. Possibility and limits of delegation

The possibility of delegating the documentation obligation under Art. 7 AMLA is controversial. According to prevailing opinion, in addition to the **clarifications pursuant to Art. 3–6 AMLA**, the **storage of** supporting documents pursuant to Art. 7 para. 2 AMLA may also be delegated to third parties (see n. 52 below). 50

With regard to the **tasks under Art. 7 para. 1 AMLA**, however, some legal scholars argue that these obligations must be fulfilled by the financial intermediaries themselves, since the supporting documents for compliance with the documentation obligation serve, among other things, the financial intermediaries themselves by providing them with a secure knowledge base for well-founded and justified decisions. In addition, the supporting documents also form the basis for the ongoing risk assessment pursuant to Art. 6 AMLA. For these reasons, the aforementioned doctrine concludes that the documentation obligation cannot, in principle, be delegated and must therefore be exercised by the financial intermediary itself. Other doctrines, however, also allow the delegation of the preparation of supporting documents to third parties within the scope of the usual duties (selection, instruction, and supervision). In our opinion, the same conclusion applies to the possibility of delegating the periodic review and updating pursuant to Art. 7 para. 1bis AMLA. However, delegating the periodic review and updating to third parties does not release the financial intermediary from its responsibility to ensure that, despite the involvement of a third party, it complies with the due diligence obligations under the AMLA and is in a position to take the necessary measures where necessary on the basis of the updated information. 51

As mentioned (see n. 50), the **storage of supporting documents may be delegated to third parties**, which has become particularly relevant in the age of electronic files and cloud applications. However, data protection aspects must be taken into account and banks and securities firms, for example, must comply with the requirements of FINMA Circular 2018/3 (Outsourcing). 52

B. Compliance with the documentation requirement for AI applications

53 Unless an exception applies, banks and securities firms must, in accordance with Art. 20 para. 2 GwV-FINMA, have IT systems in place that enable them to automatically detect suspicious transactions. Banks are currently examining the use of systems based on "artificial intelligence" (hereinafter "AI applications"). The aim of such technical solutions is to meet regulatory requirements more efficiently and effectively. The documentation requirements apply regardless of the technology used. When monitoring transactions using **AI applications**, the documentation requirement has two levels. First, documentation on how the AI application works must be available. This includes, among other things, that the documentation shows which data is fed into the system and according to which rules and indicators evidence of conspicuous criteria is generated. It must also be possible to verify that the selected rules, parameters, etc. comply with the minimum legal standards. Second, as with any transaction monitoring, the clarifications made by employees and the analyses performed by the AI application must be documented.

VII. LEGAL CONSEQUENCES OF A VIOLATION

A. Preliminary remarks

54 The AMLA does not stipulate any supervisory or criminal law consequences for a violation of the documentation obligation. It is incumbent on the competent supervisory authorities or self-regulatory organizations to take the appropriate supervisory measures in the event of violations (see n. 55 ff.). In addition, a violation of Art. 7 AMLA may result in criminal (see n. 58 f.) and civil law consequences (see n. 60 ff.).

B. Supervisory consequences

55 A violation of Art. 7 AMLA may result in supervisory measures for **financial intermediaries subject to special legislation**. If there is suspicion of a violation of supervisory provisions, FINMA may, for example, initiate enforcement proceedings against financial intermediaries subject to its supervision. In this case, it has the supervisory instruments listed in Art. 31 ff. FINMASA at its disposal. Serious organizational deficiencies may call into question the neces-

sary guarantee of proper business conduct and result, for example, in a professional ban pursuant to Art. 33 FINMASA. In particularly serious cases, the licence will be revoked. The ESBK, the intercantonal supervisory and enforcement authority in the area of gambling, and the Central Office also have far-reaching powers of intervention with regard to licence holders under Art. 42bis EMKG.

Banks and other financial intermediaries that are required to comply with the VSB are generally sanctioned for violating the obligation to ensure compliance under Art. 44 VSB 20 and not for violating the relevant duty of care if, due to a lack of documentation, compliance with the due diligence obligations under Art. 3-5 AMLA can no longer be verified. 56

If a **member of an SRO** violates the relevant regulations, the SRO may take the enforcement measures provided for in its regulations (Art. 25 para. 3 lit. c AMLA). Sanctions of up to CHF 1 million are possible in some cases. As a last resort, it may expel the member concerned (Art. 25 para. 3 lit. a AMLA), which is equivalent to a ban on acting as a financial intermediary if the financial intermediary concerned does not join another SRO or submit an application for affiliation within two months (Art. 12 para. 1 AMLO). 57

C. Criminal law consequences

A breach of the documentation obligation may also have criminal law consequences. In particular, criminal liability under **Art. 305ter SCC** may arise if a natural person breaches the obligations under Art. 7 AMLA and is therefore accused of not having exercised due diligence in identifying the beneficial owner. By keeping appropriate documentation in accordance with Art. 7 AMLA, companies can prove that they are complying with their due diligence obligations under the AMLA, thereby ruling out criminal liability for inadequate organization under Art. 102 para. 2 SCC in this context. 58

If a financial intermediary is subject to accounting requirements and the documents affected by the breach of the documentation requirement are accounting documents, this may result in a fine of up to CHF 10,000 under Art. 325 SCC (**improper keeping of business records**) in conjunction with Art. 106 para. 1 SCC. For banks and collective investment schemes, the relevant special provisions pursuant to Art. 46 para. 1 lit. b BankG and Art. 148 para. 1 lit. e CISA apply. 59

D. Civil law consequences

60 According to Federal Supreme Court case law, the documentation requirement under Art. 7 AMLA, like the other due diligence obligations under the AMLA, does **not constitute a protective provision** within the meaning of Art. 41 CO. Thus, non-contractual liability under Art. 41 CO in connection with a breach of the documentation requirements is excluded due to lack of illegality.

61 **Contractual liability** on the part of the financial intermediary may arise if the supervisory provision of Art. 7 AMLA is used to specify the documentation obligations of the agent under private law (according to the theory of spillover effect). In addition to a breach of the duty of care, however, damage and an adequate causal link must also be proven in order for a contractual claim for damages to be upheld.

62 In the case of financial intermediaries subject to accounting requirements, a breach of the supervisory documentation obligation may also constitute a **breach of the retention obligation under accounting law** (Art. 957 et seq. CO) and thus give rise to civil law claims for damages.

VIII. OUTLOOK

63 In its message on the Federal Act on Transparency of Legal Entities and Identification of Beneficial Owners (TJPG), the Federal Council proposed various measures designed to strengthen the integrity and competitiveness of Switzerland as a financial and business center. In addition to the introduction of a federal register of beneficial owners, this also applies in particular to the **extension of due diligence obligations to certain advisory activities** (in particular legal advice) that involve an increased risk of money laundering. The structuring of companies and real estate transactions are considered particularly risky. The due diligence requirements for this new category of advisors would also include the documentation requirement under Art. 7 AMLA. However, during its 2024 winter session, the Council of States decided to separate the planned amendments to the AMLA from the bill introducing the TJPG. While the Council of States has approved the latter, the amendments to the AMLA are expected to be debated in the 2025 spring session. It is not yet possible to estimate when the bill, which has been criticized by the preliminary consultation committee, will come into force.

BIBLIOGRAPHY

Bommer Felix/Goldschmid Peter, Kommentierung zu Art. 265 StPO, in: Niggli Marcel Alexander/Heer Marianne/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung, 3. Aufl., Basel 2023.

Bühlmann Lukas/Reinle Michael, Kommentierung zu Art. 6 DSG, in: Blechta Gabor P./Vasella David, (Hrsg.), Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz, 4. Aufl., Basel 2024.

De Capitani Werner, Kommentierung zu Art. 7 GwG in: Schmid Niklaus/Bernasconi Paolo/de Capitani Werner, Kommentar Einziehung – Organisiertes Verbrechen – Geldwäscherei, Bd. II, Zürich 2002.

Fritsche Claudia M., Kooperieren oder nicht?, in: GesKR 2016, S. 376–386.

Goldberg Emmanuel, Überprüfung des wirtschaftlich Berechtigten und Aktualisierung der Kundendaten nach der Revision von Geldwäschereigesetz und -verordnung, in: Recht relevant. für Compliance Officers, S. 2–4, Zürich 2023.

Graber Christoph K./Oberholzer Dominik, Das neue GwG, 3. Aufl., Zürich 2009.

Heim Kathrin/Wettstein Tamara, Praxiskommentar zur Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken, 4. Aufl., Zürich 2019.

Huber Roman, Interne Untersuchungen und Anwaltsgeheimnis, in: GesKR 2019, S. 65–82.

Jutzi Thomas/Wess Ksenia, Die (neuen) pflichten im Execution-only-Geschäft: Zusammenspiel von FIDLEG und OR, SZW 2019, S. 589–617.

Kilgus Sabine/Losinger Paolo, Kommentierung zu Art. 1 GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Lang Carsten, Aktualisierung der Auslegungs- und Anwendungshinweise der BaFin zum Geldwäschegesetz, in: Geldwäsche & Recht 2025, S. 5-10.

Lengauer Daniel/Ruckstuhl Lea, Compliance, Zürich 2017.

Lötscher Bernard/Sievi Nino, Kommentierung zu Art. 7 GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Meyer Patrick K./Ryhner Samuel, Kommentierung zu Art. 5 GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Müller Thomas, Kommentierung zu Art. 7 GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar, Geldwäschereigesetz (GwG), Bern 2017.

Peyer Martin, Kommentierung zu Art. 8 GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Rappo Aurélia, LBA - Actualisation des données clients, in: EF 2019, S. 1013–1016.

Roth Pellanda Katja/Kopp Lara, Kommentierung zu Art. 29 FINMAG, in: Watter Rolf/Bahar Rashid (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

Stengel Cornelia, Transaktionsmonitoring mittels künstlicher Intelligenz, in: Jusletter vom 5.6.2023.

Taube Tamara, Entstehung, Bedeutung und Umfang der Sorgfaltspflichten der Schweizer Banken bei der Geldwäscherei Prävention im Bankenalltag in: Bertschinger Urs (Hrsg.), SGFM Nr. 9, Zürich 2013.

Thelesklaf Daniel/Ordolli Stiliano, Kommentierung zu Art. 34 GwG, in: Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell Füssli Navigator Kommentar, GwG Kommentar/AMLA Commentary, 3. Aufl., Zürich 2019.

Wyss Ralph, Kommentierung zu Art. 7 GwG, in: Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell Füssli Navigator Kommentar, GwG Kommentar/AMLA Commentary, 3. Aufl., Zürich 2019.

MATERIALS

BaFin, Bundesanstalt für Finanzdienstleistungen, Auslegungs- und Anwendungshinweise zum Geldwäschereigesetz, Stand März 2025, abrufbar unter https://www.bafin.de/SharedDocs/Downloads/DE/Auslegungsentscheidung/dl_ae_auas_2025_gw.pdf?__blob=publicationFile&v=6, besucht am 10.3.2025.

Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG) vom 17.6.1996, BBl 1996 III 1101 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1996/3_1101_1057_993/de, besucht am 10.3.2025.

Botschaft zur Änderung des Geldwäschereigesetzes vom 26.6.2019, BBl 2019 5451 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2019/1932/de, besucht am 10.3.2025.

Eidgenössische Finanzmarktaufsicht FINMA, Erläuterung zur Teilrevision der Geldwäschereiverordnung der FINMA (GwV-FINMA) vom 27.10.2022, abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/anhoerungen/laufende-anhoerungen/20221102-gwv-finma/erlaeuterungen_gwv_finma_20221027_de.pdf, besucht am 10.3.20205.

Eidgenössisches Justiz- und Polizeidepartement EJPD, Bundesamt für Polizei fedpol, Meldestelle für Geldwäscherei (MROS), Jahresbericht 2020, Bern 2021, abrufbar unter https://www.fedpol.admin.ch/dam/fedpol/de/data/kriminalitaet/geldwaescherei/jabe/jb-mros-2020-d.pdf.download.pdf/jb-mros-2020-d.pdf, besucht am 10.3.2025.

Eidgenössisches Justiz- und Polizeidepartement EJPD, Bundesamt für Polizei fedpol, Meldestelle für Geldwäscherei (MROS), Jahresbericht 2021, Bern 2022, abrufbar unter https://www.fedpol.admin.ch/dam/fedpol/de/data/kriminalitaet/geldwaescherei/jabe/jb-mros-2021.pdf.download.pdf/jb-mros-2021-d.pdf, besucht am 10.3.2025.

Einsatz innovativer Technologien im Bereich der Finanzmarktaufsicht und -regulierung (RegTech), Bericht des Bundesrates in Erfüllung des Postulats 16.3256 Landolt vom 18.3.2016, abrufbar unter https://www.parlament.ch/centers/eparl/curia/2016/20163256/Bericht%20BR%20D.pdf, besucht am 10.3.2025.

FATF, Anti-money laundering and counter-terrorist financing measures - Switzerland, Fourth Round Mutual Evaluation Report, Paris 2016, abrufbar unter https://www.fatf-gafi.org/content/dam/fatf-gafi/images/mer/mer-switzerland-2016.pdf.coredownload.inline.pdf, besucht am 10.3.2025.

FATF, Anti-money laundering and counter-terrorist financing measures - Switzerland, 4th Enhanced Follow-up Report, Paris 2023, abrufbar unter

https://www.fatf-gafi.org/content/dam/fatf-gafi/fur/Switzerland-FUR-2023.pdf.coredownload.inline.pdf, besucht am 10.3.2025.

Medienmitteilung des Bundesrates vom 22.5.2024 «Bundesrat verabschiedet Botschaft zur Stärkung der Geldwäscherei-Bekämpfung», abrufbar unter https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-101100.html, besucht am 10.3.2025.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 7a AMLA

A commentary by Eliane Gmünder / Raoul Breuleux

SUGGESTED CITATION

Eliane Gmünder/Raoul Breuleux, Commentary of art. 7a AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Gmünder/Breuleux, art. 7a AMLA N. XXX.

Art. 7*a* Assets of low value

The financial intermediary may dispense with complying with the duties of due diligence (Art. 3–7) if the business relationship only involves assets of low value and there is no suspicion of money laundering or terrorist financing.

CONTENT

I. Purpose and system of the provision 233
II. History 234
III. International law 234
A. FATF Recommendations 234
B. European Union Anti-Money Laundering Directive 234
IV. Basic definition 235
A. General requirements 235
B. Assets of small value 235
C. No suspicion of money laundering or terrorist financing 235
V. Art. 11 GwV-FINMA 235
A. Payment instruments for cashless payment transactions that are used exclusively to pay for goods and services (Art. 11 para. 1 AMLO-FINMA) 236
1. e-money (lit. a) 237
2. Payments may only be made to Swiss merchants (lit. b) 238
3. Closed-loop systems (lit. c) 238
B. Payment instruments for cashless payment transactions that are not used exclusively to pay for goods and services (Art. 11 para. 2 AMLO-FINMA) 239
C. Non-rechargeable means of payment (Art. 11 para. 3 AMLO-FINMA) 239
D. Monitoring of the threshold values (Art. 11 para. 4 AMLO-FINMA) 240
E. Finance leasing (Art. 11 para. 4bis AMLO-FINMA) 241
F. Further exemptions (Art. 11 para. 5 GwV-FINMA) 242
VI. Legal effect of the exceptions 242
Bibliography 243
Materials 243

I. PURPOSE AND SYSTEM OF THE PROVISION

The purpose of the provision is to apply the risk-based approach in a more specific manner. It is intended to provide assistance and to describe circumstances in which the risk of money laundering is so low that compliance with the full due diligence requirements (Art. 3–7 AMLA) would not be justified. The regulation is intended to serve as a **de minimis clause** applicable to long-term relationships, in addition to that for cash transactions (Art. 3 para. 2 AMLA). It should be noted that this de minimis clause is not aimed at subjecting a financial intermediary as such, but merely at waiving compliance with individual due diligence requirements. 1

The **concretization** of the conditions of the standard by means of the terms "assets of little value" and "no suspicion of possible money laundering or terrorist financing" was carried out in Art. 11 AMLO-FINMA. The fact that this regulation is at the ordinance level means that it is quicker and easier to adapt the definitions and the cases in which they apply, which is an important aspect of promoting innovation in the Swiss financial center. Products in the areas of payment systems, platforms, e-money and virtual asset service providers (VASPs) are particularly fast-moving, which requires flexibility and dynamism on the part of the regulator and the supervisory instruments. FINMA assesses specific applications from financial intermediaries with a particular business model and associated risk profile to determine whether they qualify for a waiver of due diligence requirements in accordance with Article 7a AMLA (Article 11 para. 5 GwV-FINMA). If the financial intermediary is subject to a self-regulatory organization (SRO) rather than FINMA, the application for a potential exemption from the due diligence requirements is submitted to the responsible SRO for final review by FINMA. 2

While Art. 11 AMLO-FINMA, which is based on Art. 7a of the AMLA, governs the *waiver of* the performance of individual due diligence requirements, a related norm exists in **Art. 12 AMLO-FINMA**. This regulates a special case of *simplified* due diligence requirements, which has its origin in a letter from the Anti-Money Laundering Control Authority dated 9.10.2003, in which the Control Authority granted such exceptions. The Association of Swiss Credit Banks and Financial Institutions requested that FINMA also apply these simplifications to the area of consumer credit, which it confirmed in a letter dated June 15, 2011. This practice was then incorporated into Art. 12 GwV-FINMA. 3

II. HISTORY

4 The standard was introduced with the Federal Act of October 3, 2008 on the Implementation of the Revised FATF Recommendations and entered into force on February 1, 2009. The aim of the introduction of this provision was to grant "administrative relief" as a counterweight to the stricter due diligence requirements that were introduced at the same time.

III. INTERNATIONAL LAW

A. FATF Recommendations

5 The FATF Recommendations, on the basis of which the provision of Art. 7a AMLA was issued, allow countries not to apply certain obligations to specific institutions or to narrowly defined forms of business activity if these can be shown to have a low risk of money laundering. The FATF Recommendations specify the **risk-based approach** to the identification of the contracting partner by identifying risk-increasing and risk-reducing circumstances. In its guidance, the FATF also provides specific information and a risk matrix that show how the risk-based approach can be implemented in the area of electronic card, mobile and internet payments. Some of the criteria mentioned therein can be found in Article 11 GwV-FINMA.

B. European Union Anti-Money Laundering Directive

6 There is an analogous exemption provision in the EU. Article 15 of Directive 2015/849/EU, as amended by Directive (EU) 2018/843, stipulates that in certain areas where there is only a low risk, a member state may provide for simplified due diligence. At the same time, para. 3 of this provision clarifies that transactions and business relationships must be monitored to a sufficient extent to enable the detection of unusual or suspicious transactions, even when simplified due diligence procedures are applied. According to the proposal for the new regulation to combat money laundering and terrorist financing, an authority for combating money laundering and terrorist financing ("AMLA") is to issue so-called "technical regulatory standards" that describe the obligations for conducting due diligence with regard to customers. These regulatory standards should also include specific simplified due diligence requirements that can be applied when there is a low risk.

IV. BASIC DEFINITION

A. General requirements

Art. 7a AMLA defines the conditions under which a business relationship can be considered non-critical, with the consequence that compliance with the due diligence requirements (Art. 3–7 AMLA) may be waived. To this end, the two conditions set out below must be met cumulatively. 7

B. Assets of small value

The law does not specify the maximum amount below which assets may be classified as "**low-value** assets". Rather, this is to be determined in the context of the envisaged business model and in particular with regard to how exposed such a business model is to possible money laundering or terrorist financing. In order to set certain guidelines nonetheless, FINMA was instructed to create various case groups of financial intermediaries and financial products or services within the framework of GwV-FINMA and to set thresholds for these case groups, taking into account the anticipated money laundering risks (see no. V. below). 8

C. No suspicion of money laundering or terrorist financing

The cumulative requirement of the exclusion of suspicions of possible money laundering or terrorist financing is paradoxical in that the very purpose of the due diligence requirements – from which exemption is granted – is to be able to identify **suspicious facts**. This contradiction is already addressed in the explanatory report, which clarifies that the waiver of due diligence requirements should only apply to products and services that pose a *low to very low risk of money laundering*. This specification is consistently supported in the doctrine. In the list of cases in Article 11 AMLO-FINMA, FINMA specifically names products and services that pose a low or very low risk of money laundering, which is why it can be assumed that there are no grounds for suspicion without further audit procedures being required for this determination. 9

V. ART. 11 GWV-FINMA

The legislator (FINMA) has been commissioned by the Federal Council to selectively designate areas that it releases from compliance with due diligence 10

requirements if, in connection with a specific threshold, they show a low or very low risk of money laundering. With this approach of identifying and defining **case groups**, Switzerland is following the FATF's approach.

11 The authors believe that the list of case groups in Article 11 AMLO-FINMA, which has existed since 2008 and has remained almost unchanged since then, should be updated and expanded, given that not only the needs of financial intermediaries and their customers and thus the **business models** have changed in the meantime, but also that case law has developed further. However, the most important drivers for a revision are likely to be the new technological conditions and possibilities that have arisen as a result of the digitalization push in the financial services sector. Finally, the case groups should also be adapted to the changed circumstances because it is important to ensure that these constellations actually pose a low risk of money laundering. For example, the risk can be very significant in the case of payment systems or the transfer of cryptocurrencies that allow a transfer of value abroad, while those with restrictions on local transfers (e.g. vouchers for department stores; payment system in a ski resort, etc.) show a lower risk.

A. Payment instruments for cashless payment transactions that are used exclusively to pay for goods and services (Art. 11 para. 1 AMLO-FINMA)

12 The restriction to the "payment of goods and services" is to be interpreted restrictively, since the legislator of the ordinance thus means only goods and services from commercial traders and service providers. Payments between private individuals do not fall under para. 1, even if the reason for the payment lies in the purchase of goods and services (e.g. via internet auction houses).

13 In addition, systems that allow value transfers without the purchase of goods should not be exempted from compliance with due diligence requirements, as FINMA sees an inherent risk of money laundering in these constellations. Furthermore, it should be noted that all the amounts defined in para. 1 are explicitly to be understood as so-called *"spending limits"*. This means that it is not the amount made available (e.g. card limit) that is decisive for the threshold value, but the amount that the user of the means of payment can actually spend or pay. If the means of payment allows *"overpayment"*, then this amount is to be included in the threshold. This requires that the financial in-

termediary must have the technical means to detect the exceeding of the **threshold values** (Art. 11 para. 4 AMLO-FINMA).

The legislator has defined the following subcategories, which are part of cash- 14
less payment transactions for the exclusive payment of goods and services:

1. *e-money* (lit. a)

There is no precise definition of the terms e-money or e-commerce; howev- 15
er, they are generally understood to mean electronic means of payment for everyday use and in particular for use on the **internet**. From the point of view of the legislator, it is irrelevant whether the electronically available money is stored on a server and the customer accesses and uses it by means of virtual access (e.g. to a wallet) or whether the amount is debited from a local chip system. Traditionally, these are so-called *prepaid* systems.

In addition to the criteria in para. 1, the following conditions must be cumula- 16
tively fulfilled (lit. a):

- No more than CHF 1,000 per transaction and CHF 5,000 per calendar year and contracting party may be paid;
- any repayments of the means of payment are made only in favor of accounts held with banks authorized in Switzerland or subject to equivalent supervision abroad and in the name of the contracting party; and
- the amount of CHF 1,000 may not be exceeded per repayment.

By allowing for the possibility of repayment, the legislator wanted to prevent 17
unfair business models from being favored and customers from being subjected to pressure to buy. Nevertheless, in order to keep the risk of money laundering low, the **repayments** must be transferred to the same bank account from which the transfers originally originated. If this is not possible in individual cases (e.g. due to the balance of this account having been cleared in the meantime), then the financial intermediary must ensure that the amount is at least transferred to an account in the name of the same contractual partner. If, in individual cases, the amount has to be transferred back to a different account, then this circumstance is irrelevant for the calculation of the limit, as it is ultimately the same contractual partner.

2. Payments may only be made to Swiss merchants (lit. b)

18 In addition to the criteria in para. 1, the following conditions must be cumulatively fulfilled (lit. b):

- No more than CHF 5,000 per month and CHF 25,000 per calendar year and contractual partner may be
- to merchants in Switzerland;
- whereby charges are made exclusively to and any repayments of the means of payment are made exclusively to an account in the name of the contracting party with a bank authorized in Switzerland.

19 The higher thresholds seem justified insofar as in this constellation payments can only be made to Swiss merchants. Since this is not feasible in practice (it would be necessary to *monitor merchants in real time* with regard to their Swiss domicile), doctrine correctly states that this use case can only be realized if the circle of providers and service providers is limited (so-called *"closed-loop systems"* within the meaning of lit. c below).

3. *Closed-loop* systems (lit. c)

20 This primarily concerns store cards or the issuing of cards that are accepted within a clearly defined group of customers (e.g. merchants belonging to the same group).

21 In addition to the criteria in para. 1, the following conditions must be cumulatively met (lit. c):

- The means of payment can only be used within a specific network of service providers or suppliers; from the term "service provider" it can be inferred that the service provider pursues a commercial activity, in contrast to paragraph 2, which is intended to regulate payments between private individuals; and
- the turnover does not exceed CHF 5,000 per month and CHF 25,000 per calendar year and contractual party.

B. Payment instruments for cashless payment transactions that are not used exclusively to pay for goods and services (Art. 11 para. 2 AMLO-FINMA)

Under paragraph 2, it is not a requirement that the means of payment is used exclusively for the cashless payment of goods and services. To this end, the thresholds have been reduced to a maximum of CHF 250 per data carrier or per transaction and CHF 1,500 per contracting party. This should allow very small amounts to be transferred **between private individuals (P2P)** without having to observe the due diligence requirements. The provisions on charges or repayments to an account held in the name of the contracting party at a Swiss bank in accordance with Art. 11 para. 1 lit. b AMLO-FINMA also apply here (see N. 18). 22

C. Non-rechargeable means of payment (Art. 11 para. 3 AMLO-FINMA)

In para. 3, the criterion of a *long-term business relationship* was deliberately omitted. Instead, the following conditions apply here, which justify a waiver of the duty to comply with the due diligence requirements: 23

- the means of payment cannot be recharged;
- the credit balance serves exclusively to pay electronically for goods and services purchased by the contracting party;
- no more than CHF 250 is made available per data carrier; and
- no more than CHF 1,500 is made available per transaction and per contracting party.

In this regard, FINMA shall apply the criteria for assessing related transactions in line with those of the cash transaction. 24

D. Monitoring of the threshold values (Art. 11 para. 4 AMLO-FINMA)

25 The financial intermediary may dispense with compliance with the duties of due diligence under the following cumulative conditions:

- He must have technical facilities sufficient to detect any exceeding of the respective threshold values.
- It must take precautions to prevent any accumulation of the amount limits and violations of the provisions of Art. 11 AMLO-FINMA.
- Articles 14 and 20 AMLO-FINMA remain reserved with regard to the monitoring of transactions. Article 10 AMLO-FINMA also remains reserved, insofar as it is applicable. The obligations mentioned in the reserved provisions must therefore continue to be observed despite the waiver of the due diligence obligations.

26 It should be noted first of all that, contrary to the wording of the provision, the legislator not only requires that the **exceeding of the respective thresholds** be detected, but that the financial intermediary should also ensure that the exceeding of the thresholds is technically prevented. "It should be technically impossible to pay more than the set amount at once. Likewise, a possible accumulation of the amount limits should be prevented (prohibition of smurfing)." It is precisely this technical monitoring and the automatic blocking in *the event of a threshold being reached, with or without an accumulation of the amount limits*, that are not easy to implement in practice, especially since the contracting parties are not identified in the sense of Art. 3-7 AMLA. In this respect, it is advisable for financial intermediaries to identify the contracting parties by other means; otherwise, it would be impossible to attribute the amounts and thus monitor the thresholds. This includes, in particular, the registration of personal data such as surname, first name, date of birth, address, e-mail address, mobile phone number and IBAN (in the name of the contracting party). Even if this information does not offer an absolute guarantee, it does allow the financial intermediary to carry out certain automated checks, such as comparisons with address databases and databases specifically maintained for the purposes of a "*name check*", and thus verify the accuracy of the information.

Client-identifying information is also necessary to carry out meaningful **transaction monitoring** within the meaning of Art. 14 in conjunction with Art. 20 AMLO-FINMA and to identify transactions with increased risks, because these obligations must also be observed when applying the exception in Art. 7a AMLA due to the clarification in Art. 11 para. 4 AMLO-FINMA. Identifying customers with increased risks, particularly PEPs, is another duty that cannot be fulfilled without a "*Name Check*" comparison and, consequently, without the necessary *customer-identifying* information. 27

In conclusion, it should be noted that it was not the intention of the legislator to use this para. 4 to immediately undermine the simplifications under Art. 11 AMLO-FINMA. Instead, financial intermediaries are required to ensure appropriate and risk-based **monitoring.** It is recommended that financial intermediaries regularly validate the risks as part of their AMLA risk analysis in accordance with Art. 25 para. 2 AMLO-FINMA and adjust the measures if necessary. 28

E. Finance leasing (Art. 11 para. 4bis AMLO-FINMA)

In the case of a finance lease, there is a three-way system in which the lessor acts as the pre-financing and thus lending party, which ultimately leads to its **subordination requirement** under Article 2 para. 3 let. a AMLA. The lessor acquires the leased asset from the manufacturer or dealer for its own account and in its own name, but it does so at the instruction of the lessee (e.g. specification of the vehicle). Under the leasing contract, the lessor then provides the lessee with the leased property for an agreed (typically non-terminable) contract term, for which the lessee pays a so-called leasing installment. When the leasing contract ends, the leased property is either returned to the leasing company, the contract is extended, a new contract is concluded or the leased property is purchased by the lessee. 29

Because of the long or even non-terminable contract periods, the leasing business *per se* only poses a low risk of money laundering. This risk assessment was also confirmed in the National Risk Assessment Report of the interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF) of 2015. 30

31 Pursuant to Article 11 para. 4bis AMLO-FINMA, the financial intermediary may waive the duty of diligence

- if the leasing contract is a finance lease and
- the annual leasing installments to be paid, including VAT, do not exceed CHF 5,000.

32 Although the ordinance and the materials are silent on whether the amount of CHF 5,000 can be cumulated for several leasing contracts from the same lessee, this is clearly to be denied in practice due to the analogous application of Art. 11 para. 4 AMLO-FINMA. A systematic interpretation of Art. 11 GwV-FINMA and its materials also leads to the same conclusion, because the legislator already speaks out against increasing the threshold due to the **cumulation** of individual limits in its explanations on *e-money*.

33 The cases of application of Art. 11 para. 4bis AMLO-FINMA are of minor importance in practice because the leasing installments usually exceed the amount of CHF 5,000 anyway, and, should this not be the case in exceptional cases, the costs of implementing a separate process for the leasing companies would be greater than the savings from the simplifications. In this respect, the exemption is likely to be relevant only for those leasing companies that focus primarily on small contracts with installments of less than CHF 5,000.

F. Further exemptions (Art. 11 para. 5 GwV-FINMA)

34 This provision allows FINMA to exempt further business areas or products from the due diligence requirements in individual cases, as needed and taking into account changes in circumstances over time, upon **request.** The prerequisite for this is that the financial intermediary or SRO making the request is able to demonstrate that the business relationship is of a lasting nature and that the risk of money laundering is low to very low as defined in Article 7a AMLA.

VI. LEGAL EFFECT OF THE EXCEPTIONS

35 A financial intermediary who operates in the area of exceptions may dispense with the duty to exercise due diligence (Art. 3–7 AMLA). Nevertheless, the financial intermediary remains **subject to** the law. This is apparent, for example, in the duty to comply with organizational measures (Art. 8 AMLA) and the

duty to report (Art. 9 AMLA). It should be noted that the documentation requirement also continues to apply, even though Art. 7 AMLA, which governs the documentation requirement, would actually be among the excluded obligations. A complete waiver of compliance with the due diligence requirements would not be permissible under the FATF recommendations. Furthermore, Art. 11 para. 4 AMLO-FINMA clarifies that Art. 14 and Art. 20 AMLO-FINMA on the monitoring of transactions and, where applicable, Art. 10 AMLO-FINMA must also be complied with when applying the simplified due diligence measures within the meaning of Art. 7a AMLA.

BIBLIOGRAPHY

Jutzi, Thomas, in: Kunz, Peter V./Jutzi, Thomas/Schären, Simon (Hrsg.), Geldwäschereigesetz, Stämpflis Handkommentar, Bern 2017.

Müller, Thomas/Nagel, Thomas, in: Hsu, Peter Ch./Flühmann, Daniel (Hrsg.), Basler Kommentar zum Geldwäschereigesetz, Basel 2021.

Wyss, Ralph, in: Thelesklaf, Daniel/Wyss, Ralph/Zollinger, Dave/van Thiel, Mark (Hrsg.), GwG Kommentar, 3. Aufl., Zürich 2019.

MATERIALS

Anhörungsbericht zur Geldwäschereiverordnung-FINMA vom 3.6.2015, abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/anhoerungen/abgeschlossene-anhoerungen/gwv-finma-revision/ab_gwv_finma_20150603_de.pdf?sc_lang=de&hash=D5FF3F2FA92310BDB3F0CEA40B231191, zuletzt besucht am 20.1.2025 (zit. Anhörungsbericht GwV-FINMA 2015).

Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz, Juni 2015, abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/42572.pdf, zuletzt besucht am 25.1.2025.

Botschaft zur Umsetzung der revidierten Empfehlungen der Groupe d'action financière (GAFI) vom 15.6.2007, BBl 2007 6269, abrufbar unter https://www.fedlex.admin.ch/eli/fga/2007/938/de, zuletzt besucht am 20.1.2025 (zit. Botschaft GAFI 2007).

Erläuterungsbericht zur Geldwäschereiverordnung-FINMA (GwV-FINMA) vom 8.6.2010, abrufbar unter https://www.finma.ch/de/~/media/finma/importiertedokumente/regulierung/anhoerungen/25-zusammenfuerung-gwv/erlaeuterungsbericht-geldwaeschereiverordnung-finma-20100611-de.pdf?sc_lang=de&hash=33AB93C142CA19582D12724D253BF229, zuletzt besucht am 20.1.2025 (zit. Erläuterungsbericht GwV-FINMA 2010).

FATF-Empfehlungen 2012 (updated November 2023), abrufbar unter: https://www.fatf-gafi.org/content/dam/fatfgafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf, zuletzt besucht am 20.1.2025.

FATF Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services, June 2013, abrufbar unter: https://www.fatfgafi.org/en/publications/Fatfrecommendations/Rba-npps-2013.html, besucht am 20.1.2025.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 8 AMLA

A commentary by Thomas Nagel / Delia Zellweger

SUGGESTED CITATION

Thomas Nagel/Delia Zellweger, Commentary of art. 8 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Nagel/Zellweger, art. 8 AMLA N. XXX

Art. 8 Organisational measures

Financial intermediaries must take the measures that are required to prevent money laundering and terrorist financing in their field of business. They must in particular ensure that their staff receive adequate training and that checks are carried out.

CONTENT

I. General 247
II. Organizational measures in detail 248
A. New products, business practices and technologies (Art. 23 MLO-FINMA) 248
B. Money Laundering Reporting Office (Articles 24 and 25 MLO-FINMA) 249
1. General 249
2. Personnel requirements for the anti-money laundering unit 250
3. Tasks of the anti-money laundering unit 250
C. Decision-making authority for reporting (Art. 25a MLO-FINMA) 253
D. Internal directives (Art. 26 MLO-FINMA) 253
1. General 253
2. Increased risks 254
3. Transaction monitoring 254
4. Involvement of the anti-money laundering unit 254
5. Staff training 254
6. Politically exposed persons (PEPs) 255
7. Reporting 255
8. Involvement of third parties 256
9. Further allocation of tasks and responsibilities 256
10. Updating customer records 256
E. Integrity and training 257
III. Legal consequences of violating Article 8 AMLA 258
Bibliography 258
Materials 259

I. GENERAL

Art. 8 stipulates that financial intermediaries must take the necessary **measures in** their field to prevent money laundering and terrorist financing. These include, but are not limited to ("**in particular**"), adequate **training of** personnel and **controls**. This is to ensure that the provisions of the AMLA are complied with throughout the entire business. Due to the clear wording of the law, Art. 8 AMLA applies only to financial intermediaries in accordance with Art. 2 para. 1 let. a AMLA, but not to dealers in accordance with Art. 2 para. 1 let. b AMLA. 1

The content and purpose of the standard are disputed in legal doctrine. Some legal scholars are of the opinion that Art. 8 AMLA represents an **independent due diligence requirement** in that it requires financial intermediaries to establish an organization that prevents money laundering and terrorist financing to the greatest extent possible. Another school of thought interprets Art. 8 AMLA as a pure implementing provision that serves to implement the due diligence requirements in Art. 3–7 AMLA. Jutzi combines the two views and assumes a hybrid function of Art. 8 AMLA. In his opinion, Art. 8 AMLA is an independent due diligence requirement based on a systematic and grammatical interpretation. This means that it is, on the one hand, a provision for implementing the other due diligence requirements of the AMLA and, at the same time, an independent due diligence requirement. The message on the AMLA does not help with the interpretation, but only repeats the legal text. According to the view presented here, Art. 8 AMLA is embedded in Chapter 2 of the AMLA (and thus in the due diligence requirements), but in most cases has no independent significance. Art. 8 AMLA serves to ensure consistent compliance with the due diligence requirements. Accordingly, in practice it is hardly possible for Art. 8 AMLA to be violated in isolation. A violation of Art. 8 MLA is usually accompanied by a violation of another due diligence requirement of the MLA in the narrower sense (e.g. the documentation requirement or the reporting requirement). For example, it may happen that the contracting party is not correctly identified because the training concept or the instructions were insufficient. In order for a financial intermediary to be able to consistently comply with the obligations, it is often a prerequisite that Art. 8 AMLA be fulfilled. According to the view presented here, Art. 8 AMLA is a due diligence obligation, but, strictly speaking, it is hardly independent. 2

3 The scope of the standard, i.e. the scope and type of organizational measures to be taken in connection with the prevention of money laundering and terrorist financing, are not specified in Art. 8 AMLA. However, the measures are **described in detail** in the **FINMA Anti-Money Laundering Ordinance**. For financial intermediaries supervised by self-regulatory organizations (Art. 2 para. 3 AMLA), the implementing provisions can be found in the regulations of the responsible self-regulatory organization. The risk-based approach applies when implementing Art. 8 AMLA. Depending on the size and area of activity of a financial intermediary, these can vary greatly. It can be seen from Art. 8 AMLA that the financial intermediaries must take action in "their area". The organizational measures must therefore relate to financial transactions within the meaning of Art. 1 AMLA and/or financial intermediary activities; it must be ensured that the necessary organizational competence (factual and formal) is vested in the most senior executive body in these areas. According to Federal Supreme Court rulings, the organizational measures must also be documented. The duty under Art. 8 AMLA is therefore a permanent duty that must always be observed. The measures taken must be regularly evaluated and, if necessary, adapted.

II. ORGANIZATIONAL MEASURES IN DETAIL

4 Art. 23 ff. AMLO-FINMA substantiate Article 8 AMLA and explain the "organizational measures" mentioned. These will be discussed individually below. It should be noted that certain **special laws** (e.g. Article 3 paragraph 2 letter a Banking Act) contain organizational provisions that also cover the fight against money laundering. These will not be discussed further in this commentary.

A. New products, business practices and technologies (Art. 23 MLO-FINMA)

5 Pursuant to Art. 23 MLO-FINMA, the financial intermediary is responsible for **in advance assessing** the risks of money laundering and terrorist financing that may arise from the development of new products or business practices or from the use of new or further developed technologies and for **adequately recording**, limiting and monitoring these risks as part of risk management. Art. 23 MLO-FINMA is an application of Art. 13 para. 2 let. c MLO-FINMA and therefore refers primarily to cases in which there is no personal contact

with the contracting party and the beneficial owner, as well as to products, technologies and services related to virtual currencies.

As expressly stated in the wording of Article 23 MLO-FINMA, the review must be carried out **prior to the launch** of new or enhanced products, business practices and technologies. If the review reveals (potential) risks, these must be recorded, limited and monitored by the financial intermediary before making changes to the business model that may give rise to new risks. 6

B. Money Laundering Reporting Office (Articles 24 and 25 MLO-FINMA)

1. General

Arts. 24 and 25 AMLO-FINMA deal with the anti-money laundering unit. This acts as an operational body. Pursuant to Art. 24 (1) AMLO-FINMA, the financial intermediary is required to appoint one or more qualified persons as the anti-money laundering unit. Their main task is to advise and support line managers and management in implementing the AMLO-FINMA. However, this is without taking on responsibility, i.e. overall responsibility clearly remains with the financial intermediary's executive bodies and cannot be outsourced to lower-level employees. This is to prevent members of the management and board of directors of a financial intermediary from shifting the decisions "downwards" in the hierarchy. The board of directors of a joint-stock company has the non-transferable and irrevocable task of supervising the persons entrusted with the management of the company, in particular with regard to compliance with the law (Art. 716*a* para. 1 no. 5 of the Swiss Code of Obligations). As part of good governance, the anti-money laundering unit must therefore always be empowered by the internal regulations to submit sensitive decisions (e.g. on the continuation of a critical business relationship) to the management. Anything else can lead to a mixing of the compliance function and the commercially or operationally active persons, which in turn can lead to undesirable conflicts of interest. The decision on reports within the meaning of Article 9 AMLA lies with the most senior management body, which may, however, delegate this decision (Article 25*a* MLO-FINMA, see below, N. 15). In general, the anti-money laundering unit should be as independent as possible from the profit-oriented functions of a company in order to ensure the greatest possible independence and neutrality. On the basis of 7

Article 75 of the AMLO-FINMA, small asset managers are subject to relaxed requirements as compared to Article 24 of the AMLO-FINMA. Fintech institutions as defined in Article 1*b* of the Banking Act are also eligible for relaxed requirements in accordance with Article 75*a* (2) of the AMLO-FINMA.

2. Personnel requirements for the anti-money laundering unit

8 In Art. 24 para. 1 AMLO-FINMA, the legislator requires that "qualified persons" be appointed as the anti-money laundering unit. This means that the persons must have completed training in the field of law/compliance that meets the obligation to monitor and address business-specific risks. The appointed persons must have sufficient experience to be able to monitor compliance with the regulations and must also have a certain degree of credibility so that they can represent compliance issues with sufficient certainty and independence vis-à-vis the executive and the commercial or operational departments.

9 In certain cases, it is possible to appoint external persons as anti-money laundering officers as part of an outsourcing arrangement, provided that they are also "knowledgeable" (Art. 25 para. 4 AMLO-FINMA). On the one hand, an external knowledgeable person can and should be designated as an anti-money laundering officer if the financial intermediary cannot set up its own specialist unit due to its size. On the other hand, delegation can also occur when the establishment of an internal anti-money laundering unit would be disproportionate. When mandating external persons, the financial intermediary continues to bear responsibility for the execution of the ordinance (see "under its responsibility" in accordance with Article 25 (4) AMLO-FINMA). This means that it must carefully select, instruct and monitor the external service provider. Any misconduct on the part of the outsourcing service provider will be fully attributed to the outsourcing financial intermediary. If the financial intermediary is a bank, a securities firm or an insurance company, the rules of FINMA Circular 2018/3 must also be observed.

3. Tasks of the anti-money laundering unit

10 The core tasks of the anti-money laundering unit consist, on the one hand, of preparing internal directives for combating money laundering and terrorist financing and, on the other hand, of planning and monitoring the corresponding internal training (Art. 24 para. 2 in conjunction with Art. 25 et seq. AMLO-

FINMA). Furthermore, the anti-money laundering unit has a support function, i.e. it supports line managers and the executive bodies in implementing the AMLO-FINMA, without taking responsibility for this away from them (Art. 24 para. 1 second sentence AMLO-FINMA). The directives are issued by the board of directors or the most senior management body. These must be communicated to the persons concerned, i.e. the management and employees of the financial intermediary, in a suitable form (Art. 26 para. 1 AMLO-FINMA).

Article 25 AMLO-FINMA lists further tasks of the anti-money laundering unit, although these may also be assumed by another independent specialist unit (Article 25 (1) AMLO-FINMA). The anti-money laundering unit is obliged to monitor compliance with the internal directives on combating money laundering and terrorist financing in consultation with internal audit, the audit firm and line managers (Art. 25 para. 1 let. a AMLO-FINMA). It also defines the parameters for the transaction monitoring system pursuant to Article 20 MLO-FINMA (Article 25 (1) (b) MLO-FINMA) and ensures the careful evaluation of the reports generated by the system (Article 25 (1) (c) MLO-FINMA). In addition, it will initiate or conduct additional clarifications itself in accordance with Article 15 MLO-FINMA (Article 25 (1) (d) MLO-FINMA). Finally, it ensures that the responsible management body has all the information necessary to make well-founded decisions on entering into or continuing business relationships in accordance with Article 19 MLO-FINMA (Article 25(1)(e) MLO-FINMA). 11

Art. 25 para. 2 AMLO-FINMA sets out the risk analysis requirement. It requires the money laundering reporting office or another independent body to prepare a risk analysis taking into account the financial intermediary's area of activity and the type of business relationships it maintains, from the point of view of combating money laundering and terrorist financing. The risk analysis must in turn be approved by the board of directors or the management and updated periodically. The creation and maintenance of the risk analysis is thus a dynamic process that requires financial intermediaries to proactively identify, assess and manage their specific risks related to money laundering and terrorist financing. This analysis goes far beyond a mere review of regulations; rather, it is a strategic tool designed to enable financial intermediaries to strengthen their resilience to financial crime while protecting their reputation. 12

13 The scope of the risk analysis depends on the size and nature of the financial intermediary's business. The following parameters are taken into account:

- At the heart of risk analysis is a comprehensive view of the company and its environment. Both internal and external factors are taken into account. Internal factors include the products and services offered (expressly mentioned in Art. 25 para. 2 AMLO-FINMA), the organizational structure, IT systems and control mechanisms. External factors relate to the regulatory environment, the economic situation, the political climate and the company's geographical presence.
- An important aspect of risk analysis is knowing one's customers. Financial intermediaries must get to know their customers thoroughly in order to be able to assess their business activities and possible risks. In doing so, they scrutinize both the origin of the customers (registered office or domicile, expressly mentioned in Art. 25 para. 2 MLO-FINMA) and their business relationships. Financial intermediaries must pay particular attention to customers from high-risk countries, PEPs and complex financial products.
- The results of the risk analysis serve as a basis for developing customized risk mitigation measures. These measures may take the form of additional audits, enhanced monitoring measures or employee training, for example. It is important that the measures are regularly reviewed and adjusted to reflect changing circumstances.
- Risk analysis is not only a legal requirement, but can also be a strategic advantage. By proactively managing risk, companies can strengthen their competitiveness and protect their reputation as a reliable partner. In addition, risk analysis helps to increase the efficiency of compliance processes and reduce costs.

14 In summary, risk analysis in the prevention of money laundering is a complex and multifaceted process. It requires a thorough understanding of the applicable regulations, one's own business activities and the constantly changing regulatory and economic situation. Based on the results of the risk analysis, the financial intermediary determines the measures for managing, controlling, monitoring, reporting and supervising these risks. By consistently implementing the risk analysis, financial intermediaries can contribute to the fight against financial crime while protecting their own interests. In 2023, FINMA reviewed the risk analysis processes of over 30 banks and concluded that a

significant proportion of the risk analyses examined did not meet the basic requirements for such an analysis. In response, FINMA published Guidance 05/2023 on money laundering risk analysis in accordance with Article 25(2) of the FINMA Anti-Money Laundering Ordinance (AMLO-FINMA) (dated August 24, 2023), in which FINMA transparently presents its practical observations and experiences regarding risk analysis.

C. Decision-making authority for reporting (Art. 25a MLO-FINMA)

15 The financial intermediary's management must decide on the submission of reports in accordance with Art. 9 AMLA (reporting obligation) and Art. 305ter para. 2 SCC (right to report) (Art. 25*a* MLO-FINMA). However, this task may be delegated to one or more of its members who are not directly responsible for the business relationship, to the anti-money laundering unit or to a largely independent unit (Art. 25*a.* para. 2 AMLO-FINMA). If the task is delegated, responsibility for implementing the reporting obligations nevertheless remains with the executive body of the financial intermediary (Art. 24 para. 1 AMLO-FINMA). Art. 25a AMLO-FINMA only allows the delegation of the implementation of the reporting obligation, but does not allow the entire ordinance to be delegated. The responsibility for reporting must be recorded in the financial intermediary's directives (Art. 26 para. 2 let. b MLO-FINMA, see also below, N. 23).

D. Internal directives (Art. 26 MLO-FINMA)

1. General

16 The financial intermediary must issue internal directives to combat money laundering and terrorist financing. These are adopted by the board of directors or the executive board and brought to the attention of the persons concerned (Art. 26 para. 1 AMLO-FINMA). The purpose of the directives is to train and raise awareness among staff. In terms of content, the directives are a specification of the requirements of the AMLO-FINMA. The directives must be regularly reviewed after their issue and amended as necessary.

17 Article 26 (2) AMLO-FINMA contains a list of regulatory matters that the internal directives should cover. The list is not exhaustive. The following is a

brief discussion of the individual areas to be regulated in the internal directives.

2. Increased risks

18 According to Article 6 MLA, financial intermediaries must apply a risk-based approach. This requires them to define at least two client risk categories, which they use to decide what information and audit steps are necessary for an adequate assessment and monitoring of the business relationship. Various letters of Article 26, paragraph 2 of the AMLO-FINMA deal with the increased risks and what must be regulated in directives with regard to these risks: (i) the criteria applied to identify higher-risk business relationships in accordance with Art. 13 MLO-FINMA (lit. a); (ii) the criteria applied to identify higher-risk transactions in accordance with Art. 14 para. 1 and 2 MLO-FINMA (lit. b); and (iii) the modalities according to which the financial intermediary records , limited and monitored (lit. h). Lit. i also explicitly mentions that the amount limits of inflows and outflows must be determined to identify cases of increased risks (Art. 13 para. 2 lit. f and Art. 14 para. 2 lit. a MLO-FINMA).

3. Transaction monitoring

19 According to Article 20 (1) of the FINMA Anti-Money Laundering Ordinance, the financial intermediary shall ensure effective monitoring of business relationships and transactions and shall thus ensure that the increased risks are identified. Pursuant to Article 26 (2) (c) of the FINMA Anti-Money Laundering Ordinance, a directive must be issued that sets out the principles of this transaction monitoring. The relevant criteria from a business policy and/or regulatory perspective must be included.

4. Involvement of the anti-money laundering unit

20 According to Art. 26 (2) (d) AMLO-FINMA, a directive is required stating the cases in which the internal anti-money laundering unit must be involved and the management must be informed.

5. Staff training

21 The principles of employee training must also be set out in a directive (Art. 26 (2) (e) MLO-FINMA). This means that each financial intermediary must define the details regarding the implementation, supervision and content of the

training, as well as the documentation and monitoring. The consequences for employees who do not satisfactorily complete the training must also be set out.

6. Politically exposed persons (PEPs)

The business policy with regard to politically exposed persons (PEPs) is to be set out in directives (Art. 26 para. 2 let. f AMLO-FINMA). This includes a financial intermediary defining which PEPs can be accepted as clients under which circumstances and subject to which requirements. Special requirements may include, for example, more stringent checks, decisions by executive bodies and further approval processes. The modalities by which a financial intermediary records increased risks also include the handling of PEPs (Art. 26 para. 2 let. h MLO-FINMA). 22

7. Reporting

In accordance with Article 26 (2) (g) of the FINMA Anti-Money Laundering Ordinance, a directive must also be issued to specify who is responsible for reporting to the Money Laundering Reporting Office. In principle, reporting to the Money Laundering Reporting Office is the last step in an extensive clarification process. According to Art. 25a MLO-FINMA, it is the responsibility of the financial intermediary's most senior management body to decide on reporting in accordance with Art. 9 AMLA and Art. 305bis para. 2 SCC. This responsibility can be delegated to one or more of its members who are not directly responsible for the business relationship in question. It can also be delegated to the anti-money laundering unit or to a largely independent body. The aim of this regulation is to avoid potential conflicts of interest that could arise if members of the executive board also manage client relationships themselves and would thus be involved in the decision-making process regarding whether or not to report. However, the overall responsibility for compliance with the reporting requirement under supervisory law remains with the board of directors or the management (see Art. 24, para. 1, GwV-FINMA), while the delegation merely concerns the implementation of the associated tasks. 23

8. Involvement of third parties

24 Subject to certain conditions, the financial intermediary may, in accordance with Article 28(1) of the Ordinance on the Prevention of Money Laundering in the Financial Sector (MLO-FINMA), appoint persons and companies to carry out the identification of the contracting party, the establishment of the controlling person or the beneficial owner of the assets, as well as additional clarification duties. It is necessary to conclude a written agreement with the delegated person, except when the delegation occurs within a group or a conglomerate with uniform due diligence standards or to another financial intermediary that is subject to comparable supervision and regulation to combat money laundering and terrorist financing. On-site inspections at the delegate's premises are not required. The delegatee is expressly prohibited from subdelegating the assigned tasks (see Article 28(3) AMLO-FINMA). The delegating financial intermediary continues to bear full responsibility and liability for any deficiencies, as if they were the delegating financial intermediary's own governing or executive bodies or employees. In addition, the financial intermediary is obliged to obtain a copy of all documents used to fulfil the due diligence requirements. He must obtain written confirmation that the copies provided correspond to the original documents (see Art. 29 (2) MLO-FINMA). The criteria for the involvement of third parties must be set out in a directive in accordance with Art. 26 (2) (j) MLO-FINMA. Cf. also the comments on Art. 3 and 4 regarding delegation.

9. Further allocation of tasks and responsibilities

25 The remaining internal allocation of tasks and responsibilities between the anti-money-laundering unit and the other business units entrusted with the duty to exercise due diligence must also be set out in a directive (Art. 26 para. 2 let. k AMLO-FINMA). This is to enable a clear distinction between the *first line of defense* and the *second line of defense*, which has been established in practice and adopted in Art. 26 (2) (k) AMLO-FINMA. Furthermore, a clear allocation of tasks should define the responsibilities.

10. Updating customer records

26 Finally, Art. 26 para. 2 let. l MLO-FINMA requires a directive on the updating of client records. This provision is based on Art. 7 para. 1bis AMLA. This legal provision was newly inserted into the AMLA with effect from January 1, 2023

(see the commentary on Art. 7). The intervals at which client records must be updated depend on external circumstances (e.g. indications of a change in the contracting party, beneficial owners or controlling persons) and on the specific risks of the client relationship (the files of high-risk clients must be updated more regularly than those of low-risk clients).

E. Integrity and training

. Integrity and appropriately trained staff are essential in the fight against money laundering and terrorist financing. Art. 27 (1) of the Money Laundering Ordinance-FINMA explicitly states this. This requirement primarily applies to employees of the financial intermediary who have contact with clients, their superiors and all persons who are involved in the financial intermediary activity itself or in the activity of the anti-money laundering unit. The recruitment of personnel who meet the requirements of Article 27 (1) GwV-FINMA is part of proper business management. Checking integrity is a difficult undertaking and usually consists of obtaining extracts from the debt collection and criminal records, as well as a differentiated recruitment procedure (checking CVs, references and other relevant aspects). In the case of prudentially supervised institutions, the examination of integrity is usually ensured by further express guarantee regulations and corresponding audit procedures by FINMA (see, for example, Art. 11 FINIG). The required integrity is to be understood comprehensively. Integrity means acting according to firm moral and ethical principles and remaining true to them, even in difficult situations (e.g. in the event of conflicting objectives within the company). Integrity is not limited to mere compliance with the law, but goes beyond it: ethical behavior, honesty and reliability are also part of integrity. On the one hand, it should ensure that clients cannot use the financial intermediary for money laundering or terrorist financing. On the other hand, it should also guarantee that employees and governing bodies do not themselves commit criminal acts (whether knowingly or not). 27

In addition to the careful selection of personnel, the financial intermediary must also ensure regular training for all employees concerned (Art. 27 para. 2 AMLO-FINMA). The criterion of the training obligation can relate to internal and external persons (in the case of delegation of duties). The training should cover the aspects of combating money laundering and terrorist financing that are relevant for the respective employee. This includes, on the one hand, a 28

basic understanding of the legal and reputation-related risks and, on the other hand, aspects that are specific to the employee's respective function. This is to ensure that all employees involved comply with the processes and that a tight-knit and meaningful anti-money laundering system is implemented. Furthermore, this should create a corporate and compliance culture that results in lawful behavior by all parties involved and does not create false incentives (e.g. no rewarding of behavior that is illegal or borders on illegality).

III. LEGAL CONSEQUENCES OF VIOLATING ARTICLE 8 AMLA

29 A deficiency in or violation of the requirements of the organizational measures may result in consequences under supervisory and criminal law. For those subject to FINMA, there is a risk of the opening of enforcement proceedings, in the course of which FINMA can apply its supervisory instruments in accordance with Art. 29 et seq. of the FINMASA. According to Art. 25 para. 3 let. c MLA, the self-regulatory organizations must issue regulations that, among other things, define appropriate sanctions. If a financial intermediary under the supervision of a self-regulatory organization violates Art. 8 MLA or the implementing provisions of the regulations of the self-regulatory organization, the competent self-regulatory organization may apply the sanction mechanisms contained in the regulations.

30 Under Article 102 SCC, a company can be fined up to CHF 5 million if it has not taken all necessary and reasonable organizational precautions to prevent crimes such as money laundering under Article 305bis SCC; the amount of the fine depends on the severity of the organizational deficiency, the damage caused and the economic capacity of the company. The failure to comply with internal company anti-money laundering regulations (and thus a violation of Art. 8 AMLA) can thus be an indication of inadequate organization in accordance with Art. 102 StGB.

BIBLIOGRAPHY

De Capitani Werner, Kommentierung zu Art. 8 GwG, in: Schmidt Niklaus (Hrsg.), Kommentar Einziehung – Organisiertes Verbrechen – Geldwäscherei, Bd. I, 2. Aufl., Zürich et al. 2007 (zit. KEOVG II-De Capitani, Art. 8 GwG).

Forster Michael, Die strafrechtliche Verantwortlichkeit des Unternehmens nach Art. 102 StGB, Bern 2006 (zit. Forster, Verantwortlichkeit).

Jutzi Thomas, Kommentierung zu Art. 8, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg,), Stämpflis Handkommentar zum Geldwäschereigesetz (GwG), Bundesgesetz vom 10. Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Bern 2017 (zit. SHK-Jutzi, Art. 8 GwG).

Meyer Patrick K./ Ryhner Samuel, Kommentierung zu Art. 4, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021 (zit. BSK-Meyer/Ryhner, Art. 4 GwG).

Nagel Thomas, Interessenskonflikte des Compliance Officers: Mit besonderer Betrachtung der Meldepflicht nach Art. 9 GwG, SJZ 2021, S. 102–109 (zit. Nagel, SJZ 2021).

Peyer Martin, Kommentierung zu Art. 8, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021 (zit. BSK-Peyer, Art. 8 GwG)

Schott Ansgar/Kessler Martina A., Kommentierung zu Art. 8a, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar zum Geldwäschereigesetz (GwG), Bundesgesetz vom 10. Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Bern 2017 (zit. SHK-Schott/Kessler, Art. 8a GwG).

Taube Tamara, Entstehung, Bedeutung und Umfang der Sorgfaltspflichten der Schweizer Banken bei der Geldwäschereiprävention im Bankenalltag, Zürich et al. 2013 (zit. Taube, Sorgfaltspflichten).

Wyss Ralph, Kommentierung zu Art. 8, in: Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell Füssli Kommentar, Geldwäschereigesetz, 3. Aufl., Zürich 2019 (zit. OFK-Wyss, Art. 8 GwG).

MATERIALS

Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Gelwäschereigesetz) vom 17.6.1996, BBl 1996 III 1101 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1996/3_1101_1057_993/de, besucht am 31.8.2024 (zit. Botschaft GwG 1996).

Erläuterungsbericht zur Totalrevision der Geldwäschereiverordnung-FINMA (GwV-FINMA) vom 11.2.2015, abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/anhoerungen/abgeschlossene-anhoerungen/25-zusammenfuehrung-der-geldwaeschereiverordnungen-der-finma/erlaeuterungsbericht-geldwaeschereiverordnung-finma-20100611-de.pdf?sc_lang=de&hash=0F2352A48C31F45C8213AEBB0C553E25, besucht am 31.8.2024 (zit. Erläuterungsbericht GwV-FINMA 2015).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 8a AMLA

A commentary by Thomas Nagel

SUGGESTED CITATION

Thomas Nagel, Commentary of art. 8a AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Nagel, art. 8a AMLA N. XXX

Section 1*a* Dealers' Duties of Due Diligence

Art. 8*a*

[1] Dealers under Article 2 paragraph 1 letter b must fulfil the following duties if they accept more than 100,000 francs in cash in the course of a commercial transaction:

a. verification of the identity of the customer (Art. 3 para. 1);

b. establishing the identity of the beneficial owner (Art. 4 para. 1 and 2 let. a and b);

c. duty to keep records (Art. 7).

[2] They must clarify the economic background and purpose of a transaction if:

a. it appears unusual, unless its legality is clear;

b. there are indications that assets are the proceeds of a felony or an aggravated tax misdemeanour under Article 305bis number 1bis SCC or are subject to the power of disposal of a criminal or terrorist organisation (Art. 260ter SCC) or serve the financing of terrorism (Art. 260^{quinquies} para. 1 SCC).

[3] Dealers are subject to the duties under paragraphs 1 and 2 even if the cash payment is made in two or more instalments and the individual instalments are less than 100,000 francs, but when added together exceed this amount.

[4] They are not subject to the duties if the payments that exceed 100,000 francs are made through a financial intermediary.

[5] The Federal Council shall specify the details of the duties under paragraphs 1 and 2 and stipulate how they are to be fulfilled.

CONTENT

I. General 264
II. Due diligence requirements for dealers 264
A. General 264
B. Identifying the contracting party (Art. 8a para. 1 let. a in connection with Art. 3 para. 1 AMLA and Art. 17 AMLO) 265
C. Identifying the beneficial owner (Art. 8a para. 1 let. b in conjunction with Art. 4 para. 1 and 2 let. a and b AMLA and Art. 18 AMLO) 265
D. Documentation requirement (Art. 8a para. 1 let. c in conjunction with Art. 7 AMLA in conjunction with Art. 21 AMLO) 267
E. Additional clarifications (Art. 8a para. 2 AMLA in conjunction with Art. 19 AMLO) 267
F. Amount threshold and circumvention (Art. 8a paras. 1 and 3 AMLA) 268
III. Involvement of third parties (Art. 16 AMLO and Art. 8a para. 4 AMLA) 269
IV. Legal consequences of violating the due diligence requirements 269
V. Additional obligations 270
VI. De facto ban on cash payments over 100,000 francs 270
Bibliography 271
Materials 272

I. GENERAL

1 According to Art. 2 para. 1 let. b AMLA, so-called "dealers" are covered by the AMLA in addition to financial intermediaries. According to the law, dealers are natural or legal persons who trade **in goods on a commercial basis and accept cash in payment**. The terms "dealer", "commercial trade" and "goods", which are used in Art. 2 para. 1 let. b AMLA, are defined in Art. 13–15 AMLO. For more information on these terms, the history of the dealer provisions, the FATF provisions and EU law, please refer to the commentary on Art. 2 para. 1 AMLA (N. 18 ff.).

2 The AMLA applies only to persons who, in the course of a commercial activity as dealers in goods, accept cash in the amount of **more than CHF 100,000** (see Art. 8a para. 1 AMLA). The due diligence requirements of Art. 8a para. 1 AMLA thus limit the personal scope of the AMLA for dealers.

II. DUE DILIGENCE REQUIREMENTS FOR DEALERS

A. General

3 The dealer **due diligence requirements** under Art. 8a AMLA are specified in Art. 17–21 AMLO (see Art. 8a para. 5 AMLA). The law explicitly refers to the duties that apply to financial intermediaries. In particular, the duties for financial intermediaries that relate to spot transactions are applicable to dealers. Deviations for dealers can only be assumed if explicitly defined rules to the contrary are set out in the law or in the ordinances. Accordingly, reference is made at this point to the comments on Art. 3, Art. 4 and Art. 7 AMLA. The comments contained therein can be applied to dealers, unless the provisions of Art. 8a AMLA in conjunction with 17–21 AMLO-FINMA deviate from the AMLA provisions on financial intermediaries.

4 The due diligence requirements for dealers require the **cooperation of the contracting party** of the dealer (i.e. the buyer) or the representative acting on behalf of the dealer. Without their cooperation, the dealer cannot fulfill the obligations and is required not to accept the cash payment of CHF 100,000.

B. Identifying the contracting party (Art. 8a para. 1 let. a in connection with Art. 3 para. 1 AMLA and Art. 17 AMLO)

A merchant who accepts more than CHF 100,000 must identify the contracting party (i.e. the buyer). The merchant **must establish the person's surname, first name, address, date of birth and nationality** (Art. 17 para. 1 AMLO), unless the use of this information is not customary in the person's country of origin (Art. 17 para. 2 AMLO). The person must be identified by inspecting the original of an official form of identification, i.e. passport, ID card or driver's license (Art. 17 para. 3 lit. a AMLO). The merchant must check whether the ID can be assigned (Art. 17 para. 3 let. b AMLO), make a copy of the ID (Art. 17 para. 3 let. c AMLO) and note on the copy that the original has been inspected (Art. 17 para. 3 let. d AMLO). The copy must be kept (documentation requirement, see Art. 21 AMLO). Unlike financial intermediaries (see FINMA Circular 2016/7), traders are not required to identify the contracting party via digital channels. 5

The contracting party to be identified is the person who purchases the goods from the dealer and thus becomes the **owner of the** goods. The representative who may act on behalf of the buyer does not need to be identified. If the representative acts on the basis of a power of attorney, the information on the buyer contained in the power of attorney must match the information determined by the dealer. A representative must either provide the information in accordance with Article 17, para. 1 AMLO if the buyer is a natural person or the company name and registered office of the buyer if the buyer is a legal entity (Article 17, para. 4 AMLO). 6

C. Identifying the beneficial owner (Art. 8a para. 1 let. b in conjunction with Art. 4 para. 1 and 2 let. a and b AMLA and Art. 18 AMLO)

A dealer is obliged to determine the identity of the beneficial owner (Art. 8a para. 1 let. b in conjunction with Art. 4 para. 1 and 2 let. a and b AMLA) by asking the contracting party or the contracting party's representative whether the contracting party is the beneficial owner of the cash to be handed over (Art. 18 para. 1 AMLO). In other words, it must be determined whose money or on whose account the goods were purchased by the dealer. In simple terms, it is about who “owns” the cash. This determination can be legally 7

complex. If the contracting party is not the beneficial owner, the dealer must request a **written declaration** from the contracting party or the contracting party's representative stating the identity of the beneficial owner (Art. 18 para. 2 AMLO). The written declaration may be made using the form or document referred to in Art. 21 AMLO and Annex 1 AMLO (Art. 18 para. 6 AMLO). The beneficial owners are the natural persons on whose account the purchase is made (Art. 18 para. 2 let. a AMLO). The beneficial ownership of the object of purchase is not required in itself – even if, according to the view represented here, the explanatory report on the AMLO is to the contrary – (and in exceptional cases this may differ from the beneficial ownership of the cash). In principle, the beneficial owner(s) is/are one or more natural persons. In the case of an acquisition for the account of an unlisted, operationally active legal entity or partnership, the beneficial owners are either the natural persons who have voting rights or capital of at least 25 percent directly or indirectly, alone or in concert with third parties (Art. 18 para. 2 lit. b no. 1 AMLO), or natural persons who exercise control in some other way (e.g. by directly influencing business activities) (so-called control holders, Art. 18 para. 2 lit. b no. 2 AMLO). In the case of legal entities, the dealer is therefore obliged to ask the contracting party about the ownership and control structure (e.g. powers of attorney or shareholder agreements). If no beneficial owners can be identified, the identity of the most senior member of the governing body must be established (Art. 18 para. 3 AMLO). In the case of companies listed on the stock exchange, the beneficial owners do not have to be identified. If it is an association or a foundation that has no beneficial owner, this must be recorded accordingly (Art. 18 para. 7 AMLO). To identify the beneficial owners, the dealer requires the following information: first name and last name, address, date of birth and nationality (Art. 18 para. 4 AMLO).

8 Even though the duty to identify the beneficial owner is modeled on and even explicitly refers to Article 4 AMLA, there are **some differences**: the object of beneficial ownership is always cash (Art. 18, para. 1 AMLO). Furthermore, Art. 18 AMLO seems to deviate from the definition of beneficial ownership in Art. 4. This is probably largely due to the questionable decision of the legislator to link to Art. 4 AMLA on the one hand and to formulate an order to the Federal Council to further specify the duty for dealers in accordance with Art. 8a para. 2 AMLA at the ordinance level on the other.

D. Documentation requirement (Art. 8a para. 1 let. c in conjunction with Art. 7 AMLA in conjunction with Art. 21 AMLO)

According to the legal provisions, dealers are obliged to document the fulfillment of their due diligence obligations, whereby the provision for dealers refers to the regulation for financial intermediaries (Art. 8a para. 1 lit. c in conjunction with Art. 7 AMLA). The form of the documentation is largely unrestricted, as long as it contains all the relevant information about the contracting party, allows for a review by the auditors and ensures that any request for information or seizure can be fulfilled within a reasonable period of time (see Art. 7 para. 2 AMLA). A sample form is provided in **Annex 1 of AMLO**, but its use is optional (Art. 21 para. 1 AMLO). This form or another document must be used to record the customer's details (Art. 17 and 18 AMLO), the additional clarifications (Art. 19 AMLO) and the submission of a report (Art. 20 AMLO) (Art. 21 para. 2 AMLO). The records must be created promptly, dated (date of purchase), signed and stored physically or electronically for a period of ten years (Art. 21 para. 3 and 4 AMLO), whereby dealers must observe the FADP. 9

E. Additional clarifications (Art. 8a para. 2 AMLA in conjunction with Art. 19 AMLO)

Art. 8a para. 2 AMLA is the **counterpart for dealers to the special due diligence requirements** of Art. 6 AMLA for financial intermediaries, but is less extensive in content. If a transaction seems unusual to a dealer or there are indications of money laundering, he must check the background to the transaction and its purpose more closely (Art. 8a para. 2 AMLA). The review must be carried out without delay, in particular because the report that may subsequently have to be drawn up (Art. 9 para. 1bis AMLA) must be made without delay. The review is carried out by the merchant asking the contracting party or the representative about the background and purpose of the purchase, assessing the information for plausibility and recording the clarifications in writing (Art. 19 para. 3 AMLO). These additional clarifications may be necessary if the information gathered in accordance with Art. 17 and 18 AMLO is insufficient to provide the merchant with a clear picture of the business and the origin of the cash. They serve to improve the customer-related risk profile. A payment of CHF 100,000 in cash is not unusual *per se*. 10

11 What appears unusual to one merchant may be perfectly normal for another. Each merchant must **individually assess** when a transaction is unusual and thus when additional clarifications are required, based on the type of business, the usual clientele, experience and the location of the business itself.

12 Art. 19 para. 2 AMLO lists some possible **indications of money laundering** ("in particular") and does not do so exhaustively. Indications of money laundering include, for example, if the person pays predominantly with banknotes of small nominal value, if mainly easily sold goods with a high degree of standardization are purchased, if the person provides no or insufficient information for their identification or to establish the identity of the beneficial owner in accordance with Article 18 AMLO, if the person provides obviously false or misleading information or if there are doubts as to the authenticity of the identification documents presented. The list is based on the analogous regulation for financial intermediaries in the appendix to AMLO-FINMA, but is tailored to purchasing transactions. If dealers recognize such indications, they are obliged to carry out further clarifications. However, the presence of an indication does not automatically mean that a report must be made to MROS immediately. A report must be made if the initial suspicion is confirmed in the course of additional clarifications or if the suspicion cannot be dispelled (Art. 9 para. 1bis AMLA).

F. Amount threshold and circumvention (Art. 8a paras. 1 and 3 AMLA)

13 Art. 8a AMLA is linked to the **threshold of CHF 100,000 in cash**. Foreign currencies must be converted into francs on a daily basis in order to assess the applicability of Art. 8a AMLA. However, the obligations under Art. 8a paras. 1 and 2 AMLA also apply if the cash payment is made in several tranches and the individual tranches are less than CHF 100,000 but exceed this amount when added together (Art. 8a para. 3 AMLA, so-called "smurfing"). As soon as several transactions between the same parties are carried out in close temporal or economic connection, the partial amounts are added together, which may lead to the seller being recorded as a dealer subject to AMLA. This is the case, for example, with an installment payment of a total amount of over CHF 100,000. Various commercial transactions between the same parties that are not economically or temporally related are to be considered separate pur-

chases that do not trigger the applicability of Art. 8a AMLA. This distinction can be difficult to make in practice.

The amount threshold of CHF 100,000 is remarkably high in **comparison to other countries** (EU: EUR 10,000). For precious stone and precious metal traders, the latest bill to amend the AMLA (draft and message of May 22, 2024) provides for the thresholds to be lowered to 15,000 francs in order to be compliant with the FATF recommendations. The bill will be discussed by parliament in the near future (as of the end of August 2024). In my opinion, the amendment is to be welcomed, as the thresholds of the Swiss AMLA are far too high compared to EU-related countries and therefore there is potential for money laundering. 14

III. INVOLVEMENT OF THIRD PARTIES (ART. 16 AMLO AND ART. 8A PARA. 4 AMLA)

If dealers involve a third party to carry out the transaction and to accept the purchase price in cash, the dealers must, regardless of their legal relationship with the third party, **ensure that the due diligence and reporting requirements are complied with by the third party** (Art. 16 AMLO). If the purchase price is received in cash on behalf of the dealer (without processing), this is not subject to the AMLA, as this constitutes a collection service that is not subject to the AMLA (see Art. 2 para. 2 let. a no. 2 AMLO). If the third party is a financial intermediary, Art. 8a para. 4 AMLA applies, i.e. the dealer is not subject to the AMLA for the cash sale, but the third party is subject to it as a financial intermediary. Traders therefore have a choice: either they accept the cash and have to fulfill the AMLA obligations, or they persuade their customers to pay the debt through a financial intermediary (e.g. by bank transfer). 15

IV. LEGAL CONSEQUENCES OF VIOLATING THE DUE DILIGENCE REQUIREMENTS

The AMLA does **not provide for any criminal penalties** for dealers who violate the due diligence requirements under Article 8a AMLA. Only the violation of the reporting requirement (Article 37 AMLA) and the violation of the requirement to commission an auditor to verify compliance with the requirements (Article 38 AMLA) are subject to criminal penalties. The penal provisions of the FINMASA do not apply to dealers. Dealers can be held criminally 16

liable under Art. 305bis SCC for knowingly and willingly participating in or failing to act (the AMLA obligations establish a corresponding guarantor position). However, Art. 305ter SCC does not apply to dealers. There are no regulatory consequences to be feared, since dealers are not subject to the supervision of a self-regulatory organization or FINMA. For the penal provisions and the criticism in this regard, please refer to the comments on Art. 37 and Art. 38.

V. ADDITIONAL OBLIGATIONS

17 In addition to the due diligence requirements under Art. 8a AMLA (clarified in Art. 17 et seq. AMLO), dealers under Art. 9 para. 1bis AMLA must file a **report if** certain suspicious facts arise. In this regard, reference is made to the commentary on Art. 9 AMLA.

18 Dealers must **appoint auditors** to verify their compliance with the AMLA obligations that apply to them (Art. 15 AMLA). Please refer to the commentary on Art. 15 AMLA.

19 In doctrine, it is also argued that dealers – despite the absence of an explicit provision in the law or the ordinance – are also required to take **organizational measures** to comply with the obligations incumbent on them. This suggests – as noted in the commentary on Art. 8 AMLA (see N. 2) – that the organizational duty is not a separate due diligence requirement, but rather a prerequisite for compliance with the AMLA obligations. In my view, a merchant who violates his obligations under Art. 8a AMLA due to inadequate organization would not be guilty of violating Art. 8 AMLA. This is not possible due to the lack of a reference in Art. 8a AMLA to Art. 8 AMLA. In the event of inadequate organization and the commission of a criminal offense within the dealer's company, criminal liability under Art. 102 SCC may result under certain circumstances.

VI. DE FACTO BAN ON CASH PAYMENTS OVER 100,000 FRANCS

20 When the merchant provisions were created, it was already being predicted by academics and legislators that the regulation would lead to a de facto ban on cash payments of over 100,000 francs. This is because compliance with the obligations involves much higher costs and hardly any advantages com-

pared to involving an external financial intermediary. In my opinion, this prediction has come true. Traders have little need for advice and rarely report anything to MROS, which suggests that amounts over 100,000 are processed with the help of a financial intermediary (Art. 8a para. 4 AMLA). A follow-up question from the author to some audit firms revealed that they either have no or only very few mandates from traders. The AMLA provisions for dealers are thus neglected and, in my opinion, can be described as a "**non-starter**" – it would be less costly to completely ban cash payments above a certain threshold. Whether this is appropriate is a political question that is not easy to answer.

BIBLIOGRAPHY

Attinger Alex, Wirtschaftliche Berechtigung: Konzepte und Dogmatik, Zürich 2023, abrufbar unter https://boris.unibe.ch/193100/1/Attinger_Wirtschaftliche_Berechtigung.pdf, besucht am 31.8.2024 (zit. Attinger).

Burckhardt Peter/Hösli Andreas, Neue strafrechtliche Risiken für Händler bei Barzahlungen über CHF 100'000, in: Jusletter vom 1.2.2016 (zit. Burckhardt/Hösli, Jusletter 1. Februar 2016).

Hagi Andreas Lukas/Tschabold Stephan, Kommentierung zu Art. 15, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar zum Geldwäschereigesetz (GwG), Bundesgesetz vom 10.10.1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Bern 2017 (zit. SHK-Hagi/Tschabold, Art. 15 GwG).

Kunz Michael, Umsetzung der GAFI-Empfehlungen 2012, die Geldwäschereiprävention verlässt den Finanzsektor, in: Jusletter vom 23.2.2015 (zit. Kunz, Jusletter 23. Februar 2015).

Nagel Thomas, Der persönliche und sachliche Geltungsbereich des schweizerischen Geldwäschereigesetzes: Mit rechtsvergleichenden Hinweisen zu internationalen Standards, dem Recht der Europäischen Union und dem deutschen Recht, Zürich et al. 2020 (zit. Nagel).

Peyer Martin, Kommentierung zu Art. 8, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz, Basel 2021 (zit. BSK-Peyer, Art. 8 GwG).

Ramelet Nicolas, Kommentierung zu Art. 8a, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz, Basel 2021 (zit. BSK-Ramelet, Art. 8a GwG).

Ramelet Nicolas, Sorgfaltspflichten für «Händler» – Auslegeordnung einer Kompromisslösung, AJP 2015, S. 1160–1167 (zit. Ramelet, AJP 2015).

Schott Ansgar/Kessler Martina A., Kommentierung zu Art. 8a, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar zum Geldwäschereigesetz (GwG), Bundesgesetz vom 10. Oktober 1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Bern 2017 (zit. SHK-Schott/Kessler, Art. 8a GwG).

Wyss Ralph, Kommentierung zu Art. 8a, in: Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Geldwäschereigesetz mit weiteren Erlassen (GwG), 3. Aufl., Zürich 2019 (zit. OFK-Wyss, Art. 8a GwG)

MATERIALS

Botschaft zum Bundesgesetz über die Transparenz juristischer Personen und die Identifikation der wirtschaftlich berechtigten Personen, nicht datiert (Vorabdruck), 2024, abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/87770.pdf, besucht am 31.8.2024 (zit. Botschaft TJPG 2024).

Erläuterungsbericht zur Geldwäschereiverordnung (GwV) – Umsetzung der GAFI-Empfehlungen vom 11.11.2015, abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/41723.pdf, besucht am 31.8.2024 (zit. Erläuterungsbericht GwV 2015).

FINMA, Rundschreiben 2011/1, Tätigkeit als Finanzintermediär nach GwG: Ausführungen zur Geldwäschereiverordnung (GwV), 20.10.2010, zuletzt geändert am 4.11.2020, abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2011-01-01-01-2017.pdf?sc_lang=de&hash=C13E76F1B7CE20DFB9B822526B383187, besucht am 31.8.2024 (zit. FINMA-RS 2011/1).

MROS, Jahresbericht 2020, Bern 2021, abrufbar unter https://www.fedpol.admin.ch/dam/fedpol/de/data/kriminalitaet/geldwaescherei/jabe/jb-

mros-2020-d.pdf.download.pdf/jb-mros-2020-d.pdf, besucht am 31.8.2024 (zit. MROS, Jahresbericht 2020).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in French. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 9 AMLA

A commentary by Andrew Garbarski / Louis Muskens / Mattia Brugger

SUGGESTED CITATION

Andrew M. Garbarski/Louis Frédéric Muskens/Mattia Brugger, Commentary of art. 9 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Garbarski/Muskens/Brugger, art. 9 AMLA N. XXX

Section 2 Duties in the Event of a Suspicion of Money Laundering

Art. 9 Duty to report

[1] A financial intermediary must immediately file a report with the Money Laundering Reporting Office Switzerland (the Reporting Office) as defined in Article 23 if it:

a. knows or has reasonable grounds to suspect that assets involved in the business relationship:

are connected to an offence in terms of Article 260ter or 305bis SCC[50], are the proceeds of a felony or an aggravated tax misdemeanour under Article 305bis number 1bis SCC,

are subject to the power of disposal of a criminal or terrorist organisation, or
serve the financing of terrorism (Art. 260^{quinquies} para. 1 SCC);

b. terminates negotiations aimed at establishing a business relationship because of a reasonable suspicion as defined in letter a;

c. knows or has reason to assume based on the clarifications carried out under Article 6 paragraph 2 letter d that the data on a person or organisation passed on under Article 22*a* paragraph 2 or 3 correspond to the data of a customer, a beneficial owner or an authorised signatory in a business relationship or transaction.

^{1bis} A dealer must immediately file a report with the Reporting Office if it knows or has reasonable grounds to suspect that cash payments made in the course of a commercial transaction:

a. are connected to an offence under Article 260ter or 305bis SCC;

b. are the proceeds of a felony or an aggravated tax misdemeanour under Article 305bis number 1bis SCC;

c. are subject to the power of disposal of a criminal organisation; or

d. serve the financing of terrorism (Art. 260^{quinquies} para. 1 SCC).

^{1ter} The name of the financial intermediary or dealer must appear in any report in accordance with paragraph 1. The identity of the financial intermediary's or dealer's staff who are in charge of the case may be made anonymous in the report, provided it is guaranteed that the Reporting Office and the competent prosecution authority are able to contact them without delay.

^{1quater} In the cases referred to in paragraph 1, reasonable grounds to suspect exist if the financial intermediary has specific evidence or several indications that paragraph 1 letter a may apply to the assets involved in the business relationship and this suspicion cannot be dispelled on the basis of additional clarifications in accordance with Article 6.

[2] Lawyers and notaries are not subject to the duty to report insofar as they are bound in their activities by professional secrecy in terms of Article 321 SCC.

CONTENT

I. Introduction and General Provisions 280
A. Purpose 280
B. Purpose 280
C. International Framework 281
D. Legislative History 282
E. Scope of Application 284
1. Personnel 284
a. Financial intermediaries, traders, and advisors 284
b. Attorneys and Notaries 284
c. Audit Firms and Supervisory or Self-Regulatory Bodies 286
2. Material Scope 286
3. Territorial 287
4. Temporal 288
a. Commencement of the Obligation 288
b. Termination of the Obligation 288
F. Links to Other Provisions 290
1. The AMLA 290
2. Ordinances on Money Laundering 291
3. Right to Disclose under Art. 305ter, para. 2, of the Swiss Criminal Code 292
4. Reporting obligation under Art. 7 of the Act on the Freezing and Return of Assets of Illicit Origin Belonging to Politically Exposed Persons Abroad (LVP) . 298
5. Money Laundering (Art. 305bis of the Swiss Criminal Code) 299
6. The nemo tenetur principle (Art. 14(3)(g) of the Second UN Covenant, Art. 6(1) of the ECHR, and Art. 32 of the Swiss Constitution) 300
II. Overview of the Various Scenarios Envisaged by Art. 9 of the Anti-Money Laundering Act (AMLA) 301
III. Reporting Obligations of Financial Intermediaries (para. 1) 302
A. Addressees: Financial Intermediaries 302
B. Conditions 302
1. Reporting Obligation in the Event of Suspicions Regarding Assets Involved in the Business (para. 1(a)) 303
a. Subject of the suspicion: Assets involved in the business relationship 303
b. Nature of the Suspicion: Link to Certain Crimes or Offenses 304
c. Threshold of Suspicion and Triggering Factor: Knowledge or Reasonable Suspicion 313
2. Obligation in the Event of Termination of Negotiations (para. 1(b)) 320
a. Subject of the Suspicion: Assets Intended for Use in a Business Relationship Under Negotiation 320
b. Nature of the Suspicion: Link to Certain Crimes or Offenses offenses 322
c. Threshold for Suspicion: Well-Founded Suspicion 323

d. Triggering Event: Termination of Negotiations Due to Well-Founded Suspicions ... 324
3. Obligation in the Event of a Match with a Terrorist List (para. 1(c)) ... 325
a. Subject of the suspicion: Information concerning a contracting party, beneficial owner, or signatory ... 325
b. Content of the Suspicion: Match with a Terrorist List ... 327
c. Threshold for Suspicion and Triggering Event: Knowledge or Reasonable Suspicion ... 328
C. Consequence: Reporting Obligation and Parallel Obligations ... 330
IV. Reporting Obligations of Traders (para. 1bis) ... 330
A. Applicable Parties: Dealers ... 330
B. Conditions ... 330
1. Preliminary Remarks: Limitation to Significant Trading Transactions ... 330
2. Subject of the Suspicion: Currency Used in a Trading Transaction ... 332
3. Nature of the Suspicion: Link to Certain Crimes or Offenses ... 332
4. Threshold for Suspicion and Triggering Event: Knowledge or Reasonable Suspicion ... 333
C. Consequence: Reporting Obligation and Parallel Obligations ... 334
V. Reporting Obligations of Advisors (Art. 9 para. 1ter nAMLA) ... 335
A. Applicable Parties: Advisors ... 335
B. Conditions ... 335
C. Consequence: Reporting Obligation and Parallel Obligations ... 336
VI. Reporting Procedures ... 336
A. Responsibilities and Obligations Within the Financial Intermediary, Dealer, or Advisor ... 336
B. Recipient of the Report ... 340
C. Form and Content of the Report ... 341
D. Timing of the Report ... 343
VII. Effects of the Report and Related Obligations ... 345
A. MROS Procedure ... 345
B. Parallel Obligations ... 346
C. Exclusion of Liability in the Case of Reports Made in Good Faith ... 349
VIII. Consequences of a Breach of the Reporting Obligation ... 350
Bibliography ... 351

I. INTRODUCTION AND GENERAL PROVISIONS

A. Purpose

1 Article 9 of the Federal Act on Money Laundering (AMLA) addresses the**obligation** of financial intermediaries and traders to report their suspicions—particularly those related to money laundering—to the Money Laundering Reporting Office (MROS).

2 Although the marginal note to Art. 9 AMLA uses the singular ("Obligation to Report"), the provision actually envisages **several distinct scenarios** that may trigger the obligation of financial intermediaries or traders to report their suspicions to MROS.

3 **In addition to the conditions** underlying these various scenarios (Art. 9, para. 1, letters a–c, and para. 1bis of the AMLA BA), the provision in Art. 9 of the Anti-Money Laundering Act (AMLA) includes a legal definition of the concept of "reasonable suspicion" (para. 1^{quater}) and provides certain clarifications regarding the protection of employees' personal data in the context of reporting (para. 1ter). Finally, Art. 9 of the Anti-Money Laundering Act clarifies the scope of the reporting obligation with respect to attorneys and notaries (para. 2).

B. Purpose

4 The reporting obligation plays a **central role** in the Swiss anti-money laundering system ' money laundering. This system aims, in conjunction with relevant criminal provisions, to prevent funds of criminal origin from entering the legal monetary system, to identify assets subject to money laundering, and to prosecute those responsible, in order to ensure the integrity of the Swiss financial center. Although it is an instrument governed by administrative law, the reporting obligation is primarily intended to identify funds subject to money laundering and serves as a "link" between the due diligence obligations incumbent upon financial intermediaries, on the one hand, and the prosecution of money laundering by criminal authorities, on the on the other.

5 Thus, the reporting obligation is intended to enable the State to **prosecute and punish** acts of money laundering (Art. 305bis of the Swiss Criminal Code, SCC) and the financing of terrorism (Art. 260^{quinquies} SCC) and to **seize and**

subsequently confiscate the relevant assets (Art. 70 et seq. SCC). Without the information provided by financial intermediaries and dealers to MROS, many criminal acts and assets subject to confiscation would escape the attention of law enforcement authorities. According to case law, Art. 9 of the Anti-Money Laundering Act (AMLA) also serves, incidentally, to prevent offenses, reduce risks for financial intermediaries, and, finally, **preserve the reputation of the Swiss financial center**. Thus, the reporting obligation pursues a broader objective than Article 305bis of the Swiss Criminal Code (CP), which criminalizes money laundering.

This does not mean, however, that the reporting obligation transforms the financial intermediary or trader into a "**police auxiliary**," since it is merely an administrative obligation—albeit one subject to criminal penalties—imposed on actors in a sector presenting a definite risk of money laundering and terrorist financing. 6

C. International Framework

To combat the growing problem of money laundering at the international level, an international intergovernmental organization was established in 1989. This is the **Financial Action Task Force on Money Laundering (FATF)** whose primary mission is to establish international standards in the fight against money laundering and terrorist financing, as well as to monitor their implementation in the various member countries. Switzerland is a founding member of the FATF. 7

One of the main objectives of Swiss anti-money laundering legislation is to **implement these international recommendations in Switzerland**. This also applies to the to report provided for in Article 9 of the Anti-Money Laundering Act (AMLA). 8

The **first FATF recommendations in 1990** already stipulated that financial institutions suspecting that funds were of criminal origin should be "*authorized or required*" to promptly report their suspicions to the competent authorities. 9

Today, the **2012 FATF recommendations** address the reporting obligation in Recommendation 20, which provides as follows: "*Where a financial institution suspects, or has reasonable grounds to suspect, that funds are the proceeds of criminal activity or are related to the financing of terrorism, it should* 10

be required by law to immediately file a suspicious transaction report with the financial intelligence unit." The related interpretive note clarifies that the FATF understands this reporting requirement to be a binding obligation. It also defines the offenses whose suspicion must trigger the reporting obligation.

11 During the FATF's most recent comprehensive **evaluation** of Switzerland in 2016, its reporting system was deemed largely compliant with Recommendation 20, although the FATF did not fail to point out that the coexistence of a right and an obligation to report creates legal uncertainty (see in detail *infra* N. 42 et seq.). The latest follow-up report, dated 2023, contains the same conclusions.

D. Legislative History

12 Since its entry into force on April 1, 1998, Art. 9 of the Anti-Money Laundering Act (AMLA) has been amended several times, with each **revision** essentially pursuing three objectives: expanding the scope of the reporting obligation, aligning it with international standards—particularly those of the FATF—and codifying Swiss case law. Over time, this has resulted in a dense and complex provision, which, in our view, should be simplified or split into several provisions during a future legislative reform, in order to improve its readability and, to a certain extent, its predictability for financial sector participants.

13 **Originally**, the reporting obligation was limited to cases where the financial intermediary suspected, based on reasonable grounds, a link between assets and money laundering money laundering, criminal origin, or a criminal organization's control over such assets (see current para. 1, let. a, subsections 1–3). The professional secrecy of attorneys and notaries was expressly exempted (see para. 2).

14 Successive revisions of the provision in Art. 9 of the Anti-Money Laundering Act (AMLA) have gradually expanded its material and personal scope of application. In **200 9**, the reporting obligation was extended to include terrorist financing and the offense of criminal organization, as well as situations where pre-contractual negotiations are terminated due to a well-founded suspicion (see para. 1(a)(4) and (b)). The protection of employees of financial intermediaries was also strengthened by allowing their names to be withheld in the report (see para. 1ter).

The **2016** revision marked an important milestone, with the extension of the rule to assets derived from a qualified tax offense and the introduction of a reporting obligation in cases of matches with terrorist lists provided by supervisory authorities (see para. 1, let. a, subpara. 2, and let. c). Furthermore, also as part of the the 2016 amendment, a parallel reporting obligation was established for merchants accepting cash payments (see para. 1bis, letters a–c). Furthermore, the option for anonymization was extended to the merchant's employees handling the case (see para. 1ter). 15

In **2021**, the provision in Art. 9 of the Anti-Money Laundering Act (AMLA) was amended to revised Art. 260ter of the Swiss Criminal Code, so that the reporting obligation now refers to criminal or terrorist organizations (see para. 1, letter a, subparagraph 3, and para. 1bis, letter c). For merchants, the obligation to report cash intended for the financing of terrorism was also added (see para. 1bis, letter d). 16

The most recent revision of Art. 9 of the Anti-Money Laundering Act (LBA), which entered into force in **2023**, clarified the provision regarding terrorist lists (see para. 1(c)) and, most importantly, codified the case-law definition of "reasonable suspicion" (see para. 1^{quater}), thereby aligning it with the definition applicable to financial institutions (see Art. 20, para. 1, OBA). 17

The momentum toward implementing international recommendations and expanding the reporting obligation continues, as evidenced by the latest revision of the AMLA adopted on September 26, **2025**, concurrently with the Federal Act on the Transparency of Legal Entities (LTPM). This amendment extends Art. 9 of the AMLA to advisors (see Art. 9, para. 1ter of the new AMLA), a status that has also been newly introduced (see Art. 2, paras. 3bis–4ter of the new AMLA). The text of the law adopted by the Federal Chambers is the result of intense parliamentary debates and differs considerably from the Federal Council's draft. In addition, Parliament also extended the legal definition of "reasonable suspicion" *by analogy* to dealers and advisors (see Art. 9, para. 1^{sexies} of the new AMLA) and amended the wording regarding the professional secrecy of attorneys and notaries (see Art. 9, para. 2 of the new AMLA) to clarify it. These amendments will take effect on October 1, 2026. 18

E. Scope of Application

1. Personnel

a. Financial intermediaries, traders, and advisors

19 Art. 9 of the Anti-Money Laundering Act (AMLA) currently applies to **financial intermediaries** (para. 1) and **traders** (para. 1bis). These two terms are defined in Art. 2 of the AMLA. Their obligations under Art. 9 AMLA are examined in greater detail below (see *infra*, Chapters III and IV).

20 In September 2025, the Federal Parliament also decided to extend the reporting obligation to the category of **advisors**, which will also be defined in Art. 2 of the New Anti-Money Laundering Act (see *supra* N. 18; *infra* Chapter V).

b. Attorneys and Notaries

21 It follows from Art. 9(2) of the Anti-Money Laundering Act that the reporting obligation does not apply to **attorneys and notaries** to the extent that they are subject to professional secrecy under Art. 321 of the Swiss Criminal Code. This exception based on professional secrecy takes into account the concerns expressed during the drafting of the AMLA. It is therefore important to distinguish between activities protected by Art. 321 of the Swiss Criminal Code and those that are not. Only so-called "**typical**" professional activity is covered by professional secrecy; for attorneys, this includes, in particular, drafting legal documents, assisting or representing a person before an administrative or judicial authority, as well as providing legal or tax advice. For notaries, notarial practice is defined by cantonal legislation. It commonly involves the execution of authentic instruments. By contrast, financial intermediation or trading activities carried out by a lawyer or a notary fall under so-called "atypical" activities , which is not covered by professional secrecy under Art. 321 of the Swiss Criminal Code (CP) and, consequently, is not exempt from the reporting obligation under Art. 9 of the Anti-Money Laundering Act (LBA). However, it is not always easy to distinguish between "typical" activities, which are subject to professional secrecy, and "atypical" activities that fall within the scope of the reporting obligation, particularly in the case of so-called "mixed" mandates, and it should also be noted that the burden of proof regarding the typical nature of the activity rests with the attorney or notary claiming protection under professional secrecy.

The **targeted nature of the exception** concerning the typical activities of attorneys and notaries—that is, the fact that this exception was established solely in the context of the reporting obligation and not more generally in relation to the scope of application of the Anti-Money Laundering Act—has the subject of much scholarly debate. Some authors argue that Art. 9(2) of the Anti-Money Laundering Act (AMLA) is merely declaratory in nature (an "improperly named" exception), since typical activities do not fall within the scope of the AMLA in any case—to such an extent that the other obligations under the AMLA, particularly the due diligence obligations, would not apply in the context of typical activities. We share this view. In our opinion, the legislature did not intend to target the typical activity of a lawyer or notary when enacting the AMLA, even when elements that could constitute financial intermediation are part of that typical activity (for example, collecting a judgment awarded at the conclusion of a civil lawsuit on behalf of a client). The exception in Art. 9(2) of the Anti-Money Laundering Act (AMLA) therefore constitutes, in our view, an impropriately named exception. However, since typical activities may occasionally involve elements characteristic of financial intermediation and the distinction between typical and atypical activities is not always straightforward, we believe it is necessary for the legislature to clarify the scope of application of the AMLA as a whole, without limiting itself to the specific exception in Art. 9(2) of the Anti-Money Laundering Act. 22

However, the **revision of the Anti-Money Laundering Act adopted in September 2025** specifically provides for the introduction of such a general exception, which is to be welcomed. Art. 2, para. 4, subpar. f of the new AMLA expressly excludes from the scope of the AMLA "*attorneys and notaries who carry out activities in the context of judicial, criminal, administrative, or arbitration proceedings, including representation in proceedings and advice related to the preparation and conduct of proceedings, the clarification of the facts, the assessment of litigation risks, how to prevent such proceedings, or the implementation of the results of the proceedings*." That said, this wording leaves something to be desired. The provision in Art. 2, para. 4, let. f of the new Anti-Money Laundering Act (nLBA) does not expressly refer to the concept of "typical activity" and only partially incorporates its definition; surprisingly, the provision of legal advice is not mentioned. The distinction between legal advice that falls within the scope of "typical activity" and that which does does not fall within it. Furthermore, the wording cited above ap- 23

pears to describe primarily the activities of attorneys, but says little about those of notaries.

24 In addition, the September 2025 amendment also led to a **rewording of Art. 9(2) of the Anti-Money Laundering Act (AMLA)**, such that attorneys and notaries are subject to the reporting obligation only if they carry out a financial transaction in the name of or on behalf of a client (subpar. a) and the information at their disposal is not protected by professional secrecy within the meaning of Art. 321 of the Swiss Criminal Code (subpar. b). From a substantive standpoint, the new Art. 9(2) of the amended Anti-Money Laundering Act (nLBA) should not change anything compared to the current Art. 9(2) of the Anti-Money Laundering Act (LBA). The exception for facts covered by professional secrecy corresponds to current law, and the subjection of attorneys and notaries to the Anti-Money Laundering Act (AMLA) only when they participate in a financial transaction stems from the scope of the law, more specifically from the concept of a financial intermediary. However, this clarification takes on full significance in the context of the inclusion of the new category of advisors under Art. 9 of the Anti-Money Laundering Act (AMLA), as advisory activities may fall under both typical and atypical activities.

c. Audit Firms and Supervisory or Self-Regulatory Bodies

25 Finally, Art. 9 of the Anti-Money Laundering Act (AMLA) does not apply to **audit firms** of financial institutions, to authorities and **supervisory bodies**, as well as **self-regulatory organizations**, for which the AMLA provides separate reporting obligations (see Art. 15(5), Art. 16, and Art. 27(4 AMLA).

2. Material Scope

26 The **material scope** of Art. 9 AMLA cannot be determined in general terms but varies depending on the scenario covered by the provision. It may apply to assets involved in a business relationship (para. 1(a)), or intended to be involved in a future business relationship (para. 1(b)), to data concerning a contracting party, a beneficial owner, or an authorized signatory of a business relationship or transaction (para. 1(c)), or to cash used in a trading transaction (para. 1bis). Since these concepts cannot be separated from the substantive conditions of the reporting obligation, we will discuss them in more detail below in connection with those conditions (see *infra*, Chapters III and IV).

3. Territorial

Like the AMLA itself, Art. 9 AMLA does not explicitly define its territorial scope of application. Thus, the reporting obligation, as a rule of administrative law, is subject to the **principle of territoriality**, according to which Swiss public law generally applies only to facts and situations that occur in Switzerland. 27

According to a relatively old—but since confirmed—Federal Supreme Court ruling, the decisive connecting factor is not the place of domicile or registered office of the person subject to the AMLA, nor that of their business partner's domicile, nor even the location of the assets in question, but rather **the place where the activity covered by the AMLA** is carried out. In the case of cross-border financial services, this place must be determined on a case-by-case basis, depending on the specific circumstances. To this end, it is necessary to examine, in light of the purpose of the AMLA—namely, the prevention of circumvention of prudential supervision and the protection of the integrity of the Swiss financial center, whether the activity in question has a sufficiently close connection to Switzerland to justify its subjection to the AMLA. This is generally the case when the activity is carried out primarily in Switzerland, even if certain operational or back-office activities take place abroad. 28

These principles are explicitly set forth **in the ordinances** implementing the Anti-Money Laundering Act (AMLA). Indeed, the Anti-Money Laundering Ordinance (AMLO) specifies in Art. 2(1) that it applies to financial intermediaries and dealers "*who conduct their business in Switzerland or from Switzerland*," a concept that must be interpreted in light of the aforementioned case law. Similarly, pursuant to Art. 5(1) of the FINMA Money Laundering Ordinance (OBA -FINMA), financial intermediaries must ensure that their branches abroad, as well as foreign group companies, comply with certain principles of the Anti-Money Laundering Act (AMLA), while Art. 5, para. 4, AMLO-FINMA expressly provides that the reporting of suspicious transactions or business relationships is governed by the provisions of the host country. 29

4. Temporal

a. Commencement of the Obligation

30 As a reminder, the reporting obligation under Art. 9 of the Anti-Money Laundering Act (AMLA) **took effect** on April 1, 1998, at the same time as the AMLA (see *supra* N. 13).

31 The reporting obligation is **triggered** as soon as the statutory threshold for suspicion is met (see *infra* N. 99). Case law interpreting Art. 9(1)(a) AMLA holds that, in particular, it is not necessary for the financial intermediary to already have control over the assets, as its suspicions may also relate to specific or identifiable assets intended to come under its sphere of influence. Furthermore, the reporting obligation already applies when the financial intermediary, based on well-founded suspicions, terminates negotiations aimed at establishing a business relationship (Art. 9(1)(b) AMLA; see *infra* N. 131). Such an early reporting requirement is justified because, otherwise, a financial intermediary harboring well-founded suspicions could simply refuse to enter into a and thus evade the reporting obligation, to the extent that the illicit assets could be placed with another financial intermediary, whether Swiss or foreign.

b. Termination of the Obligation

32 The question of when the reporting obligation ends is closely linked to the purpose of Art. 9 AMLA. This issue was long controversial. The Federal Supreme Court ultimately held, in a landmark ruling, that the reporting obligation lasts **as long as the illicit assets can be traced and confiscated**.

33 Consequently, the reporting obligation does not end with the internal freezing of funds or the termination of the business relationship, because—according to the Federal Supreme Court—*"Art. 9 AMLA must allow the prosecution of money laundering, and it would be shocking if the financial intermediary, who has a well-founded suspicion, could be released from all obligations by terminating the business relationship"*. Nor does the obligation automatically cease merely because a third party reports the facts to the criminal authorities or because the criminal authorities initiate proceedings in connection with the disputed assets . The reporting obligation remains in effect as long as the criminal authorities are unaware of the fate of the assets in question—that is, **as long as these assets may still elude them**. According to the Federal

Supreme Court, this approach is justified because the reporting obligation is ultimately intended to facilitate the discovery and forfeiture of the assets in question. However, it would be disproportionate and unjustified in light of the objective of the Anti-Money Laundering Act (AMLA) to set the end of the obligation at the time of the (actual) seizure of said assets. The relevant point in time is when the criminal prosecution authority has **all the relevant information necessary** for the discovery and seizure of the disputed assets, regardless of whether they have actually been seized. *A fortiori* , when the assets are seized from the relevant financial intermediary, any reporting obligation on the part of the financial intermediary ceases. To assess whether the criminal authorities have sufficient information regarding the assets in question and are therefore in a position to order their seizure, recent case law relies on **Art. 3 OBCBA**, which governs the required content of reports submitted to MROS.

Given that case law makes the termination of the reporting obligation on the status of the information available to the criminal authorities—and since persons subject to the reporting obligation are often unaware of this status— it is advisable, **in practice**, to refrain from reporting to MROS only with the utmost caution. This is all the more true given that the report must be made immediately upon the emergence of reasonable suspicion. 34

The reporting obligation also ends, for the financial intermediary and the dealer concerned, on the day they **submit the required report**, including all necessary information pursuant to Art. 3 OBCBA, namely, in particular, data identifying other persons authorized to sign for or represent the customer, the current status of the account in question, a description of the business relationship—including the account numbers and dates of account opening—as well as the information at their disposal supporting the suspicions underlying the report. Even a report that is presumably incomplete may satisfy the reporting obligation provided that, as a result of such a report, law enforcement authorities have all the information necessary to enable them to seize the in question. 35

It should be noted that, furthermore, it is not necessary for the information enabling the identification and seizure of the assets to come from the person subject to Art. 9 of the Anti-Money Laundering Act; the reporting obligation ends even if the relevant information **is transmitted to the criminal justice** 36

authority by a third party, if necessary without the financial intermediary's knowledge.

37 One may also ask whether the reporting obligation ceases when the financial intermediary or dealer has **no additional information** beyond what is already in the possession of the criminal authorities, if that information is insufficient to identify and seize the assets in question. A teleological interpretation supports this view, but finds no basis in the plain language of the provision, so that a report must, *a priori*, also be made in such a case, if only as a precaution.

38 The aforementioned case law, according to which the reporting obligation lasts as long as the assets can still be traced and confiscated, could mean that an obligation to report may **arise, for the first time, after the end of the business relationship**—for example, when newspaper clippings or other information that has come to the financial intermediary's attention gives rise to well-founded suspicions *a posteriori*. Such a report could prove useful from the perspective of criminal prosecution for money laundering and confiscation (see *supra* N. 5), subject, however, to the passage of time and the fact that the financial intermediary is often unaware of the fate and location of the assets in question. It is important to note, however, that there is no general obligation on financial intermediaries to actively monitor closed business relationships. Furthermore, no specific clarifications may be required in the event that reasonable suspicion arises after the termination of a business relationship; consequently, reporting in such a situation must be based on the documents in the financial intermediary's possession, for which the statutory retention period is 10 years (Art. 7(3) AMLA).

F. Links to Other Provisions

1. The AMLA

39 Art. 9 AMLA is not the only provision of the AMLA that imposes an obligation to report to MROS. **Such an obligation** also applies to other participants in the financial system: as already mentioned above (see *supra* N. 25), Art. 15(5) of the AMLA applies to the auditors of dealers, Art. 16 AMLA to supervisory authorities and bodies, and Art. 27(4) AMLA to self-regulatory organizations.

The reporting obligation under Art. 9 AMLA is also closely linked to **other provisions of the AMLA**. For example, the purpose of the inquiries under Art. 6(2) AMLA is precisely to enable the financial intermediary to determine whether or not a report must be filed and to provide the necessary information for such a report (see *infra* N. 101 et seq.). Furthermore, Art. 9*a* et seq. AMLA govern the obligations of financial intermediaries following a report (see *infra* N. 199 et seq.), and Art. 11 AMLA excludes civil and/or criminal liability in connection with reports made in good faith (see *below* N. 209). Art. 23 of the Anti-Money Laundering Act (AMLA), supplemented by the AMLA Implementation Ordinance, defines the role and obligations of MROS (see *below* N. 178 et seq. and N. 195 et seq.). Finally, Art. 37 AMLA penalizes violations of Art. 9 AMLA (see *below* N. 212). 40

2. Ordinances on Money Laundering

The Article 9 of the AMLA is supplemented by various **provisions of the ordinances implementing the AMLA**. Thus, Articles 12*a* et seq. of the Anti-Money Laundering Ordinance (OBA) set forth the obligations that financial intermediaries must comply with in cases of suspected money laundering (see *below*, N. 199 et seq.). Art. 20 AMLO specifies the reporting obligation of traders under Art. 9(1)^{bis} AMLA (see *below*, Chapter IV). Art. 22*a* FINMA-AMLO requires financial intermediaries to notify FINMA or the supervisory authority of reports concerning significant assets and to document any decision not to report (see *below* N. 205). Art. 25*a* OBA -FINMA governs, within certain financial intermediaries, the decision-making authority regarding reports to MROS, and Art. 26(2)(g) OBA-FINMA requires that internal guidelines specify the decision-making authority for reports (see *below* N. 170 et seq.). Art. 74(1)(f) OBA-FINMA requires financial intermediaries to retain a copy of the reports submitted (see *below* N. 170 et seq.). Other relevant provisions can also be found in the CFMJ Anti-Money Laundering Ordinance (OBA-CFMJ) concerning casinos, in the FDJP Anti-Money Laundering Ordinance (OBA-DFJP) concerning large-scale gaming operators, and in the OFDF Anti-Money Laundering Ordinance (OBA-OFDF) concerning the trading of bank-grade precious metals.

3. Right to Disclose under Art. 305ter, para. 2, of the Swiss Criminal Code

42 The reporting obligation has a complex relationship with the **right to report** within the meaning of Art. 305ter, para. 2, of the Swiss Criminal Code (CP). The issue has become even more pronounced with the lowering of the threshold for "reasonable suspicion" established by case law—now codified in Art. 9, para. 1^{quater}, of the Anti-Money Laundering Act (AMLA)—and the concomitant expansion of the scope of application of Art. 9 of the Anti-Money Laundering Act (AMLA), coinciding with a narrowing of the scope of Art. 305ter, para. 2 of the Swiss Criminal Code (SCC).

43 **According to Art. 305ter, para. 2 of the SCC**, persons who accept, hold in custody, or assist in placing or transferring assets belonging to a third party in the course of their professional activities have the right to report to MROS any indications giving rise to a suspicion that assets originate from a crime or a qualified tax offense.

44 Let us first note the clear differences between the two regimes. First, with regard to their **effect**: Article 9 of the Anti-Money Laundering Act (AMLA) establishes a genuine reporting obligation, the failure to comply with which entails administrative and criminal consequences (see *infra* Chapter VIII), whereas Article 305ter, para. 2, of the Swiss Criminal Code (CP) serves as a justifying ground within the meaning of Art. 14 CP, allowing the financial intermediary to report its suspicions on a voluntary basis, without violating, in particular, banking secrecy (Art. 47 of the Banking Act, BA). As for their **personal scope of application**, the activities listed in Art. 305ter, para. 1 of the Swiss Criminal Code, to which Art. 305ter, para. 2 of the Swiss Criminal Code refers, are those of financial intermediaries in the broad sense pursuant to Art. 2, paras. 2 and 3 of the Anti-Money Laundering Act. It follows that the right to report applies only to financial intermediaries, but not, for example, to traders. With regard to the **grounds for reporting**, Art. 305ter, para. 2 of the Swiss Criminal Code (CP) mentions only the suspicion that the assets derive from a crime or a qualified tax offense—that is, the scenario covered by Art. 9, para. 1, let. a, ch. 2 of the Anti-Money Laundering Act (AMLA)—whereas Art. 9 of the AMLA has a broader scope. Furthermore, the right to report is not expressly limited to assets **involved in the business relationship** or intended to be involved in a business relationship currently under negotiation and therefore has a potentially broader scope. Finally, the right to disclose provid-

ed for in Art. 305ter, para. 2, of the Swiss Criminal Code (CP) may be exercised at any **time**, which means that it does not, in particular, cease once the criminal authorities have obtained the information necessary to identify and seize the assets in question.

The question of the distinction between Art. 305ter, para. 2, of the CP and Article 9 of the Anti-Money Laundering Act (AMLA) therefore ultimately arises only when a financial intermediary is involved and when assets—whether already involved in or intended to be involved in the business relationship—are suspected of deriving from a crime or a qualified tax offense. The distinction between these two provisions revolves primarily around the **required threshold of suspicion**, namely a mere suspicion in the case of Art. 305ter, para. 2, of the Swiss Criminal Code (CP), and reasonable suspicion in the case of Art. 9 of the Anti-Money Laundering Act (AMLA). The relationship between these two provisions must be examined in light of the genesis and evolution of these two concepts. 45

The right to report under Art. 305ter, para. 2, of the Swiss Criminal Code (CP) was introduced on August 1, **1994**—some four years before the Anti-Money Laundering Act (LBA) came into force—in order to free financial intermediaries from the dilemma of, on the one hand, violating their confidentiality obligations if they were to disclose their suspicions to the authorities, and, on the other hand, incurring criminal liability for money laundering if they refrained from reporting and allowed the transfer of potentially illicit assets. At the time, the Federal Council considered it essential to establish a right to report, independent of the subsequent introduction of a reporting obligation, "*in particular because a financial professional may become aware of information whose suspicious nature may reach a level that, while justifying the dilemma* [...]*does not yet establish a reporting obligation*." 46

While, until **1996**, the FATF recommendations provided that financial institutions "*should be authorized or required*" to report their suspicions, they were amended that year to the effect that a reporting obligation must necessarily be established by member states. Switzerland has often been criticized for failing to fully implement the FATF recommendations. 47

When Art. 9 of the Anti-Money Laundering Act (AMLA) was adopted in **1997**, the Federal Council emphasized that the right to report and the obligation to report "*must be understood as different degrees of the same concept.* [...] *The* 48

various degrees of suspicion on the part of the financial intermediary range from a hunch based on vague indications to absolute certainty. They encompass the situation in which, due to the absence of clearly established facts, a report to the competent authorities is justified but not yet inevitable, as well as the situation where the intermediary is obligated to report its suspicions because they prove to be well-founded. From this perspective, the two concepts do not are not contradictory but complementary." This was the rationale for retaining Art. 305ter, para. 2, of the Swiss Criminal Code (CP) following the introduction of Art. 9 of the Anti-Money Laundering Act (LBA).

49 In the years that followed, MROS gradually came out in favor of lowering the applicable thresholds. In its **2007** annual report, for example, it emphasized that the "*the legislature did not intend to establish a reporting obligation solely for cases where the financial intermediary has concrete* knowledge" and that suspicion is sufficiently well-founded, within the meaning of Art. 9 of the Anti-Money Laundering Act (AMLA), if "*the financial intermediary presumes or at least cannot rule out that the assets are of criminal origin*." Furthermore, MROS has regularly reiterated that a financial intermediary may exercise its right to report "*based on a probability, a doubt, or even a sense of unease regarding the continuation of the business relationship*."

50 In **2008**, in a civil case involving a financial intermediary who had filed a report allegedly harmful to its client, the Federal Supreme Court ruled that a "**mere doubt**" remaining at the end of the clarification process was sufficient to trigger the reporting obligation, such that the financial intermediary was not held civilly liable. This case law, *a priori* favorable to financial intermediaries from the perspective of their potential civil liability, subsequently backfired on them when it was adopted, as early as 201 5, by the Federal Criminal Court and subsequently also by the Federal Supreme Court in the context of criminal proceedings concerning violations of the reporting obligation (Art. 37 AMLA).

51 The Federal Council first considered repealing the right to report in **2014**, as part of the preliminary draft on the implementation of the FATF recommendations. In support of this proposal, it emphasized that the coexistence of the right and the obligation to report could be confusing and prove ineffective. Faced with reservations expressed during the consultation process, the Federal Council ultimately abandoned this repeal. In **2016**, however, the FATF criticized Switzerland for the fact that the coexistence of an obligation and a right

to report "*hampers financial intermediaries' understanding and interpretation of the circumstances giving rise to an obligation to report a suspicion to MROS*," such that "[t]*he legislative framework should be clarified to specify the distinction between the right and the obligation to report and to prevent the same level of suspicion from falling under both regimes*." On this basis, the Federal Council once again considered repealing the right to report, this time as part of
the preliminary draft revision of the Anti-Money Laundering Act (AMLA) of **2018**. Citing the FATF's opinion and the aforementioned case law—which lowered the threshold for reasonable suspicion—the Federal Council concluded that there was no longer any place for Art. 305ter, para. 2, of the Swiss Criminal Code. The majority of consultation respondents, however, objected that the right to report constitutes an effective tool in the fight against money laundering, allowing for the elimination of any risk of criminal liability. It was also emphasized that one should not attach so much importance to the 2008 Federal Supreme Court ruling, which addressed incidentally on the scope of the reporting obligation. The Federal Council thus once again refrained from repealing Art. 305ter, para. 2 of the Swiss Criminal Code in its draft bill, while offering interesting insights into the relationship between the right to disclose and the reporting obligation in its explanatory memorandum.

In particular, the Federal Council explained that the right to report is a **subsidiary instrument** relative to the reporting obligation and that "*before exercising the right to report, the financial intermediary must always examine whether the reporting obligation applies*" and that "*therefore, even when exercising the right to report, preliminary clarifications within the meaning of Art. 6(2) of the Anti-Money Laundering Act (AMLA). In other words, the right to report cannot be used to report cases to MROS without conducting any preliminary clarifications*." 52

In **2021**, in a landmark ruling, the Federal Supreme Court finally clarified its case law on the concept of "reasonable suspicion" in the following terms: "[i]*t must be understood from this case law that if, following a concrete examination of the business relationship, the suspicion cannot be dispelled during the investigations conducted pursuant to Art. 6(2) of the Anti-Money Laundering Act (AMLA)* [...], *it is therefore not unfounded and must be reported to MROS*" (see *infra* N. 101). 53

54 A few months later, still in **2021**, Parliament decided to codify this case law and establish it as a legal definition. Effective January 1, **2023**, Art. 9(1)^{quater} of the Anti-Money Laundering Act (AMLA) now provides that "*there are reasonable grounds for suspicion when the financial intermediary has a concrete indication or several clues suggesting that the criteria defined in para. 1, subpara. a, could be met with respect to the assets involved in the business relationship, and that the additional clarifications carried out pursuant to Art. 6 do not dispel the suspicions*" (see *infra* N. 101).

55 Given the evolution of case law and legislative developments, it is clear that the right to report has been **significantly eroded** over time. Indeed, on the one hand, it follows from the statutory definition in Art. 9(1^{quater}) of the Anti-Money Laundering Act (AMLA) and from case law that well-founded suspicions—triggering the reporting obligation—exist as long as a suspicion, or even a mere doubt, remains that has not been dispelled by the clarifications. On the other hand, the Federal Council has emphasized that Art. 305ter (2) of the Swiss Criminal Code (CP) cannot be used to make "defensive" reports without first undertaking the necessary clarifications. In other words, if the financial intermediary conducts clarifications, one of two things will occur: either a doubt remains at the end of this process, in which case the financial intermediary is required to file a report under Art. 9 of the Anti-Money Laundering Act (LBA), or the doubts have been fully dispelled, and there is no longer any basis for a report, even under Art. 305ter, para. 2, of the Swiss Criminal Code (CP). The fact that the right to report has thus lost its relevance is not in itself cause for concern, since the original objective of Art. 305ter, para. 2, of the CP—namely, to free the financial intermediary from the dilemma of either violating its obligations of secrecy or confidentiality or risking liability for money laundering—is addressed addressed by Art. 14 of the Swiss Criminal Code (CP) and, since 2009, explicitly by Art. 11 of the Anti-Money Laundering Act (LBA). Furthermore, and more generally, it should be emphasized that the right and the obligation to report have the same legal effects under the current system (see Art. 9*a* et seq. AMLA), so that, from the perspective of legal consequences, it does not appear essential to maintain the right to disclose. Furthermore, there is no historical justification for retaining it either: due to the criticism raised during the most recent consultation procedures, the Federal Council had indeed (reluctantly) refrained from proposing the repeal of Art. 305ter, para. 2, of the Swiss Criminal Code (CP) to Parliament. That said, Parliament approved the codification of the concept of "reasonable

suspicion" in Art. 9, para. 1^{quater}, of the Anti-Money Laundering Act (LBA), thereby confirming that Art. 305ter, para. 2, of the Swiss Criminal Code now plays a role reduced to the bare minimum.

The only two possible **alternative interpretations** of Article 305ter, paragraph 2, of the Swiss Criminal Code that lead to a different result are not convincing. First, recognizing the right to report based merely on a vague sense of unease—as proposed by MROS—would expand this right almost without limit, which would be contrary to the letter and purpose of the provision and risks further overburdening MROS with reports of highly relative relevance and utility. Furthermore, it would then be necessary to distinguish between a sense of unease and (mere) unresolved doubt, which seems just as difficult. Second, it would be of little more use to depart from the Message—which states that clarifications must also be sought before exercising the right to report—because while the financial intermediary could certainly make an initial report based on the right to report, it would still be required to seek clarifications in accordance with Art. 6(2) of the Anti-Money Laundering Act (AMLA). However, such clarifications would either render the initial report moot or lead to a new, more precise report that would be more useful for the fulfillment of MROS's tasks. Finally, these two alternative approaches seem difficult to reconcile with the substantive requirements set forth in Art. 3(1) *cum* Art. 2(a) of the OBCBA. 56

In light of the foregoing, Art. 305ter(2) of the Swiss Criminal Code (CP) has lost most of its rationale, and its **repeal** would alter the legal situation for financial intermediaries only marginally, if at all. It would likely also contribute to legal certainty. Its retention, in our view, can be explained solely by its historical significance and the caution of the Federal Council, which likely did not wish to jeopardize the aforementioned reforms of the Anti-Money Laundering Act (AMLA) aimed at clarifying the legal framework and preferred to address this in its respective messages. 57

These various considerations imply that, in practice, the **distinction between the right and the obligation to report is not always straightforward**. This ambiguity is particularly problematic given that Art. 37 of the Anti-Money Laundering Act (AMLA) imposes a criminal penalty for violating the reporting obligation under Art. 9 AMLA. In particular, one may wonder whether a person who makes a report based on the right to report, even though the conditions for the reporting obligation have been met, is in viola- 58

tion of their reporting obligation. In our view, a financial intermediary who makes a report based on Art. 30 5[ter], para. 2, of the Swiss Criminal Code (CP) does not violate its reporting obligation within the meaning of Art. 37 of the Anti-Money Laundering Act (AMLA), insofar as both types of reporting *a priori* contain virtually identical information with respect to the objective set forth in Art. 9 of the AMLA (see Art. 3, para. 1, *in conjunction with* Art. 2(a) of the AMLA Reporting Regulations). Furthermore, there is the more delicate question of whether a financial intermediary who mistakenly believes they are only entitled to report and therefore refrains from doing so, even though when in reality they are obligated to do so, is in violation of their reporting obligation under Art. 37 of the Anti-Money Laundering Act (AMLA). This question undoubtedly calls for an affirmative answer, provided that the financial intermediary can be held liable for intent or negligence, bearing in mind that an error in legal classification is not an error of fact within the meaning of Art. 13 of the Swiss Penal Code (CP) nor an error regarding unlawfulness within the meaning of Art. 21 CP.

4. Reporting obligation under Art. 7 of the Act on the Freezing and Return of **Assets of Illicit Origin Belonging to Politically Exposed Persons Abroad** (LVP)

59 The Federal Act on the Freezing and Return of Assets of Illicit Origin Belonging to Politically Exposed Persons Abroad (LVP) entered into force on July 1, 2016. Its purpose is, as its title suggests, to ensure the return to foreign states, as quickly and transparently as possible, of assets of criminal origin deposited in Switzerland. In Art. 7, para. 1, the LVP also establishes a reporting obligation: individuals and institutions that hold or manage in Switzerland assets belonging to persons subject to a freezing measure within the meaning of Article 3 of the Act must report them without delay to MROS. This also applies to individuals and institutions that, without holding or managing such assets in Switzerland, become aware of them in the course of their duties (Art. 7(2) LVP).

60 For the sake of efficiency, it was decided that reports under Art. 7 LVP should be made not to the Federal Department of Foreign Affairs, but to MROS, which thus acts as a "**one-stop shop**."

61 Unlike the reporting obligation under Art. 9 of the Anti-Money Laundering Act (AMLA), the obligation under Article 7 of the LVP is based solely on a

comparison with a list and does not require any further clarification. Another **difference** between the two regimes lies in the fact that the personal scope of application of the LVP is broader than that of the AMLA.

The **coexistence** of the reporting obligations under Article 7 of the LVP and Article 9 of the AMLA stems from the very different objectives pursued by these two laws. It follows that a report under the LVP has no effect on the obligations under the LBA, and vice versa. A report pursuant to the LVP therefore does not necessarily mean that there are reasonable grounds for suspicion within the meaning of Art. 9 LBA, nor that a report to that effect must *a fortiori* be filed with MROS. On the other hand, a match with the list of persons subject to a preventive freezing measure under the LVP triggers clarification obligations for financial intermediaries subject to the AMLA pursuant to Art. 6 AMLA. 62

5. Money Laundering (Art. 305bis of the Swiss Criminal Code)

The reporting obligation under Art. 9 of the Anti-Money Laundering Act (AMLA) and the offense of money laundering under Art. 305bis of the Swiss Criminal Code are **closely linked**, if only - because the reporting obligation serves as a pivotal link between the obligations under the AMLA and criminal prosecution, particularly that of money laundering (see *supra* N. 4). 63

In a landmark decision, the Federal Supreme Court relied in particular on the reporting obligation to conclude that the financial intermediaries held a **position of guarantor** within the meaning of Art. 11 of the Swiss Criminal Code. Indeed, our High Court ruled that "*since the AMLA came into force, financial intermediaries have been in a special legal situation that obliges them, in particular, to clarify the economic background and purpose of a business relationship when there are indications that assets may be derived from a crime, and to immediately notify the* [MROS] *if they know or suspect, based on reasonable grounds, that the assets involved in the business relationship are related to an act of money laundering or are derived from a crime*." Consequently, and given the current state of Federal Supreme Court case law, persons subject to the Anti-Money Laundering Act (AMLA) may be punished for money laundering by omission, particularly if it is established, from the perspective of hypothetical causation, that performing the act that was wrongfully omitted (typically, reporting to MROS) would have prevented the occurrence of the result that actually occurred. It should be noted, however, that 64

when a financial intermediary or dealer subject to the AMLA is organized as a business (see *below* N. 167 et seq.), the group of potential perpetrators of money laundering by omission is strictly defined by **Art. 29 of the Swiss Criminal Code (CP)**, which covers officers, partners, employees with independent decision-making authority, and de facto managers—thus specifically excluding, in particular, subordinate employees.

65 Furthermore, in practice, there is a certain tendency to view failure to comply with the reporting obligation under Art. 9 of the Anti-Money Laundering Act (AMLA) as **evidence of intent** with respect to money laundering . Such a simplistic conclusion must be **rejected**. Indeed, even if it is theoretically conceivable, in certain specific cases, that the failure to report to MROS might indicate the perpetrator's intent to obstruct the forfeiture of assets of illicit origin, any automatic conclusion or presumption in this regard would not only be dangerous but also contrary to the *ratio legis* of Art. 9 of the Anti-Money Laundering Act (AMLA). Indeed, a person who violates their administrative obligations—even intentionally, where applicable—does not *ipso facto* intend to obstruct the confiscation of assets. Recent case law from the Federal Supreme Court also supports this view. Indeed, according to a significant ruling handed down in September 2025, the fact that a financial intermediary has violated its due diligence obligations under the Anti-Money Laundering Act (AMLA) does not in itself allow for the conclusion that existence of (possible) intent to launder within the meaning of Art. 305bis of the Swiss Criminal Code. Furthermore, it should also be noted that, in the context of Art. 37 of the Anti-Money Laundering Act (AMLA), the perpetrator's intent need not relate to the criminal origin of the assets, but (solely) to the existence of a reportable fact. This additional element confirms that any conflation of the reporting obligation and the criminal offense of money laundering would be legally erroneous.

6. The *nemo tenetur* principle (Art. 14(3)(g) of the Second UN Covenant, Art. 6(1) of the ECHR, and Art. 32 of the Swiss Constitution)

66 Reporting under Art. 9 of the Anti-Money Laundering Act (AMLA) is an **active form of cooperation with the criminal justice system**, to which the financial intermediary or dealer is bound by Art. 37 of the AMLA. Thus, one may ask whether a financial intermediary or dealer who risks incriminating themselves—particularly in light of Art. 37 of the Anti-Money Laundering Act

(AMLA), or even Art. 305bis or 305ter of the Swiss Criminal Code (SCC)—in the context of a report to MROS—can invoke the **principle of *nemo tenetur* to refrain from making the report**. Indeed, according to this principle—which is enshrined in Art. 14(3)(g) of the Second UN Covenant and derived by case law from Art. 6(1) of the ECHR and Art. 32 of the Swiss Constitution—the defendant in criminal proceedings is not required to testify, nor, *a fortiori*, to actively contribute to his or her own incrimination. Furthermore, the exercise of this right may not prejudice the defendant nor constitute evidence or an indication of guilt.

To date, **case law** has not clearly answered the question of whether invoking the *nemo tenetur* principle exempts the person concerned from the obligation to provide information. **Legal scholarship** is also divided on this issue, although the majority of scholars seem to favor this possibility. 67

In our view, it is not possible to agree with those who regard the *nemo tenetur* principle as a justification for failing to make a report in accordance with Art. 9 of the Anti-Money Laundering Act (LBA). The key point is that the **nemo tenetur principle applies only in criminal proceedings**. Indeed, according to settled case law, the *nemo tenetur* principle grants—in the context of a criminal trial—the right not to actively contribute to one's own incrimination, which implies that criminal authorities—and they alone—may not rely on evidence obtained through pressure or coercion, against the will of the accused. It follows that the *nemo tenetur* principle cannot preclude the disclosure obligation, which falls solely under administrative law; however, it may, where applicable, nevertheless result in evidence gathered on this basis being inadmissible in any criminal proceedings against the person who made the disclosure. 68

II. OVERVIEW OF THE VARIOUS SCENARIOS ENVISAGED BY ART. 9 OF THE ANTI-MONEY LAUNDERING ACT (AMLA)

Art. 9 of the Anti-Money Laundering Act (AMLA) currently covers four scenarios in which it establishes a reporting obligation. Furthermore, in September 2025, the legislature decided to extend the reporting obligation to advisors as part of the revision of the AMLA, which will take effect on October 1, 2026 (see *supra* N. 18). Thus, the scenarios covered by Art. 9 of the Anti-Money Laundering Act (AMLA) can be summarized schematically as follows: 69

70 The various scenarios are presented below, grouped according to the parties to whom they apply, namely financial intermediaries (see *infra* Chapter III), dealers (see *infra* Chapter IV), and advisors (see *infra* Chapter V). Where the requirements are identical, reference will be made to the relevant discussions already presented.

III. REPORTING OBLIGATIONS OF FINANCIAL INTERMEDIARIES (PARA. 1)

A. Addressees: Financial Intermediaries

71 The reporting obligation set forth in Art. 9, para. 1, AMLA applies to **financial intermediaries** within the meaning of Art. 2, para. 1, AMLA, a term that encompasses both financial intermediaries subject to prudential supervision (Art. 2, para. 2, AMLA) and those that are not (Art. 2, para. 3, AMLA). Furthermore, the personal scope of application of Art. 9 AMLA has been discussed above (see *supra* N. 19 et seq.).

B. Conditions

72 Financial intermediaries are subject to a reporting obligation in three distinct scenarios. The "classic" scenario—and the most common in practice—involves a situation where the financial intermediary knows or has reasonable grounds to suspect that the assets involved in a **business relationship** are linked to certain crimes or offenses (Art. 9, para. 1, subpar. a, AMLA). The second scenario extends the reporting obligation under subparagraph (a) to the period prior to the establishment of any business relationship, in the event of a **breakdown in negotiations** aimed at establishing such a relationship (Art. 9(1)(b) AMLA). Finally, the third scenario falls within the framework of combating the **financing of terrorism** and supplements Art. 9(1)(a) AMLA (Art. 9(1)(c) AMLA). This scenario differs from the others in that it focuses on the identity of the persons involved in the business relationship business relationship rather than on the assets involved in the business relationship or intended to be involved.

1. Reporting Obligation in the Event of Suspicions Regarding Assets Involved in the Business (para. 1(a))

The reporting obligation under **Art. 9(1)(a) AMLA** is triggered as soon as the financial intermediary knows or suspects, based on reasonable grounds, that the assets involved in the business relationship are linked to certain crimes or offenses. 73

a. Subject of the suspicion: Assets involved in the business relationship

The reporting obligation under Art. 9(1)(a) of the Anti-Money Laundering Act (AMLA) exists only where there are **assets involved in a business relationship**. The assets therefore constitute the subject of the suspicion. 74

In the context of combating money laundering, the term **asset** refers to any element of one's estate or, in other words, any asset with economic value. According to case law, it must be interpreted broadly and encompasses, in particular, book money, i.e., account balances held with financial institutions. The concept of "asset" under Art. 9 of the Anti-Money Laundering Act corresponds to that in Arts. 70 and 305bis of the Swiss Criminal Code and not to the narrower meaning used in offenses against property (Arts. 137 et seq. of the Swiss Criminal Code). By contrast, the isolated view—according to which a suspicion concerning **the persons involved or their actions** also triggers the reporting obligation—appears to us to be contrary to the unambiguous wording of the provision and its purpose. It must be clearly rejected. That said, such a suspicion may necessitate further clarifications within the meaning of Art. 6(2) of the Anti-Money Laundering Act (AMLA), which must also address the assets involved in the business relationship and linked to the person concerned. 75

A **business business relationship** within the meaning of Art. 9 of the Anti-Money Laundering Act (AMLA) exists not only in the case of a long-term contractual relationship but also in the case of a one-time relationship, such as a single transaction or a cash transaction. In distinction to Art. 9(1)(b) of the AMLA, the decisive factor is above all that there is a business relationship, however simple it may be, and not merely negotiations aimed at establishing such a relationship; the relevant criterion is whether there is agreement on the essential elements of the business relationship (see *infra*, N. 120 et seq.). 76

77 *Assets over which the financial intermediary has power of disposal are deemed to be involved in the business relationship the business relationship. Also included, in light of the purpose of Art. 9 of the Anti-Money Laundering Act (AMLA), are assets over which the financial intermediary has had power of disposal in the past and which have since left its sphere of influence. The question arises, however, as to whether assets that have merely been reported can be considered to be already included in the relationship under Art. 9(1)(a) AMLA. The Appeals Chamber of the Federal Criminal Court favors this view, while scholarly opinion is divided. The inclusion of these assets—which, from a teleological perspective, may understandably appear desirable—seems to us, however, difficult to reconcile with a literal interpretation of the provision and would would extend an obligation that is already very broad. In any event, the principle of legality (Art. 1 of the Swiss Criminal Code) precludes, in our view, criminal prosecution (Art. 37 of the Anti-Money Laundering Act) of a financial intermediary who delayed or failed to report assets that had merely been declared, without ever having had the power to dispose of them .*

78 In a recent order dismissing the case—which was subsequently overturned on appeal—the Criminal Division of the Federal Criminal Court held that only **confiscatable** assets fall under Art. 9 of the Anti-Money Laundering Act (AMLA), drawing a parallel with the applicable case law on money laundering under Art. 305bis of the Swiss Criminal Code (SCC). In our view , it is not possible to simply transpose the case law established under Art. 305bis of the Swiss Criminal Code to Art. 9 of the Anti-Money Laundering Act (AMLA), because the latter provision pursues a broader objective than the suppression of money laundering. The purpose of Art. 9 AMLA thus requires that suspicions be reported in order to facilitate the prosecution of potential offenses and, ultimately, the confiscation of illicit assets (see *supra* N. 5). Furthermore, it is not the responsibility of the financial intermediary to determine whether the assets in question are subject to forfeiture; case law frequently reiterates that it is not the role of the financial intermediary to resolve complex legal issues, such such as, for example, the statute of limitations for criminal prosecution or the existence of a valid criminal complaint.

b. Nature of the Suspicion: Link to Certain Crimes or Offenses

79 The financial intermediary's suspicion that triggers the reporting obligation must relate to the **connection between the assets and certain crimes or**

offenses. Art. 9, para. 1(a) of the Anti-Money Laundering Act (AMLA) contains four subparagraphs, with several sub-variants, describing which offenses are relevant and what the connection must be between the assets in question and these offenses. It thus follows from the structure of the law that the suspicion cannot relate to just any criminal offense or factual situation, but only to those explicitly defined.

Subparagraph 1 of Art. 9(1)(a) of the Anti-Money Laundering Act (AMLA) concerns the suspicion that the assets are related to one of the offenses set forth in Articles 260ter and 305bis of the Swiss Criminal Code (SCC), namely participation in or support of a criminal or terrorist organization and money laundering, respectively. This provision serves as a catch-all clause covering situations not covered by the other provisions. Furthermore , it is hardly possible to require the financial intermediary to conduct a detailed analysis of the elements of the two offenses; its reasonable suspicion is sufficient in any case. 80

Therefore, the "**connection**" to the aforementioned offenses must not be interpreted narrowly; it refers to any link that is sufficiently direct for the report to MROS to contribute to the criminal prosecution of the aforementioned offenses and, where applicable, to the forfeiture of the relevant assets. 81

regarding the first variant of paragraph 1, Art. 260ter of the Swiss Criminal Code prohibits participation in and support of a **criminal or terrorist organization**. This applies to organizations whose purpose is to commit acts of criminal violence or to obtain income through criminal means (so-called criminal organizations), or to commit acts of criminal violence aimed at intimidating a population or compelling a State or an international organization to perform or refrain from performing any act (so-called terrorist organizations) . In addition to mafia-style criminal syndicates, the concept of a criminal organization also encompasses terrorist groups. By contrast, extremist parties, opposition political groups, and organizations that strive through appropriate, non-criminal means to attain political power in their country of origin or that wage a struggle for freedom against dictatorial regimes are, in principle, not considered as such. **B Participation**B in a criminal or terrorist organization is intended to punish individuals who are functionally integrated into the criminal organization and who carry out activities aimed at furthering its criminal objectives, without these activities having to be, in and of themselves, illegal or constitute offenses. In the absence of such integration, **support** alone is sufficient; it consists of a conscious contribution to the promotion of the orga- 82

nization's criminal activities, and proof of a causal contribution to a specific offense is not required. According to legal scholarship, the reference to Art. 260ter of the Swiss Criminal Code (CP) is intended to cover situations in which assets are linked to a criminal or terrorist organization but cannot be connected to a crime within the meaning of Art. 10(2) CP (a scenario covered by subparagraph 2; see *infra* N. 85 et seq.), nor are they subject to the control of such an organization (a scenario covered by subparagraph 3; see *infra* N. 94 et seq.), nor are they used to finance terrorism (a scenario covered by subparagraph 4; see *infra* N. 97 et seq.).

83 With regard to the reference to Art. 305bis of the Swiss Criminal Code (CP), namely **money laundering**, this provision applies to anyone who commits an act intended to obstruct the confiscation of assets that they know or should presume to be derived from a crime or an aggravated tax offense (see *supra* N. 63 et seq.). An **act intended to obstruct confiscation** is any conduct that hinders the criminal justice authorities to the proceeds of a crime or a qualified tax offense, thereby complicating the determination of the illicit origin of said assets. Thus, the provision primarily targets conduct intended to give said assets the appearance of legality, with the aim of reintroducing them into the legal economy and avoiding their confiscation by the authorities. The following, in particular, are considered acts intended to obstruct confiscation: (i) active physical concealment, (ii) the consumption of the assets but not their destruction, (iii) currency exchange transactions, particularly into another currency, (iv) transactions that go beyond a simple conversion of cash into book money or a simple bank deposit—such as, in particular, the deposit of money into an account whose holder is not the beneficial owner , (v) cash withdrawals that sever the "*paper trail*," (vi) transfers or disposals between accounts abroad, to the extent that the transaction is actually likely to impede confiscation abroad, and (vii) the purchase or sale of real estate. By contrast, neither the investment of the assets in question in goods for personal use nor the mere deposit into a personal bank account —opened at the place of residence and used for routine private payments—do not, in and of themselves, constitute acts of obstruction. The same applies to the mere possession or safekeeping of tainted assets. With regard to domestic and international bank transfers, it should be noted that a mere extension of the "*paper trail* " generally does not constitute an act of money laundering, as long as there are no other acts of concealment and the assets are still subject to forfeiture. Due to its accessory nature, the offense of money laundering requires, in addition to

proof of the act of obstruction, proof of **the predicate offense** as well as the origin of the assets from the predicate offense.

Art. 9(1)(a)(1) of the Anti-Money Laundering Act (AMLA) has only a **limited scope** with respect to money laundering under subparagraph 2, which encompasses all assets derived from a felony or a qualified tax offense that are susceptible to laundering. Subparagraph 1 therefore ultimately applies to assets that do not derive from a felony or a qualified tax offense but that nevertheless a connection to money laundering. This is primarily the case with the consideration that the perpetrator of simple money laundering—that is, money laundering that is not aggravated within the meaning of Art. 305bis, para. 2, of the Swiss Criminal Code (CP)—receives for their actions, to the extent that it does not derive from the predicate offense. 84

Subparagraph 2 of Art. 9(1)(a) of the Anti-Money Laundering Act (AMLA) is **the most common** in practice. It covers situations where the assets derive from a felony within the meaning of Art. 10(2) of the Swiss Criminal Code (SCC) or from an aggravated tax offense within the meaning of Art. 305bis, item 1bis of the Swiss Criminal Code (CP). This excludes offenses within the meaning of Article 10(3) of the Swiss Criminal Code (with the exception of aggravated tax offenses), as well as misdemeanors within the meaning of Art. 103 of the Swiss Criminal Code (CP). In substance, the assets subject to reporting correspond to those that may be the subject of money laundering within the meaning of Art. 305bis of the Swiss Criminal Code (CP). 85

With regard to the concept of **origin**, the Federal Supreme Court has ruled—admittedly in connection with Arts. 30bis 5bis and 70 of the Swiss Criminal Code, but in a manner applicable to Art. 9(1)(a)(2) of the Anti-Money Laundering Act (AMLA), that assets derive from a crime when the causal link to the crime is natural and adequate. Two clarifications are in order here. 86

First, "derive from" obviously does not mean "be intended for." The causal link must therefore run **in a specific direction**. Indeed, if the assets were acquired legally, they are not subject to the reporting obligation simply because they are intended for subsequent use for criminal purposes, subject to the other scenarios set forth in Art. 9 of the Anti-Money Laundering Act (LBA). Similarly, as recently clarified by MROS in its negative typologies, when the financial intermediary's client is the victim of fraudulent activities resulting in transfers to the fraudsters, no reporting obligation is triggered because the as- 87

sets are lawful and become tainted, from a criminal law perspective, only after their transfer from the victim's account to that of the perpetrators of the offense in question. The absence of criminal origin also applies in the event of losses to the financial intermediary's own funds, for example due to cyberattacks or fraudulent payments; these assets never having been involved in a business relationship in the first place.

88 Second, a **sufficient causal link** undoubtedly exists for the direct proceeds of the principal offense (*producta sceleris*), as well as for the reward received by the perpetrator for committing the offense (*pretium sceleris*; see Art. 70(1) of the Swiss Criminal Code) . Furthermore, according to case law regarding Articles 305bis and 70 of the Swiss Criminal Code (CP), it is not necessary for the assets to result directly and immediately from the offense; this is similar to assets arising from a contract whose conclusion was facilitated by acts of corruption. The concept of "proceeds" referred to in Article 9 of the Anti-Money Laundering Act (LBA), when interpreted teleologically, may be even broader. Indeed, the Federal Administrative Court has held that Art. 9 of the Anti-Money Laundering Act (AMLA) is based on a broader objective than Art. 305bis of the Swiss Criminal Code (SCC), particularly with regard to prevention and the reputation of the Swiss financial center, and that, consequently, the reporting obligation must be interpreted to cover the greatest possible number of assets for which there are reasonable grounds to suspect criminal origin. Furthermore, the Federal Administrative Court emphasizes that, in practice, financial intermediaries are often unable to analyze in detail which offense the assets stem from and whether it constitutes a predicate offense to money laundering. Indeed, since reasonable suspicion is sufficient under Article 9 of the Anti-Money Laundering Act (AMLA), the financial intermediary is not required to establish the source with certainty. However, the suspicion must relate to a link that is as concrete as possible to a predicate offense (in the non-technical sense), as a report cannot be based on mere risk factors or the fact that the customers are suspected.

89 The reporting obligation under Art. 9(1)(a)(2) of the Anti-Money Laundering Act (AMLA) applies to assets derived from a **crime**, that is, an offense punishable by imprisonment for more than three years (Art. 10(2) of the Swiss Criminal Code) . In an international context—which is not uncommon in money laundering cases—the concept of a "crime" is always that defined under Swiss law, although the act must also be punishable under the law of the place

where it was committed (see Art. 305bis, item 3, of the Swiss Criminal Code). Given that it will often be difficult for the financial intermediary to identify the specific crime or make the legal distinction between a felony and a misdemeanor, the requirement of a "crime" under Art. 9(1)(a)(2) of the Anti-Money Laundering Act (AMLA) should not be interpreted too strictly, especially since the reporting obligation does not require certainty but rather reasonable suspicion. According to a recent ruling by the Federal Criminal Court, "*it is not necessary for the financial intermediary to know exactly what type of crime the assets stem from , nor is it necessary for the reasonable suspicion to be linked to a specific crime* [...]. *In this context, knowledge of or a presumption regarding a serious predicate offense is sufficient to trigger the reporting obligation*." In cases of doubt regarding the legal classification of the predicate offense or its capacity to generate assets subject to forfeiture, a report must therefore be filed. An exemption from this obligation is possible only if it is established with certainty that there is no prior offense or that it does not constitute, respectively, a crime or (in a non-technical sense) a "serious offense." This is particularly the case in the presence of a simple misdemeanor (Art. 103 Swiss Criminal Code) . The cautious approach mentioned above is, moreover, consistent with Art. 20(2) of the Anti-Money Laundering Ordinance (OBA) applicable to money transmitters (see *infra*, Chapter IV), which provides that a report to MROS must also be filed when the money transmitter cannot link the cash payments to a specific offense.

In addition to felonies, **aggravated tax offenses** within the meaning of Art. 305bis, item 1bis of the Swiss Criminal Code (CP) may also trigger the reporting obligation. The legal definition set forth in this provision is based on two cumulative conditions, which raise undeniable practical difficulties. 90

First, the legal definition covers offenses of forgery within the meaning of Art. 186 of the Federal Income Tax Act (LIFD) and **tax fraud** within the meaning of Art. 59(1) of the Federal Law on Indirect Taxes (LHID) in the context of taxes on income and wealth, profits and capital, as well as real estate gains. However, it is usually impossible for the financial intermediary to detect the use of forged documents—an essential element of these two tax offenses—because the intermediary typically does not have access to the relevant tax documents. In light of Art. 9(1)^{quater} of the Anti-Money Laundering Act (AMLA), the central question is therefore often whether there are indications requiring the financial intermediary to conduct further investigations; this is the case, in par- 91

ticular, if the use of a forgery is characteristic of or necessary for the tax fraud in question. If the suspicions cannot be dispelled, the reporting obligation comes into play. With regard to tax offenses committed abroad, the relevant classification is that under Swiss law, as mentioned above for crimes. However, the act must also be punishable under the (foreign) law of the place where the act was committed. In this regard, the Explanatory Memorandum advocates a broad interpretation, holding that the punishability of "simple" tax evasion abroad is already sufficient.

92 Second, Art. 305bis, para. 1bis of the Swiss Criminal Code (CP) requires that the evaded taxes amount to **more than 300,000 francs** per tax period. The practical application of this threshold is somewhat facilitated by Art. 21 of the FINMA Anti-Money Laundering Ordinance (OBA-FINMA), pursuant to which financial intermediaries may apply the maximum tax rate of the client's country of tax residence to determine whether the evaded taxes have reached 300,000 francs.

93 Finally, further clarification is needed regarding the concept of **source in connection with tax offenses**: the main issue here is that tax evasion generally does not directly generate assets, but rather a tax savings—that is, a lack of expenditure. Such assets are **not in themselves traceable** within the offender's perpetrator. The Federal Supreme Court nevertheless recognizes that such savings, achieved through a tax offense, may be subject to forfeiture and thus constitute proceeds of money laundering in the event of a potential obstruction of their forfeiture. Legal scholars have therefore sought a criterion that would nevertheless allow them to be identified, through a sort of legal fiction. One approach that has been considered—but largely rejected—would be to consider that the taxpayer's entire estate is tainted. Other, more measured solutions have also been proposed: (i) tainting limited to undeclared assets or those generally used to pay taxes; (ii) tainting of undeclared assets in proportion to the undue tax savings realized; (iii) tainting of undeclared assets up to the amount of the tax savings , assuming that this amount is either the first (the so-called "oil film" theory) or the last (the so-called "sediment" theory) to be reached by any acts of disposition. To the best of our knowledge, case law has not yet had the opportunity to clarify how, in practice, contaminated assets should be identified within a person's estate in the event of an aggravated tax offense. There is therefore currently a **state of uncertainty** that is all the more regrettable given that criminal penalties may apply to acts of disposition

involving such assets. Admittedly, in the more general context of the commingling of illicit assets with lawful assets—typically in a bank account—the Federal Supreme Court recently ruled in favor of the so-called "sedimentation" or "floor" approach, while reserving judgment on cases where the *modus operandi* corresponds to acts typical of money laundering. However, there is no indication at this stage that the reasoning in that ruling can be applied *mutatis mutandis* to the laundering of proceeds from a qualified tax offense.

Subsection 3 of Article 9(1)(a) of the Anti-Money Laundering Act (AMLA) refers to assets that are subject to the control of a criminal or terrorist organization. No prior offense is required, as long as the assets are subject to the control of such an organization. 94

The concept of a **criminal or terrorist organization** has already been discussed in connection with paragraph 1, to which reference is made (see *supra* N. 82). 95

Furthermore, the assets involved in the business relationship must be subject to the **power of disposal** of the criminal or terrorist organization. This concept also appears in Art. 72 of the Swiss Criminal Code (CP) on confiscation and may be interpreted analogously. Thus, one should not rely on a formal legal approach. What is decisive, first and foremost, is the economic conception of beneficial ownership, which includes the actual power to dispose of the assets. This is justified above all in light of the methods typically used by organized crime to manage its assets —namely, the use of shell companies or straw men, but also of bona fide third parties. Furthermore, the concept of power of disposition is closely related to that of "control," which plays an essential role in property offenses and which, according to case law, consists of the ability and willingness to possess the assets ("*in der tatsächlichen Sachherrschaft, verbunden mit dem Willen, sie exercise*"). Consequently, a criminal organization clearly exercises power of disposition when the business relationship falls under its control or when members of the organization can, as part of their membership (or even on the organization's orders), dispose of assets deposited with a financial intermediary. In this context, it is worth noting the second sentence of Art. 72 of the Swiss Criminal Code (CP), which contains a rebuttable presumption that assets belonging to a person who has participated in or supported a criminal or terrorist organization are presumed to be to the organization's power of disposal. Although this provision is not directly applicable in the context of the Anti-Money Laundering Act (AMLA), 96

the legal definition of "reasonable suspicion" under Art. 9(1^{quater}) AMLA is very similar, since the financial intermediary is, in principle, required to conduct additional due diligence as soon as it has any doubt regarding a person's membership in such an organization; only if it succeeds in dispelling all of its suspicions regarding the assets involved in the business relationship that it may refrain from reporting. The question of whether a criminal organization exercises power of disposal when its members are merely the beneficial owners of the assets depends on the organization's actual ability and willingness to exercise control. However, even if the organization lacks power of disposal, Art. 9(1)(a)(1) of the Anti-Money Laundering Act (AMLA) may still be applicable. This provision simply requires a connection between the assets and the offense of participation in or support of a criminal or terrorist organization (see *supra* N. 80 et seq.).

97 **Paragraph 4** of Art. 9(1)(a) of the AMLA refers to assets that are used to finance terrorism. This provision was introduced as part of the expansion of the AMLA to combat the financing of terrorism, notably based on recommendations from the FATF. While money laundering involves reintroducing illegally acquired capital into the legal economic system, in the context of terrorist financing, it is lawful funds that are, in principle, used for criminal purposes. These lawful funds are the subject of suspicion under paragraph 4. Within the framework of Art. 9(1)(a) of the Anti-Money Laundering Act (AMLA), this provision thus primarily covers funds that do not originate from a criminal offense (a scenario covered by paragraph 2; see *supra* N. 85) and that are not subject to the control of a terrorist organization (a scenario covered by paragraph 3; see *supra* N. 94 et seq.). The scope of application of subparagraph 4 therefore appears limited, given that the consideration for supporting a terrorist organization is deemed to derive from a crime and that the concept of power of disposal is interpreted broadly.

98 In practice, it will often be difficult for the financial intermediary to recognize the indicators of **terrorist financing**. As in Art. 260^{quinquies} of the Swiss Criminal Code, to which Art. 9 of the Anti-Money Laundering Act (AMLA) explicitly refers, terrorism consists of an act of criminal violence intended to intimidate a population or to compel a state or an international organization to perform or refrain from performing any act, unless the act is intended to establish or restore a democratic regime or the rule of law, or to enable the exercise or protection of human rights. The concept of financing, for its part,

must be interpreted broadly; it is sufficient that funds be made available to a person associated with terrorism or, again, as in Art. 260^{quinquies}, para. 1, of the Swiss Criminal Code (CP), that they are merely gathered for future use for such purposes.

c. Threshold of Suspicion and Triggering Factor: Knowledge or Reasonable Suspicion

99 The reporting obligation under Art. 9(1)(a) of the Anti-Money Laundering Act (AMLA) is triggered if the financial intermediary **knows or suspects, based on reasonable grounds,** that the assets are linked to any of the offenses listed in items 1 through 4 above.

100 The term "**know**" means that the financial intermediary has no doubt regarding the existence of this link. In legal scholarship, it is often described as the highest degree of suspicion. The practical scope of this threshold of suspicion is limited, however, since it is rare for a financial intermediary to have certain knowledge of a link between the assets and a criminal offense. Legal scholarship discusses the relatively theoretical scenario in which the reason for the transfer would be disclosed to the financial intermediary by the contracting party or would be evident from a court decision. Even in such cases, however, the source must be credible for the financial intermediary to be said to "know." The term "know" in the context of Art. 9 of the Anti-Money Laundering Act (AMLA) does not correspond to the element of intent in Art. 305bis of the Swiss Criminal Code (SCC), as intent—in relation to money laundering—generally plays no role under Art. 9 of the AMLA.

101 The threshold that is most often decisive in practice is therefore that of a presumption based on **reasonable suspicion**. This concept has been codified since January 2023 in Art. 9, para. 1^{quater} of the Anti-Money Laundering Act (AMLA), according to which there is reasonable suspicion when the financial intermediary "*has a concrete indication or several clues suggesting that the criteria defined in paragraph 1, subparagraph a, might be met with respect to the assets involved in the business relationship, and that the additional clarifications carried out pursuant to Article 6 do not dispel the suspicions*." This legal definition, modeled on recent Federal Supreme Court case law and the definition set forth in the Anti-Money Laundering Ordinance (OBA) for dealers, was adopted by the Federal Parliament shortly before the final vote on the comprehensive revision of the Anti-Money Laundering Act (LBA) in 2021. It

thus follows from Art. 9 para. 1quater of the Anti-Money Laundering Act (LBA) that the financial intermediary, as soon as it harbors suspicions, must continue its investigations until it ascertains the facts. Either the transaction that appeared suspicious is legitimate, or its doubts are not fully dispelled, in which case its suspicions are deemed well-founded and must be reported to MROS. From From a theoretical perspective, this process can be divided into two stages: the initial suspicion and further clarification.

10 2 In the first stage, leading up to the threshold that triggers the reporting obligation, the financial intermediary must **have a concrete indication or several clues suggesting** that the criteria defined in para. 1(a) might be met (Art. 9(1quater) AMLA, first part of the sentence). It is not easy to determine what the legislature—and, before it, case law and the Federal Council—meant by the reference to "*a concrete indication*" or "*several indications*." This wording primarily conveys the idea that suspicion depends on both the quality and the quantity of the elements underpinning it. Thus, the circumstances that may give rise to suspicion are numerous and can stem from a wide variety of sources, both internal and external to the financial intermediary, such as the media or information from criminal prosecution authorities. However, these circumstances must reach a certain minimum threshold of suspicion. Indeed, since the adoption of the Anti-Money Laundering Act (AMLA), established case law has consistently emphasized that, in principle, it is not the responsibility of the financial intermediary to systematically search for potential criminal conduct in every transaction, while specifying that the financial intermediary is required to exercise the due diligence called for by the circumstances. This minimum threshold generally corresponds to that set forth in Art. 6 of the Anti-Money Laundering Act (AMLA), specifically paragraph 2, since the second part of the legal definition now enshrined in Art. 9, para. 1quater of the AMLA expressly refers to additional clarifications within the meaning of that article. This also appears consistent from a systematic and teleological perspective, as the reporting obligation serves as a link between the due diligence obligations—of which Art. 6 of the AMLA is a part—and the measures taken by criminal prosecution authorities . It should also be noted that the existence of signs or indications of money laundering must be assessed *ex ante*—that is, by returning to the time when the events occurred—which is particularly relevant in connection with the criminal liability incurred under Art. 37 of the Anti-Money Laundering Act (AMLA) in the event of a breach of the reporting obligation.

With reference to legal scholarship, the case law cites, as **examples of indications of money laundering**, the urgency of a financial transaction, the inability to contact the customer, the customer's refusal to provide the information necessary to clarify the economic background of the transaction or the business relationship, or media reports regarding the initiation of criminal proceedings concerning a crime against the customer or the beneficial owner of the assets involved in the business relationship. In accordance with case law, reference should also be made to the list of indicators of money laundering in the annex to the OBA-FINMA. While this list expressly states that, taken individually, these indicators generally do not provide sufficient grounds for suspicion of money laundering, and that it is rather the combination of several of these elements that may indicate its presence. Nevertheless, it is entirely possible, in light of the legal framework—if not the wording of Art. 9(1)^{quater} of the Anti-Money Laundering Act (AMLA), that the presence of **a single indicator of money laundering** — if it cannot be dispelled by further inquiries — is sufficient to trigger the reporting obligation. According to the general indicators contained in the annex to the FINMA Anti-Money Laundering Ordinance (OBA-FINMA), transactions present a particular risk of money laundering when they have no recognizable economic purpose or an absurd economic purpose, when they involve a rapid withdrawal of assets without a plausible justification, or when they are inconsistent with the information known to the financial intermediary regarding the customer or the business relationship. Any customer who provides false or misleading information, or who refuses, without valid reason, to provide the information requested by the financial intermediary, is also considered suspicious. Furthermore, regular transfers to or from high-risk countries, or countries near areas of terrorist activity, may constitute indicators of money laundering. In addition to these general indicators, the Annex to the OBA-FINMA also contains specific indicators for particular transactions, such as cash, account, or deposit transactions, as well as fiduciary transactions. Finally, there are indicators that the Annex considers to be "qualified." These primarily concern client behavior that reveals a clear intent to conceal or manipulate financial transactions, such as a client's desire to close an account in order to open new ones without leaving a paper trail, a request for fictitious receipts, or the desire to make transfers with an inaccurate payer or to use the institution's internal accounts (such as Nost ro or "Miscellaneous"). Furthermore, the existence of criminal proceedings against the customer for corruption, embezzlement of

10 3

public funds, or a serious tax crime or offense constitutes a qualified indication of money laundering.

10 4 If there is one or more indications suggesting that the criteria defined in Art. 9(1)(a) of the Anti-Money Laundering Act (AMLA) might be met, the second step toward meeting the threshold set forth in Art. 9(1)^{quater} of the Anti-Money Laundering Act (AMLA)—and which will effectively trigger the reporting obligation—requires that the **additional inquiries** conducted by the financial intermediary pursuant to Art. 6 of the Anti-Money Laundering Act (AMLA) do not dispel the suspicions. It follows from the legal definition that "reasonable suspicion" should not be understood as suspicion that has intensified or been confirmed as a result of the inquiries, but rather as suspicion that **could not be entirely dispelled** following the inquiries. The distinction is subtle, but nonetheless essential. In the event of (mere) doubt remains following the clarifications, there is an obligation—and not merely a right—to report.

10 5 This raises the question of the **procedures for clarifications** that may, or rather must, be carried out by the financial intermediary before suspicions are deemed well-founded. As a general rule, in order to reach a decision, the financial intermediary must clarify the economic background and purpose of a transaction or the business relationship (see Art. 6(2) AMLA). According to case law, the business relationship must always be assessed as a whole, as the specific obligation to clarify is not limited to isolated transactions. The practical implementation of these clarifications involves a balancing act between the requirements of speed and quality.

10 6 Regarding the **timing of** additional clarifications, one can, on the on the one hand, draw on Art. 17 of the Anti-Money Laundering Ordinance (OBA) -FINMA, which requires the financial intermediary to undertake additional due diligence as soon as initial suspicions arise and to complete it as quickly as possible. This is also consistent with the requirement of immediacy arising from Art. 9 of the Anti-Money Laundering Act (see *infra* N. 188 et seq.). On the other hand, despite these requirements for speed, the quality of the communication—and thus the scope of the investigations—must not be neglected, as MROS rightly emphasized in its 2024 Annual Report: "[The system under Art. 9 of the Anti-Money Laundering Act] *presupposes that* [financial intermediaries] *can take the time necessary to conduct the required due diligence to an adequate degree. The time required varies from case to case depending on the risk, the facts, and the complexity of the business relationship. The* [finan-

cial intermediary] *needs a certain degree of flexibility in choosing how to clarify the case and the time required to do so. Consequently, it is not possible to generalize about the correct or appropriate duration required for clarifications.* [...] *Nevertheless, the purpose of clarifications is for the* [financial intermediary] *to examine the facts in depth and form a well-founded opinion. Suspicion reports and the must meet certain substantive quality standards so that MROS can process them effectively. Incomplete or unclear facts complicate the analysis or even render it impossible. Such suspicious activity reports clog the reporting system and tie up unnecessary resources at MROS. They have a detrimental effect on the efficiency of report processing and, overall, weaken the anti-money laundering* ."

Consequently, one of the most important questions arising in light of Art. 9(1)^{quater} of the Anti-Money Laundering Act (AMLA) is undoubtedly that of the**scope of the additional due diligence** that the financial intermediary must undertake. Such due diligence must serve the purpose of the law, which aims to enable the confiscation of assets of illicit origin, or, more generally, to support criminal prosecution efforts. According to the aforementioned case law, the financial intermediary must conduct its investigations into the business relationship and/or the disputed transaction in a manner that allows it to ascertain the facts. However, the aim is to verify **plausibility**, without the financial intermediary being required to obtain clarifications to the point of establishing absolute certainty. The scope of the clarifications to be obtained will thus depend on the specific circumstances of the individual case. The financial intermediary must act with due diligence and, **to the extent possible and reasonable**, seek the clarifications that would dispel the initial suspicion. 10 7

When the clarifications lead to an **intensification of the suspicion**, it is easier to conclude that there are well-founded suspicions. Thus, case law holds that the report must be filed without delay—even if clarifications are still ongoing—if it appears that, in all likelihood, the doubt cannot be dispelled in any event. This may be the case if customers refuse to provide the requested information, it being noted that the absence of a response for a certain period may, in itself, give rise to additional doubts. 10 8

On the other hand, when the clarifications **reduce the suspicion**, without however completely dispelling it, it should be permissible, from a proportionality standpoint, to conduct a new round of clarifications if the financial intermediary has sufficient reason to believe that they may be successful and that it 10 9

can carry them out within a reasonable timeframe. In each specific case, a balancing of interests should therefore be conducted. This also applies where the clarifications are unsuccessful because the counterparty does not immediately respond to the financial intermediary's requests, although it should be noted that the information provided by the counterparty is the sole source of information. If the clarifications carried out within the described framework do not dispel the suspicions, a report must be filed without fail, even if the financial intermediary ultimately harbors merely a simple doubt.

110 The question also arises as to whether further clarifications must be undertaken even in the presence of an **obvious or immediately well-founded suspicion**. The wording of Art. 9(1)^{quater} of the Anti-Money Laundering Act (AMLA) suggests that the financial intermediary must, in all cases, conduct clarifications before filing a report with MROS. This is also the position expressed by MROS, which is of the opinion that "financial *intermediaries must always conduct due diligence within the meaning of Art. 6, para. 2, the AMLA before submitting a report*." According to MROS, this provision ensures the quality of reports submitted by financial intermediaries and the effectiveness of Switzerland's anti-money laundering framework. MROS notes in this regard that all reports must be as precise as possible.

111 The Federal Council's Message takes the same view, but qualifies this statement by specifying that "*in principle*," additional clarifications are necessary. It justifies its position by noting that it is necessary to avoid **so-called "defensive" reports** by financial intermediaries, who might otherwise be led to report any unusual transaction or any alert flagged by their monitoring system. This concern of the Federal Council appears legitimate. The practice of defensive reports is also criticized by MROS, even though it is understandable given the sanctions—particularly criminal ones—faced by financial intermediaries in the event of a breach of the reporting obligation.

112 In our view, when the financial intermediary knows—that is, has no doubt (or virtually no doubt)—that the assets are linked to a criminal offense (see *supra* N. 100), it should be able to **dispense with additional clarifications**—particularly for the sake of expediency—as long as the quality of the report's content is ensured. This applies *a fortiori* in cases where the business relationship is active and potentially confiscable assets are still available, bearing in mind that the purpose of the reporting obligation is to detect offenses and to enable the seizure of related assets as quickly as possible to seize assets linked to

such offenses. The decision to forgo any additional clarifications is also supported by recent case law. Indeed, case law holds that when a financial intermediary learns that criminal proceedings have been initiated against its client for a serious offense and that the assets in question could be linked to those proceedings, it must, as a general rule, opt for immediate reporting.

To determine whether there are reasonable grounds for suspicion, one must adopt **an ex ante perspective**. Given the clear wording of Art. 9 of the Anti-Money Laundering Act (AMLA), the facts known to the financial intermediary at the time the reporting was required are decisive, and circumstances discovered subsequently cannot be taken into account. 11 3

Furthermore, the question arises as to whether the obligation to report is triggered only when the financial intermediary has actually harbored reasonable suspicion, or whether it may also apply when the financial intermediary *should have* harbored such suspicion by exercising the diligence required by the circumstances. The practice of the Federal Criminal Court in applying Art. 37 of the Anti-Money Laundering Act (AMLA) has opted for the latter approach, which in a sense amounts to penalizing the violation of the obligation to investigate (Art. 6 AMLA). Such an approach seems hardly compatible with the plain language of Art. 9(1)(a) AMLA, which focuses on knowledge or suspicions (actually) held by the financial intermediary in question. It also conflicts with the principle of legality in criminal law (Art. 1 of the Swiss Criminal Code). That said, Art. 9(1)^{quater} of the Anti-Money Laundering Act, introduced on January 1, 2023, constitutes a first step toward the—desirable—objectivization of the trigger for the reporting obligation. Indeed, it provides that suspicions are well-founded whenever the financial intermediary "has a concrete indication or several clues suggesting that the criteria in paragraph 1(a) could be met with respect to the assets involved in the business relationship." The objectification is not, however, complete, since the provision further requires that "the additional clarifications carried out pursuant to Article 6 do not dispel the suspicions ," which once again falls within the discretion of the financial intermediary concerned. These observations highlight that Art. 9 of the Anti-Money Laundering Act (AMLA) contains inconsistencies that would justify a comprehensive revision. 11 4

Finally, it should also be noted that, in many cases, suspicions can be dispelled through additional due diligence. This situation forms the basis for Article 22a(2) of the OBA-FINMA, which provides that financial intermediaries have 11 5

an **obligation to document**, in a so-called *No-AML* report, the reasons why they did not file a report after dispelling any suspicions through additional clarifications. To the best of our knowledge, this obligation is typically incorporated into the regulations of self-regulatory organizations (SROs) for financial intermediaries not subject to the OBA-FINMA.

2. Obligation in the Event of Termination of Negotiations (para. 1(b))

11 6 Pursuant to **Art. 9(1)(b) of the Anti-Money Laundering Act (AMLA)**, financial intermediaries are required to file a report with MROS if they terminate negotiations aimed at establishing a business relationship due to well-founded suspicions that assets intended to be involved in the business relationship are linked to certain crimes or offenses.

11 7 This provision implements the FATF recommendations. Its **objective** is, on the one hand, to prevent the reporting obligation from being circumvented by terminating negotiations aimed at establishing a business relationship and, on the other hand, to enable the criminal justice authorities to be informed of illicit assets so that they can take appropriate measures. Statistics show that in recent years, approximately 5 to 8% of reports to MROS have resulted from the termination of negotiations.

a. Subject of the Suspicion: Assets Intended for Use in a Business Relationship Under Negotiation

11 8 Unlike Art. 9(1)(a) of the Anti-Money Laundering Act (AMLA), which concerns assets involved in an already established business relationship, Art. 9(1)(b) of the Anti-Money Laundering Act (AMLA) applies even before such a relationship is established—namely, during the negotiation phase. Consequently, the subject of the suspicion consists of assets **intended to be involved** in a business relationship currently under negotiation.

11 9 The concepts of "**assets**" and "**business relationship**," as well as the implicit condition—erroneously posited by certain court decisions and some legal scholars—that these assets must be **confiscatable**, have already been discussed in the context of Art. 9(1)(a) of the Anti-Money Laundering Act (AMLA). Reference may therefore be made to the above discussion (see *supra* N. 75 et seq.).

The central question is during what period the assets must be considered "**intended to be involved in a business relationship under negotiation**"—or, to put it another way, when a mere contact becomes a negotiation regarding a business relationship and when such a negotiation leads to a business relationship, since Art. 9(1)(b) of the Anti-Money Laundering Act (AMLA) applies only during this intermediate period of negotiations. 120

With regard to the **start of negotiations**, the Federal Council's Explanatory Memorandum expressly excludes "*initial discussions during the period when the financial intermediary does not yet have sufficient information*." It must therefore be determined whether an exchange of information has already taken place between the financial intermediary and the potential client. Personalized information appears relevant in this context, excluding, for example, the mere communication of the terms and conditions of financial services by the financial intermediary. Thus, the client must have provided a minimum amount of information about themselves and the desired financial services for it to be considered that negotiations have begun under the terms of Art. 9(1)(b) of the Anti-Money Laundering Act (AMLA). 121

With regard to the **end of negotiations**, there is a lively debate in legal scholarship, and to our knowledge, case law has not yet settled the issue. Legal scholars refer sometimes to the formal conclusion of the contract, sometimes to the receipt of funds, sometimes to the decision to activate the account, or even to the client's ability to use the services. It seems to us that reaching an agreement on the essential elements of the business relationship should be the relevant criterion (see *supra* N. 76). In any case, from a teleological perspective, the precise moment at which negotiations give way to a business relationship is, in our view, not decisive for the interpretation of Art. 9 of the Anti-Money Laundering Act (AMLA). Indeed, as Villard points out, "*one of two things will happen: either the financial intermediary terminates the negotiations due to a suspicion, in which case its decision will be based on Art. 9(1)(b) of the Anti-Money Laundering Act, or it does not do so, in which case the report must, if applicable, be based on Art. 9(1)(a) or (c) of the Anti-Money Laundering Act*." The most important point, therefore, is that a report to MROS must be filed in the presence of reasonable suspicion, regardless of the specific legal basis underlying it. That said, the timing of the termination of negotiations is relevant in determining whether the financial intermediary can still **terminate** the relationship with its client. Indeed, while terminating ne- 122

gotiations is possible, even in the case where the financial intermediary has reasonable suspicion, Art. 12*a*(1) OBA prohibits the financial intermediary from terminating the business relationship, once it has been established, when the conditions for reporting are met—regardless of whether a report has actually been filed—subject to the exceptions provided for in Art. 12*b* OBA (see *infra* N. 201 et seq.). The fact that the assets have not yet come under the financial intermediary's control is, moreover, irrelevant in this context.

b. Nature of the Suspicion: Link to Certain Crimes or Offenses offenses

12 3 As with Art. 9(1)(a) AMLA, the suspicion within the meaning of Art. 9(1)(b) AMLA must relate to the fact that the assets have a **connection to certain crimes or offenses**. Art. 9(1)(b of the Anti-Money Laundering Act (AMLA) refers to subparagraph (a), whose paragraphs 1 through 4 are therefore directly applicable. Thus, the reporting obligation applies if the assets intended to be involved in the business relationship (1) are related to one of the offenses listed in Articles 260ter or 305bis of the Swiss Criminal Code (CP), (2) derive from a qualified tax crime or misdemeanor, (3) are subject to the control of a criminal or terrorist organization, or (4) are used to finance terrorism (see *supra* N. 80 et seq.).

12 4 Conversely, in the absence of such a reference, a **match with a terrorist list** under Art. 9(1)(c) *in conjunction with* Art. 22*a*(2) and (3) of the Anti-Money Laundering Act (AMLA) does not fall within the scope of Art. 9(1(b) of the Anti-Money Laundering Act (see *infra* N. 138). This situation is considered unsatisfactory by legal scholars, who note that "*the only solution would be that, when faced with such a suspicion,* [the financial intermediary] *should not terminate the negotiations but should establish a business relationship in order to be able to make the report*." In our view, a report could nevertheless be based on Art. 9(1)(b) *in conjunction with* Art. 9(1)(a, subparagraphs 3 and/or 4 of the Anti-Money Laundering Act (AMLA) in such a scenario.

12 5 The requirement of a link to the offenses set forth above is important, as it implies that the financial intermediary's suspicion must not relate exclusively to the potential client as a person, but to the **assets** that the client intends to bring into the business relationship . In this regard, reference may be made to what has already been discussed in connection with Art. 9(1)(a) AMLA (see *supra* N. 75).

c. Threshold for Suspicion: Well-Founded Suspicion

Art. 9(1)^{quater} AMLA, which defines the concept of "**well-founded suspicion**," is also applicable in the context of Art. 9(1)(b) AMLA. Consequently, the threshold of suspicion triggering the reporting obligation under Art. 9(1)(b) AMLA is, in principle, the same as that under Art. 9(1)(a) AMLA, to which reference is made (see *supra* N. 101 et seq.). However, three specific features must be taken into account. 12 6

First, Art. 9(1)(b) of the Anti-Money Laundering Act does not mention the "**knowing**" variant; that is to say, strictly speaking, the provision does not cover the scenario where the financial intermediary is aware of the link between a criminal offense and the assets intended for the proposed business relationship. In our view, this constitutes a **true gap in the law**, as there is no indication that the legislature intended to exempt the financial intermediary from the reporting obligation in such a case, while subjecting them to such an obligation in the presence of reasonable suspicion. It must therefore be concluded that Art. 9(1)(b) of the Anti-Money Laundering Act (AMLA) applies, *a fortiori*, in cases where the financial intermediary has actual knowledge of a fact subject to reporting (see *supra* N. 100). 12 7

Second, the question arises as to whether **additional clarifications** are necessary for the suspicion to be deemed well-founded. One argument in favor of this view lies in the wording of Art. 9(1)^{quater} of the Anti-Money Laundering Act (AMLA), which also applies to Art. 9(1)(b) of the Anti-Money Laundering Act (AMLA) and requires the conduct of further due diligence. On the other hand, the Federal Council's Message on the extension of the reporting obligation to the negotiation phase is equally clear in the opposite direction, stating that "*requesting additional information could arouse the customer's suspicion." Therefore, in the event of a breakdown in negotiations aimed at establishing a business relationship, the financial intermediary is required to file a report only on the basis of the information available to it at the time of the breakdown. The extension of the reporting obligation does not impose any additional duty of clarification on the financial intermediary. Thus, the financial intermediary has no obligation to request additional information from the 'client' or to take specific investigative measures to substantiate its suspicions*." Legal scholarship concurs with the Federal Council's view. 12 8

12 9 However, several points warrant mention. On the one hand, the concept of "reasonable suspicion" was codified in Art. 9(1)^{quater} of the Anti-Money Laundering Act (AMLA) years after the publication of this Federal Council Message, the relevance of which is thus open to question. On the other hand, the concern regarding the risk of *tipping-off*, which underlies the position expressed by the Federal Council, is not specific to the case of Art. 9(1)(b) of the Anti-Money Laundering Act (AMLA), but obviously applies as well in the context of subparagraph (a). Thus, in our view, based on the wording of Art. 9(1)^{quater} of the Anti-Money Laundering Act, that conducting additional due diligence prior to a potential breakdown in negotiations **remains a condition** —in principle, a necessary one—for establishing a reasonable suspicion and thereby triggering the reporting obligation provided for in Art. 9(1)(b of the Anti-Money Laundering Act, with the scope and nature of the clarifications naturally having to be adapted to the circumstances of the specific case. However, this does not apply to situations involving obvious or immediately well-founded suspicions; when the financial intermediary knows, or has virtually no doubt, that the assets intended to be involved in the future business relationship are linked to a criminal offense, it should be able to dispense with further clarifications, particularly for reasons of expediency, as long as the quality of the communication's content is guaranteed (see *supra* N. 110 et seq.).

13 0 Third, unlike Art. 9(1)(a) of the Anti-Money Laundering Act (AMLA), the reporting obligation under Art. 9(1)(b) of the AMLA is not yet **triggered** by the mere existence of , but also requires that the financial intermediary terminate negotiations on the basis of such well-founded suspicions (see *infra* N. 131) . If, despite well-founded suspicions, negotiations are not terminated and the business relationship is established, the financial intermediary is not relieved of its reporting obligation; rather, the obligation must then be based on Art. 9(1)(a) of the Anti-Money Laundering Act (AMLA).

d. Triggering Event: Termination of Negotiations Due to Well-Founded Suspicions

13 1 The event that triggers the reporting obligation under Art. 9(1)(b) of the Anti-Money Laundering Act (AMLA) is the **termination of negotiations** aimed at establishing the business relationship business relationship due to well-founded suspicions.

The concept and temporal scope of **negotiations** have already been addressed in the context of the subject matter of the suspicion (see *supra* N. 121 et seq.). 13 2

The term "**termination**" must be understood in a broad sense. It includes the explicit or implicit expression of the intention to no longer wish to negotiate or enter into the contemplated business relationship. Any rejection by the financial intermediary of the customer or of the contemplated business relationship, regardless of its nature, must suffice. 13 3

Furthermore, the termination of negotiations must occur **due to reasonable suspicion**. If negotiations are terminated for other reasons or at the client's initiative, there is no obligation to report. The same applies if the financial intermediary only develops reasonable suspicion after the negotiations have been terminated for other reasons. 13 4

Once the report has been filed, the financial intermediary should not draw any conclusions in the event of **failure transmission** of the report by MROS to a criminal prosecution authority. Indeed, the absence of transmission does not necessarily mean that the proposed business relationship is risk-free and that negotiations should resume without further consideration. Furthermore, the financial intermediary is in no case informed by MROS of the status of its report after the termination of the business relationship (see Art. 23(5) AMLA). 13 5

3. Obligation in the Event of a Match with a Terrorist List (para. 1(c))

The reporting obligation set forth in Art. 9(1(c) of the Anti-Money Laundering Act (AMLA) differs from the scenarios covered by subsections (a) and (b) in that it **does not concern financial assets**, but rather the question of whether data regarding a contracting party, beneficial owner, or authorized signatory of a business relationship or transaction matches a terrorist list, with the threshold for suspicion based on the knowledge of the financial intermediary or on based on additional clarifications. 13 6

a. Subject of the suspicion: Information concerning a contracting party, beneficial owner, or signatory

Suspicion within the meaning of Art. 9(1)(c) of the Anti-Money Laundering Act (AMLA) relates to **information** concerning a **contracting party, beneficial** 13 7

owner, or authorized signatory of a business relationship or transaction. A link to financial assets is not required.

13 8 The concept of "**business relationship**" has already been discussed above (see *supra* N. 76). The concept of "**transaction**" generally covers any legal act in the context of financial transactions, such as acceptance, safekeeping, the investment, or the transfer of assets. To the extent that the reporting obligation in the event of a match with a terrorist list presupposes a business relationship or a transaction, it does not apply in the event of a breakdown in negotiations due to suspicions of such a match; it should be noted that Art. 9(1)(b) AMLA is also inapplicable, given its to the grounds set forth solely in Art. 9(1)(a) of the Anti-Money Laundering Act (AMLA) (see *supra* N. 124).

13 9 The **contracting party** is the formal counterparty to the contract, that is, the person with whom the financial intermediary establishes the business relationship or on whose behalf it executes the transaction. The **beneficial owner** is, according to case law, the natural or legal person who has the de facto ability to dispose of the assets and is therefore the person to whom these assets belong from an economic perspective. Only an economic analysis is relevant; formal legal constructs are of no significance. However, the concept of beneficial owner requires clarification in the context of a transaction: in accordance with the objective of preventing terrorist financing, it refers not only to the person who initially controlled the assets from from an economic standpoint, but also the person who acquires that economic control through the transaction. Finally, the **authorized signatory** of a business relationship is the person authorized to bind the contracting party to the financial intermediary, either as a corporate officer or as a representative. As a general rule, these persons must be known to the financial intermediary. Indeed, the Anti-Money Laundering Act (AMLA) requires the financial intermediary to verify the identity of the contracting party and to identify the beneficial owner with the diligence required by the circumstances (Art. 3–5 AMLA). Furthermore, the financial intermediary must determine who holds a lasting power of attorney over an account or a custody account (Art. 7(1) AMLA *in conjunction with* Art. 22 and Art. 39(1)(c) AML-FINMA).

14 0 The question of whether the obligation under Art. 9(1)(c) AMLA also applies to **former contracting parties, beneficial owners, and authorized signatories** has, to our knowledge, not yet been decided by the courts. A literal inter-

pretation of Art. 9(1)((c) of the Anti-Money Laundering Act (AMLA) suggests that the match with a terrorist list must be current. Furthermore, the case law of the Federal Supreme Court, which extends the reporting obligation under Art. 9(1)(a) of the AMLA to beyond the end of a business relationship (see *supra* N. 32 et seq.) does not seem relevant in this context, as it focuses on the continued existence of confiscable assets, whereas the assets involved in the business relationship are not decisive for the purposes of Art. 9(1)(c) of the Anti-Money Laundering Act. In fact, the financial intermediary must file a report pursuant to Art. 9(1)(c) of the Anti-Money Laundering Act (AMLA) regardless of any link between the assets and terrorist activities (see *supra* N. 137 and *infra* N. 141 et seq.).

b. Content of the Suspicion: Match with a Terrorist List

The **suspicion** concerns the match between data regarding the aforementioned persons and data relating to terrorist activities, transmitted to the financial intermediary pursuant to Art. 22*a*, para. 2 or 3, of the Anti-Money Laundering Act (AMLA). 14 1

The **relevant data** is based on an international notification system that is implemented in Swiss law by Art. 22*a* of the Anti-Money Laundering Act (AMLA). This refers to data "*communicated and published by another state concerning individuals and organizations that, in accordance with United Nations Security Council Resolution 1373 (2001), have been listed in that state as engaging in or supporting terrorist activities*" (Art. 22*a*, para. 1, AMLA). The Federal Department of Finance acts as the central recipient at the international level and then forwards the data—that is, the lists received from foreign states—to the supervisory authorities, namely FINMA, the Federal Gaming Board, the Intercantonal Gaming Supervisory Authority, and the Central Office for the Control of Precious Metals, which in turn forward them to the financial intermediaries under their supervision (Art. 22*a*, paras. 1 and 2, AMLA). For a list to be transmitted, first, another state must have provided it to Switzerland as part of a defined procedure or informally; the Swiss Confederation is not required to search for lists of terrorists and terrorist organizations worldwide. Second, only foreign lists that have already been published in their country of origin may be transmitted. Third, lists of terrorists and terrorist organizations provided to Switzerland by a foreign state may be transmitted only if they are based on United Nations Security Council Resolution 14 2

1373. Adopted in the wake of the September 11, 2001, attacks, this resolution also sets forth minimum requirements for the designation of terrorists or terrorist organizations . If a list has been transmitted to the financial intermediary in violation of these rules, there is, in principle, no reporting obligation under Art. 9(1)(c) of the Anti-Money Laundering Act (AMLA); however, such a list may certainly give rise to an initial suspicion under Art. 9(1)(a) of the AMLA.

14 3 A contracting party, beneficial owner, or authorized signatory **matches** the terrorist lists when they refer to the same person, bearing in mind that a suspicion of a match is sufficient (see *infra* N. 144).

c. Threshold for Suspicion and Triggering Event: Knowledge or Reasonable Suspicion

14 4 The reporting obligation under Art. 9(1)(c) of the AMLA is **triggered** if the financial intermediary "*knows or suspects, based on clarifications carried out pursuant to Art. 6(2(d) [AMLA]*" that the contracting party, beneficial owner, or authorized signatory appears on a terrorist list.

14 5 The concept of "**knowing**" is the same as that referred to in the context of Art. 9(1)(a) of the Anti-Money Laundering Act (AMLA). It presupposes that the financial intermediary has no doubt regarding the match (see *supra* N. 100).

14 6 Although the wording of Art. 9(1)(c) of the AMLA does not refer to reasonable suspicion but only to a presumption of a match, the requirement of **suspicion** corresponds in principle to this concept. Two reasons support this interpretation: on the first, the legal definition of "reasonable suspicion" contained in Art. 9(1)^{quater} of the Anti-Money Laundering Act (AMLA) refers—at least in the first part of the sentence—to paragraph 1 in its entirety and not solely to subparagraphs (a) and (b) of that paragraph. Second, this legal definition is based on the principle that reasonable suspicion exists whenever the indications cannot be dispelled by further clarifications carried out pursuant to Art. 6 of the Anti-Money Laundering Act (AMLA)—a principle that also appears in Art. 9(1)(c) of the AMLA, which refers to Art. 6(2)(d of the AMLA. Consequently, reference should be made to the explanations regarding the concept of "reasonable suspicion" set forth in the commentary on Art. 9, para. 1(a) of the Anti-Money Laundering Act (see *supra* N. 101 et seq.), subject to the following

clarifications, which, from a doctrinal perspective, concern initial indications and additional clarifications.

The first step toward the threshold of suspicion that triggers the reporting obligation is that the financial intermediary has**indications** suggesting a match within the meaning of Art. 9(1)(c) of the Anti-Money Laundering Act (AMLA), thereby requiring the financial intermediary to carry out the additional clarifications provided for in Art. 6(2)(d) of the AMLA. In this context, the question arises as to whether the financial intermediary is legally obligated to systematically compare the terrorist lists provided with its contracting parties, beneficial owners, and authorized signatories. While such an obligation certainly does not expressly arise from Art. 9(1)(c) of the Anti-Money Laundering Act (AMLA), this provision would be rendered meaningless and defeat its purpose if the financial intermediary were allowed to ignore the terrorist lists. From a teleological perspective, and in light of Art. 6(2(d) of the Anti-Money Laundering Act (AMLA), it is therefore necessary for the financial intermediary to regularly conduct a **systematic comparison**—at least a cursory one—between its databases and the lists in question. This comparison will most often reveal indications of a match with the terrorist lists. However, it cannot be entirely ruled out that indications of a match may arise in other ways. 14 7

The report cannot be based on just any indications. Rather, the financial intermediary is required to first conduct the **additional inquiries** provided for in Art. 6, para. 2, subpar. of the Anti-Money Laundering Act (AMLA). According to the Federal Council's Explanatory Memorandum, the purpose of this is to ensure that the financial intermediary is able to explain why it knows or suspects that the contracting party, beneficial owner, or authorized signatory actually corresponds to a listed terrorist person or organization. However, according to the Explanatory Memorandum, the report must be filed even if the financial intermediary is not absolutely certain that the person in question truly corresponds to the listed individual, as a partial match of the data may also give rise to a reasonable suspicion. This is the case, for example, when there are several different spellings for the same name. Similar to the legal definition of reasonable suspicion under Art. 9(1)^{quater} of the Anti-Money Laundering Act (AMLA), reporting is thus already required when further clarifications fail to dispel the suspicion of a match. However, while the cross-reference in Art. 9(1)(c) of the Anti-Money Laundering Act (AMLA) to Art. 6(2)(d) of the AMLA suggests that, in accordance with the introductory sentence of 14 8

the latter provision, the background and purpose of the transaction or business relationship should be clarified prior to reporting, this cannot be the intended meaning of the provision. Indeed, the reporting obligation is triggered by (reasonable) suspicions that personal data matches terrorist lists, and not by the background or purpose of the transaction or business relationship in the strict sense.

C. Consequence: Reporting Obligation and Parallel Obligations

14 When the conditions for the reporting obligation under Art. 9(1)(a, b, or c of
9 the Anti-Money Laundering Act (AMLA) are met, the financial intermediary must **immediately file a report with MROS**. The procedures for this reporting (see *below*, Chapter VI), its effects—particularly regarding the financial intermediary's parallel obligations (see *below*, Chapter VII)—and the consequences of non-compliance (see *below*, Chapter VIII) will be discussed in greater detail.

IV. REPORTING OBLIGATIONS OF TRADERS (PARA. 1BIS)

A. Applicable Parties: Dealers

15 Art. 9, para. 1bis of the AMLA establishes a reporting obligation corresponding
0 to that set forth in Article 9(1)(a) of the Anti-Money Laundering Act (AMLA), but directed at merchants. This term refers to natural or legal persons who, in the course of their business, **trade in goods and receive cash as payment** (Art. 2(1)(b) AMLA; see Art. 13 et seq. of the Anti-Money Laundering Ordinance (AMLO)). Furthermore, the personal scope of application of Art. 9 of the Anti-Money Laundering Act (AMLA) has been discussed above (see *supra* N. 19 et seq.).

B. Conditions

1. Preliminary Remarks: Limitation to Significant Trading Transactions

15 Before addressing the conditions expressly set forth in Art. 9, para. 1bis of the
1 AMLA, the central question arises regarding the **material scope of material scope of application** of the reporting obligation for traders. The question is whether this obligation applies to any trading transaction or only to significant trading transactions—that is, those involving more than 100,000 francs. The

various methods of interpretation lead to partly differing conclusions; legal scholarship is divided, and case law has not yet resolved the issue.

The **clear wording** of Art. 9(1)^{bis} of the Anti-Money Laundering Act (AMLA) does not allow for the inference of a restriction on the material scope of application. The text of the provision states—in general terms—that a dealer must file a report if it has reasonable suspicion that the cash used in a transaction is linked to a crime or misdemeanor. There is is not a matter of including only certain commercial transactions. Furthermore, the legal definition of a merchant imposes no restriction in this regard, as it covers any person who, in the course of their business, trades in goods and receives cash as payment (Art. 2, para. 1, let. b, AMLA). The term "transaction" is not defined by the AMLA. 15 2

Given the clear and unambiguous wording of the law, it may in principle be deviated from only if there are valid reasons to believe that this wording does does not reflect the true meaning of the provision. The question arises as to whether this interpretive rule should also apply in the context of dealers' reporting obligations. Admittedly, from a systematic perspective, it is difficult to reconcile the fact that dealers' due diligence obligations apply only to trading transactions exceeding 100,000 francs (Art. 8 (a)(1) AMLA), whereas the reporting obligation would apply to every transaction—especially since the triggering reasonable suspicions must, in principle, be based on additional inquiries conducted in accordance with the due diligence obligation (see Art. 20(1 in conjunction with Art. 19 AML Ordinance; see Art. 8a(2) AMLA and Art. 9(1sexies) New AMLA). This is, in fact, why MROS proposes applying the 100,000-franc threshold to Art. 9(1bis) AMLA. However, it should not be forgotten that these are two different mechanisms: the due diligence obligation is subject to a de minimis threshold—admittedly a very high one—which is based on a compromise between, in short, the fight against money laundering and economic freedom. By contrast, the reporting obligation applies only when there are indications suggesting that the means of payment are linked to certain offenses and thus require further clarification. Consequently, and particularly in light of the ratio legis—which is to identify acts of money laundering, prosecute offenses, and ultimately confiscate illicit assets—it is reasonable—when there is indeed evidence, even in connection with transactions below 100,000 francs—to require the merchant to seek further clarification and, if such clarification fails to dispel the doubts, to file a report. The risk of 15 3

money laundering also exists below this threshold. In any case, uncertainty remains, and it would be desirable for the legislature to quickly clarify the substantive scope of this obligation. Indeed, the preparatory works and subsequent official documents do not make it possible to discern a clear intent on the part of the legislature. De lege ferenda, it would be appropriate to establish a minimum threshold for dealers' reporting obligations as well, if only for practical reasons.

2. Subject of the Suspicion: Currency Used in a Trading Transaction

154 The suspicion triggering the reporting obligation of merchants concerns "**cash used in a commercial transaction**."

155 This wording—which is relatively clear, particularly when read in conjunction with Art. 2(1)(b) of the Anti-Money Laundering Act (AMLA)—nevertheless gives rise to two observations: first, the term "**cash**" refers to physical currency, regardless of the currency, as opposed to payments by bank transfer or card. The defining characteristic of cash is that its transfer generally leaves no *paper trail*, which increases the risk of money laundering. Although this objective might argue for extending the term to other means of payment, such as cryptocurrencies or precious metals, the wording of the provision hardly allows for this. On the other hand, cash must constitute the **consideration** that the merchant receives in connection with the sale of movable or immovable property (see Art. 15 OBA). Consequently, payment in exchange for services does not fall within the scope of Art. 9(1)^{bis} LBA.

3. Nature of the Suspicion: Link to Certain Crimes or Offenses

156 The merchant's suspicion that triggers the reporting obligation must relate to the existence of a link between the cash and certain crimes or offenses—in simple terms, the **illicit nature of the cash** used in the transaction. The alternative conditions listed in Article 9(1bis)(a) through (d) of the Anti-Money Laundering Act (AMLA) correspond word for word to those in Article 9(1)(a) of the AMLA. These include funds related to participation in or support for a criminal or terrorist organization or to money laundering; funds derived from a felony or a qualified tax offense; funds subject to the control of a criminal or terrorist organization; and, finally, funds used to finance terrorism (see *supra* N. 79 et seq.). Art. 20 of the Anti-Money Laundering Ordinance (OBA) groups these various alternative scenarios under the term "*criminal act*." However,

this term does not accurately reflect the law and cannot have any independent scope; in any event, it cannot either broaden or narrow the grounds for reporting. Art. 20(2) of the OBA further specifies that a report must also be made when the merchant cannot identify the specific offense ("*criminal act*") from which the cash payments originate. Nor does this provision appear to have independent legal effect, since it is already established that a suspicion need not relate to a specific crime. The fact that the merchant is expected to specify the offense they suspect in support of their report does not does not change this. Ultimately, the provision in Art. 20(2) OBA does not relieve the merchant of its obligations to investigate, nor does it lower the relevant threshold for suspicion.

Despite all the similarities between the reporting obligations of financial intermediaries and merchants, there are nevertheless certain differences. On the one hand, merchants are not required to report in the event of a break in negotiations or a match with a terrorist list (situations covered by Art. 9(1)(b) and (c) of the Anti-Money Laundering Act (AMLA)). On the other hand, there are certain contextual differences related to the transactional nature of the trading operation. Thus, the question is not whether cash within the meaning of Art. 9(1bis)(c) of the AMLA remains under the control of a criminal or terrorist organization after the transaction, but only whether that was the case prior to the transaction. Otherwise, the provision would be rendered meaningless, since it is the dealer who then exercises control over the funds. The scope of Art. 9(1bis)(d) of the Anti-Money Laundering Act (AMLA), which was adopted retroactively in response to a FATF assessment, is less clear; for while the cash is intended to compensate the dealer, it does not, in principle, not for the financing of terrorism. To give effect to this provision, it would have to be interpreted to mean that suspicions regarding the financing of terrorism may relate to the transaction in general; however, this appears to be contrary to the letter of the law. 15 7

4. Threshold for Suspicion and Triggering Event: Knowledge or Reasonable Suspicion

The reporting obligation is triggered if the merchant **knows or suspects, based on reasonable suspicion,** that the cash used in a transaction is linked to any of the offenses listed in paragraphs 1 through 4 above. In this regard, 15 8

reference may be made to the discussion regarding Art. 9(1)(a) of the Anti-Money Laundering Act (see *supra*, note 99 et seq.).

159 With regard to merchants, the concept of **reasonable suspicion** is further defined by Art. 20(1) OBA. This provision states that "[r]*easonable suspicion exists, triggering a reporting obligation within the meaning of Art. 9(1bis of the AMLA when the suspicions are based on a concrete indication or on several clues suggesting that the cash payments originate from a criminal act and that the additional clarifications referred to in Art. 19* [AML Ordinance] *do not dispel them* ." This wording is modeled on the definition contained in Art. 9, para. 1quater of the Anti-Money Laundering Act (AMLA) applicable to financial intermediaries. It has already been noted that the generic term "criminal act" in this legal definition is not consistent with Art. 9, para. 1bis of the AMLA (see *supra* N. 156).

160 As part of the revision of the Anti-Money Laundering Act (AMLA) adopted in September 2025, the federal legislature has, moreover, planned to **move the legal definition** of "reasonable suspicion" applicable to dealers **into the Act** (see Art. 9, para. 1sexies, new AMLA).

161 Under both current and new law, the existence of reasonable suspicion presupposes **two stages** (see *supra* N. 101 et seq.): first, there must be indications suggesting that the cash payments meet one of the conditions set forth in Art. 9, para. 1bis, subpar. a through d of the Anti-Money Laundering Act (AMLA). Such indications exist, pursuant to Art. 19(2) of the Anti-Money Laundering Ordinance (OBA), in particular when the person pays with banknotes of low face value, the transactions involve readily marketable goods, or the person provides insufficient or even false information. When a merchant is faced with such indications, they are required to conduct further inquiries regarding the context and purpose of the transaction. However, the existence of an indication does not mean that the merchant must immediately notify MROS. A report must be filed only when the additional clarifications do not dispel the initial suspicion.

C. Consequence: Reporting Obligation and Parallel Obligations

162 When the conditions of one of the scenarios set forth in Art. 9(1)bis(a) through (d) of the Anti-Money Laundering Act (AMLA) are met, the business operator must **immediately file a report with MROS**—just as a financial intermedi-

ary is required to do under Art. 9(1) of the AMLA (see *supra* N. 149). The procedures for this report (see *infra*, Chapter VI), its effects—particularly with regard to the trader's parallel obligations (see *below* Chapter VII), as well as the consequences of non-compliance (see *below* Chapter VIII).

V. REPORTING OBLIGATIONS OF ADVISORS (ART. 9 PARA. 1TER NAMLA)

A. Applicable Parties: Advisors

In September 2025, the Federal Parliament decided to extend the reporting obligation to the new category of **advisors**. The relevant provisions will take effect on October 1, 2026 (see supra N. 18). The term "advisor" refers to natural or legal persons who, in a professional capacity, participate on behalf of third parties in financial transactions—including the organization of funds—in connection with certain specifically listed legal transactions (notably the purchase or sale of real estate, the creation, management, or administration of non-operational legal entities, the organization of contributions to or distributions from such an entity, as well as the sale or purchase of entities through non-operational structures), as well as service providers who make available an address or premises serving as a domicile or registered office (Art. 2(1)(c) *in conjunction with* paras. 3bis and 3ter of the new AMLA). The term also covers employees who, on the basis of a public-law relationship, serve as public officials and who, in that capacity, participate in financial transactions, including the organization of funds in connection with the aforementioned legal transactions (Art. 2(1)(c) in conjunction with Art. 3quater nLBA). The nOBA contains several useful clarifications regarding the interpretation of the concept of "advisor" as defined by the nLBA (Art. 12d et seq. nOBA). In particular, it sets the thresholds above which advisory services are deemed to be provided on a professional basis (Art. 12f nOBA). 16 3

B. Conditions

The **conditions triggering the reporting obligation** for advisors are modeled on those applicable to financial intermediaries, with Art. 9(1)^{ter}(a) through (c) of the nLBA reproducing Art. 9(1) of the LBA almost verbatim. Thus, the advisor must file a report as soon as he knows or suspects, based on reasonable grounds, that the assets involved in the transaction or the provision of 16 4

services that he is preparing or executing are related to participation in or support of a criminal or terrorist organization or to money laundering; that they derive from a crime or a serious tax offense; that they are under the control of a criminal or terrorist organization, or that they are used to finance terrorism (Art. 9(1ter)(a)(1)–(4) nLBA). The obligation also applies when the advisor terminates negotiations due to such suspicions (Art. 9(1ter)(b) nLBA), as well as when the advisor determines, based on the in-depth due diligence conducted in cases of increased risk, a match between data relating to a listed person or organization within the meaning of the counterterrorism measures and that of a client, beneficial owner, or signatory (Art. 9, para. 1ter, subpar. c, nLBA). In principle, the reporting obligation for advisors is interpreted analogously to Art. 9, para. 1 and 1bis of the Anti-Money Laundering Act (AMLA), which apply to financial intermediaries and dealers; the relevant case law is therefore applicable *mutatis mutandis* (see *supra* N. 79 et seq.).

165 The concept of "**reasonable suspicion**" is the same as for financial intermediaries, since Art. 9 para. 1quater of the Anti-Money Laundering Act (or Art. 9 para. 1quinquies of the new Anti-Money Laundering Act) is expressly applicable by virtue of the reference in Art. 9(1sexies) of the new Anti-Money Laundering Act. The concept thus presupposes one or more indicators justifying the suspicion that cannot be dispelled by further clarification (see *supra* N. 101 et seq.).

C. Consequence: Reporting Obligation and Parallel Obligations

166 When the conditions for the reporting obligation under Art. 9(1ter)(a) through (d) of the New Anti-Money Laundering Act (nLBA) are met, the advisor must **immediately file a report with MROS**—just as a financial intermediary must under Art. 9(1) of the Anti-Money Laundering Act (see *supra* N. 149).

VI. REPORTING PROCEDURES

A. Responsibilities and Obligations Within the Financial Intermediary, Dealer, or Advisor

167 The reporting obligation generally rests with the financial intermediary, dealer, and advisor, as defined (or to be defined) in Art. 2 of the Anti-Money Laundering Act (AMLA), whether they are **natural or legal persons**.

Within a company, the reporting obligation rests more specifically with the persons designated for this function by law or by internal guidelines. 168

With regard to **designation by law**, this concept should be understood as a reference to the law in the substantive sense, including, in particular, the ordinances on money laundering. 169

For financial intermediaries subject to the **OBA -FINMA**, the ordinance provides that the highest level of management decides whether to make reports pursuant to Art. 9 AMLA (or pursuant to Art. 305ter, para. 2, of the Swiss Criminal Code), but that it may delegate this task to one or more of its members who do not have direct responsibility for the business relationship, to the specialized anti-money laundering unit, or to a largely independent unit (Art. 25*a* AMLA-FINMA). Before addressing the group of individuals to whom decision-making authority regarding reporting may be delegated, a general observation regarding this provision is in order: its purpose, in addition to assigning reporting authority to a high level of management, is to**avoid conflicts of interest** when deciding whether or not to report suspicions, such as those that may arise, for example, when a member of management personally manages client relationships subject to reporting requirements. This is an important and legitimate concern, which raises the question of whether measures to prevent conflicts of interest should also be taken at the management level. However, such an obligation cannot be directly inferred from Art. 25*a* OBA-FINMA, contrary to what some authors assert. 170

With regard to those **to whom authority to make decisions** regarding reporting has been delegated, Art. 25*a* OBA-FINMA provides, as mentioned above, that the delegation may be made to one or more members of management who do who are not directly responsible for the business relationship, or to the specialized anti-money laundering unit pursuant to Articles 24 and 25 of the OBA-FINMA. Finally, the delegation may also be made to a largely independent unit, which presupposes that the majority of its members do not engage in profit-generating activities. It may also involve a single individual; in practice, this is generally referred to as the *Money Laundering Reporting Officer* (“**MLRO**”), a role often filled by the *Head of Compliance* or the General Counsel. It is even conceivable to interpret “independent unit” as referring to external third parties. 171

17 2 Furthermore, once the decision to file a report has been made, to **delegate the execution of the report** to a lower-ranking employee or to an external third party who is properly trained and supervised.

17 3 The precise allocation of responsibilities under Art. 25a OBA-FINMA, in particular the delegation of decision-making authority and the execution of a disclosure, must be set forth in the financial intermediary's internal guidelines (see Art. 26(2)(g) OBA -FINMA). The principles set forth below apply mutatis mutandis (see infra N. 175).

17 4 For the sake of completeness, it should also be noted that Art. 49 and Art. 50(2)(g) of the **OBA-OFDF** contain equivalent rules applicable to trading in bank precious metals, while the**OBA -FDJP** on large-scale gaming operators merely refers to internal guidelines (see Art. 24(2(g) OBA-DFJP). The **OBA-CFMJ** does not explicitly address internal competencies.

17 5 As mentioned above, competencies regarding the reporting obligation may also arise from **internal guidelines or regulations**, which is, in fact, very common in practice. Generally speaking, the criteria on which such regulations must be based are as follows: the absolute priority is strict compliance with legal requirements, that is, ensuring that reports are submitted to MROS in a complete and timely manner as soon as the conditions are met. In other words, the regulations must ensure the quality and speed not only of the decision to report but also of the execution of the report. With regard to decision-making, the internal regulations must, in accordance with Art. 25*a* OBA-FINMA, prevent conflicts of interest, particularly when a person called upon to decide on the appropriateness of a report is involved in the business relationship in question. Furthermore, while collegial decision-making may *a priori* offer a better guarantee of legal compliance, when the composition of the collegial body is appropriate and the required expertise is present, it inherently carries a risk of delay, *all the more so* given the applicable quorum or voting rules. Furthermore, members of the collegial body may rely on one another and consequently feel less personally invested in the matter of reporting to MROS, sometimes underestimating the responsibility that may be involved (see *below* N. 176 et seq.). Conversely, a decision made by a single person specifically designated for this purpose within the company promotes speed but is truly effective only if independence and expertise are ensured. In the latter case in particular, care must be taken to ensure that the decision-maker

holds an appropriate position within the company's hierarchy, so as to be able to resist attempts at pressure or obstruction.

The issue of decision-making authority regarding reporting within a company subject to the AMLA is central, particularly from a criminal law perspective. According to a standard recitation of the Federal Criminal Court, the circle of potential perpetrators of a violation of Art. 37 of the Anti-Money Laundering Act (AMLA) include, among others, the person responsible for making the report in accordance with the institution's internal regulations, the external person appointed for this purpose, the bodies responsible for establishing rules governing the training and supervision of the department responsible for reporting, as well as the bodies and employees tasked with training that department. This group is very broad and is often criticized in legal scholarship for its abstract nature. 17 6

As mentioned above, the general rule is that the reporting obligation rests with the persons designated for this function by law or by internal regulations. From the perspective of potential criminal liability, it is irrelevant that the designated responsible persons must, in accordance with internal regulations, involve other bodies or functions in an advisory capacity before deciding to file a report with MROS. Furthermore, it has already been ruled that a **customer advisor** who is aware of circumstances requiring a report but who, contrary to the obligations set forth in internal regulations, fails to report them to the person responsible for deciding whether to file a report with MROS, is also subject to criminal liability under Article 37 of the Anti-Money Laundering Act (AMLA). According to the Criminal Division of the Federal Criminal Court, the same applies to **employees or bodies responsible for** preventing and combating money laundering, even if, under the internal division of responsibilities, they are not themselves responsible for reporting to MROS. Finally, when, according to internal guidelines, decision-making authority regarding reporting does not rest with a single person (typically the MLRO) but lies with a **collegial body**, each individual member of such a body assumes the role of a guarantor, which entails an independent obligation to work toward making a report, if necessary by proposing that the matter be put to a vote within the body. Therefore, in the event of a delayed or omitted report, the individual member may be subject to criminal prosecution under Art. 37 of the Anti-Money Laundering Act (AMLA). 17 7

B. Recipient of the Report

17 8 It follows from Art. 9 of the Anti-Money Laundering Act (AMLA) that the report must be addressed to the **MROS** (*Money Laundering Reporting Office Switzerland*), c' that is, the Money Laundering Reporting Office within the meaning of Art. 23 AMLA. The MROS plays a **pivotal** role between those subject to the reporting obligation and the criminal prosecution authorities: the MROS verifies and analyzes the information reported to it, requests additional information as needed, and immediately refers the case to the competent criminal prosecution authority if there are reasonable grounds for suspicion (see Art. 23, paras. 2 and 4, AMLA; see *infra* N. 195 et seq.). Thus, the tasks assigned to MROS as the national financial intelligence unit within the anti-money laundering system are designed to prevent criminal prosecution authorities from being overwhelmed by reports lacking sufficient grounds, to ensure specialized screening and preliminary review in order to identify genuinely suspicious cases, as well as to highlight connections between different pieces of information that would be overlooked in a decentralized process, and to gain an overview of money laundering methods and trends, thereby providing high-quality information to financial intermediaries, supervisory bodies, and law enforcement authorities.

17 9 The obligation to report within the meaning of Art. 9 AMLA is thus **not fulfilled** when MROS is "bypassed" and suspicions are reported directly and exclusively to law enforcement authorities, the self-regulatory body, or foreign authorities. Such practices also entail concrete criminal risks, particularly in connection with the violation of banking secrecy (Art. 47 BA) or, potentially, in cases involving foreign elements that could justify the jurisdiction of foreign criminal authorities, offenses against state sovereignty (Art. 271 and 273 of the Swiss Criminal Code, in particular).

18 0 Furthermore, MROS can only accept and process reports of suspicion if they fall within its jurisdiction due to the **principle of specialty**. Thus, MROS is not able to accept reports from natural or legal persons not subject to the Anti-Money Laundering Act (AMLA) (or the Proceeds of Crime Act), such as private individuals. The same applies to dealers regarding payments other than in cash. The latter are required to report their suspicions directly to the criminal prosecution authorities.

C. Form and Content of the Report

With regard to **form**, Art. 3a(3) of the OBCBA provides that reports to MROS must be submitted either through the **goAML** information system, or via the form provided by MROS, available on its website. GoAML is an electronic information system developed by the UN and implemented in 2020 by MROS, which enables the digital submission of suspicious activity reports via a secure portal, electronic transmission to the competent authorities, and the standardization of data formats. Although the OBCBA does not (yet) require the use of the goAML system, Fedpol has been encouraging its use for several years. In this spirit, the Federal Parliament decided, as part of the AMLA revision enacted in September 2025, to introduce Art. 23(7) of the new AMLA, according to which the exchange of information with MROS will henceforth take place exclusively via goAML. The option to submit a report on paper will therefore be eliminated as of October 1, 2026, the date on which the AMLA revision takes effect (see supra N. 18). 18 1

The **content** of reports to MROS is defined in detail in Art. 3(1) and (2) of the Anti-Money Laundering Ordinance (OBCBA), depending on the submitter (see also Art. 3*a*(4) OBCBA). In the case of financial intermediaries, the report must state the identity of the submitter and provide a means of direct contact with the responsible person, as well as the identification of the competent supervisory authority. It must also include the client's identification data (within the meaning Article 3 of the Anti-Money Laundering Act (AMLA)) and of the beneficial owner (as defined in Article 4 of the AMLA), the identification of other persons authorized to sign or represent the entity, a list of the assets in question (including the current account balance), and a precise description of the business relationship, its purpose, and its objective, along with references to account opening. Above all, the report must set forth as precisely as possible the suspicions underlying it and document these with account statements, supporting documents detailing the suspicious transactions, any links to other business relationships, as well as the results of the internal investigations conducted in accordance with Art. 6 of the Anti-Money Laundering Act (AMLA). 18 2

With regard to the level of detail, the report must be **as comprehensive as possible** to enable MROS to conduct the analysis required under Art. 23(2) and (4) of the AMLA. Furthermore, a financial intermediary or dealer who submits an incomplete report risks not being released from its reporting obligation and, consequently, may be held criminally liable under Art. 37 of the 18 3

AMLA (see *infra* N. 211 et seq.). However, given in particular the MROS's authority under Art. 11*a* of the Anti-Money Laundering Act (AMLA) to obtain additional information from the financial intermediary that submitted the report, **restraint** should be exercised before concluding that an incomplete report is deemed not to have been filed. This should only be the case if the report was, clearly not been made with due diligence or if the information transmitted to MROS is so incomplete that MROS is absolutely unable to fulfill its legal mandate (see *infra* N. 195 et seq.).

18 4 For reports from **dealers**, a similar core set of information is required, though adapted to their status (see Art. 3(2) OBCBA).

18 5 In principle, the same will apply to advisors, in accordance with the proposed amendments to the OBCBA (see Art. 3(2bis) and (2ter) nOBCBA) set forth in the annex to the nOTPM.

18 6 While the OBCBA specifies what information must be included in a report, the names of the intermediary's financial intermediary or dealer handling the case need **not be mentioned**, provided that MROS and the criminal prosecution authority retain the ability to contact them promptly (Art. 9, para. 1ter, AMLA). This provision was introduced by Parliament to protect employees from potential retaliatory measures by the person who is the subject of the report.

18 7 In its report on so-called **"negative typologies"** published in 2025, MROS laments a decline in the quality of certain reports, characterized by cases that are insufficiently substantiated, poorly documented, or of no real relevance to the fight against money laundering. MROS observes that, in many cases, the facts are only briefly clarified, or it remains unclear whether the additional clarifications required by Art. 6 of the Anti-Money Laundering Act (AMLA) have been provided. This trend is accompanied by a phenomenon known as "defensive reporting" (*defensive reporting*); financial intermediaries are submitting reports prematurely to protect themselves against criminal or administrative liability, rather than reporting on the basis of well-founded suspicions following further clarification. As justified as these observations may be, and as important as the quality of reports is to the fight against money laundering , the observed behavior of entities subject to the AMLA is is nonetheless understandable, as they face substantial criminal and/or prudential sanctions in the event of failure to report or delayed reporting. Added to this is the fact

that the threshold of suspicion triggering the reporting obligation has been lowered, first by case law and then by the legislature (see Art. 9(1)^{quater} AMLA). In this context, it is hardly surprising that entities subject to the AMLA may tend to file reports hastily.

D. Timing of the Report

Art. 9, para. 1 and para. 1bis of the AMLA provides that the report must be filed "**immediately**," without further specification. It is useful to distinguish between two aspects of this concept of immediacy, namely, on the one hand, the point in time at which the reporting obligation is triggered and, on the other hand, the time limit for preparing and submitting the report to MROS. 188

With regard to the **point in time that triggers the obligation** to report, this has already been addressed above in connection with the various scenarios set forth in Art. 9 AMLA. With the exception of the case provided for in Art. 9(1)(b) of the Anti-Money Laundering Act (AMLA), where the obligation is triggered by the termination of negotiations to establish a business relationship due to reasonable suspicion (see *supra*, N. 131), the reporting obligation generally arises as soon as the threshold of "reasonable suspicion" is reached (see *supra*, N. 99, 144, and 158). It should be noted that the legal definition of "reasonable suspicion" requires not only the presence of evidence suggesting a link to a criminal offense but also that the additional inquiries conducted have failed to dispel the suspicion (Art. 9(1)^{quater} AMLA; see *supra* N. 104). Consequently, the reporting obligation does not arise as soon as the first doubts appear, but only after clarifications have been carried out to the extent that is reasonable and necessary. 189

In principle, persons subject to the AMLA must immediately undertake **additional clarifications** pursuant to Art. 6(2) AMLA and complete them as quickly as possible, as soon as they have a concrete indication or several clues suggesting that the criteria set forth in Art. 9 AMLA might be met (see Art. 9(1^{quater}) AMLA). The scope of the inquiries depends on the specific circumstances. As explained above, the financial intermediary must act with due diligence and, at a minimum, conduct the inquiries necessary to dispel the initial suspicion. Once these clarifications have been carried out, if the suspicion(s) cannot be dispelled, a report must be filed immediately (see *supra* N. 106 et seq.). 190

19 1 According to case law, a delay in the clarification process is not a valid reason to postpone filing a report. In practice, the Federal Department of Finance (FDF) generally holds that the financial intermediary has a **60-day period** to conduct clarifications—that is, to fully dispel the suspicions that have arisen—failing which it must proceed with the report. This practice stems from an earlier decision by the Swiss Federal Banking Commission (SFBC), which had held that clarifying unusual transactions some 60 days after their by a computerized transaction monitoring system was excessive. The SFBC's decision therefore does not have the scope attributed to it by the FDF. Furthermore, this decision contains no explicit rationale justifying the choice of a 60-day deadline. It should also be noted that this time frame was not incorporated into either the AMLA or the OBA-FINMA. In any event, the 60-day deadline can, in our view, only be understood as an **absolute limit** on the time available to conduct in-depth investigations. Under no circumstances should it be interpreted as a "standard" or automatically applicable deadline.

19 2 It is also worth noting that when a financial intermediary is aware of the criminal origin of the assets or has a **well-founded suspicion from the outset** (for example, upon learning from a reliable source that the client is the subject of criminal proceedings related to the assets in question), the reporting obligation must (exceptionally) be fulfilled immediately, without first conducting further clarifications, provided that the available information ensures the quality of the report (see *supra* N. 110 et seq.).

19 3 As soon as the reporting obligation is triggered, the report must be filed immediately. What this means in practice depends on the specific case. Admittedly, case law suggests—not as a general rule, but in specific cases—that a person subject to the AMLA may be required to file a report on the very day the suspicion became well-founded within the meaning of Art. 9(1^{quater}) of the Anti-Money Laundering Act (AMLA). However, this should apply only in exceptional cases, since from a purely practical standpoint, sufficient **time must be allowed to decide on the principle of the report and then to prepare and submit the report to MROS**. If a well-founded suspicion exists, but it is reported to MROS only incompletely or imprecisely due to a lack of time, then all additional clarifications will have been in vain and the objective of the AMLA will not have been achieved. It should be noted that, according to MROS, "[r]*eports of suspicion* [...] *must meet certain substantive standards so that MROS can process them effectively. Incomplete or unclear facts compli-*

cate or even prevent analysis. Such reports of suspicion clog the reporting system and tie up unnecessary resources at MROS. They have a detrimental effect on the efficiency of report processing and weaken the anti-money laundering framework as a whole ".

Consequently, the concept of immediacy must be interpreted teleologically, meaning that the person subject to the AMLA has, between the time a well-founded suspicion arises and the time the report is submitted to MROS, the time necessary—within the framework of sound internal organization and diligent conduct—to decide to file a report, to prepare it thoroughly, including all supporting documents required by law, and then to transmit it to MROS via a secure and rapid channel . As a general rule, **a few days** will suffice, given that the person subject to the AMLA can rely directly on the results of the additional clarifications carried out and that the goAML information system allows for immediate electronic transmission. 19 4

VII. EFFECTS OF THE REPORT AND RELATED OBLIGATIONS

A. MROS Procedure

Once **MROS has received a suspicious activity report**, it verifies and analyzes the information provided, requests additional information as needed, and immediately refers the case to the competent criminal prosecution authority if there are reasonable grounds for suspicion (see Art. 23, paras. 2 and 4, AMLA). 19 5

During its **analysis phase analysis phase**, MROS reviews the reports and conducts further investigations (see Art. 1, para. 2, letters a and b, OBCBA). To carry out its duties, it may obtain information pursuant to the Federal Act on Central Criminal Police Offices (Art. 6 OBCBA). It is also authorized to request from authorities, agencies, supervisory bodies, and self-regulatory organizations any relevant information, in particular to verify the existence of criminal or administrative proceedings, police records regarding individuals or companies, residency and business activities in Switzerland, as well as whether the financial intermediary is effectively subject to the relevant oversight (Art. 7 OBCBA). At the same time, pursuant to Art. 11*a* of the Anti-Money Laundering Act (LBA), the financial intermediary that filed the report and, 19 6

where applicable, other intermediaries involved in the transaction or business relationship must provide MROS, upon request and within the timeframe it specifies, with all available information necessary to assess the suspicions.

19 7 Upon completion of the analysis of the information, **MROS immediately reports** the case to the competent criminal prosecution authority when there are reasonable grounds to suspect that an offense within the meaning of Articles 260ter, 305bis, or 305ter, paragraph 1, of the Swiss Criminal Code (CP) has been committed, or that assets derive from a crime or an aggravated tax offense, are under the control of a criminal or terrorist organization, or are used to finance terrorism (Art. 23(4) of the Anti-Money Laundering Act (AMLA)). It is the responsibility of MROS not only to decide whether information is to be forwarded, but also which information (Art. 1(2)(c) of the OBCBA). The relevant information and MROS's assessment thereof are forwarded to the public prosecutors' offices in the form of electronic reports. These reports must not contain any information regarding the author of the report or the person who provided the information (Art. 8(1) OBCBA; see also Art. 9(1ter) Anti-Money Laundering Act). At the same time, MROS informs the financial intermediary (or advisor) that it is forwarding the information reported pursuant to Art. 9(1)(a) Anti-Money Laundering Act to a criminal prosecution authority (see Art. 23(5) of the new Anti-Money Laundering Act and Art. 9(1) of the OBCBA).

19 8 Furthermore, when MROS determines that a financial intermediary (or advisor) has failed to comply with its obligations in cases of suspected money laundering, it may **spontaneously notify the competent supervisory authority**, the competent supervisory body or the self-regulatory body (Art. 10(2) of the new OBCBA). In theory, it would even be conceivable for MROS to file a criminal complaint with the FDF on suspicion of a violation of Art. 37 AMLA (see Art. 301(1) CCP). However, we are not aware of any such instances having occurred.

B. Parallel Obligations

19 9 The AMLA and its ordinances contain **various obligations** parallel to the obligation to report, the primary purpose of which is to prevent "*tipping off*" and to preserve assets for possible subsequent forfeiture. Most of these obligations apply to financial intermediaries and take effect once the report has been filed with MROS.

Under Art. 10*a*, paras. 1 and 5, of the Anti-Money Laundering Act (AMLA), financial intermediaries—and dealers—are prohibited **from from informing** the persons concerned and third parties that they have filed a report. The Anti-Money Laundering Act (AMLA) provides for several exceptions to this rule for financial intermediaries, particularly regarding reporting to their supervisory authorities, other financial intermediaries (if necessary to comply with obligations under the AMLA), and their parent company abroad (under the conditions set forth in Art. 4^{quinquies} LB; see Art. 10*a*, paras. 1–3bis LBA). Furthermore, the prohibition on disclosure does not apply when the purpose is to safeguard one's own interests in the context of civil, criminal, or administrative proceedings (Art. 10*a*, para. 6 LBA). 20 0

The financial intermediary is also subject to the **prohibition on terminating the business relationship** when the conditions for reporting are met (Art. 12*a*, para. 1, OBA). This prohibition therefore applies even before the report is submitted to MROS, during the (short) period of preparation for the report. Furthermore, it follows from the wording of Art. 12*a*, para. 1, OBA ("*when the conditions for a report are met*") that the financial intermediary may not terminate a business relationship for the purpose of evading or delaying a report to MROS. In other words, the prohibition applies even if the financial intermediary refrains from reporting or delays in doing so. 20 1

That said, if MROS does not notify the financial intermediary that it is forwarding the reported information to a criminal prosecution authority within 40 business days following a report within the meaning of Art. 9(1)(a) of the Anti-Money Laundering Act (AMLA), the financial intermediary **may terminate** the business relationship (Art. 9*b*(1) AMLA). This also applies in the additional cases specified in Art. 12*b*(1) AMLO. If the financial intermediary terminates the business relationship after this deadline, this fact, along with the date on which the termination occurred, must be reported to MROS (Art. 9*b*(3) AMLA; Art. 12*b*, para. 3, OBA). Furthermore, the financial intermediary may authorize the withdrawal of significant assets only in a form that allows law enforcement authorities to trace them (Art. 9*b*, para. 2, AMLA; see also Art. 12*a*, para. 2, let. b, and 12b, para. 2, OBA). The prohibition on disclosure also continues to apply even after the business relationship has been terminated (Art. 9*b*(4) AMLA). 20 2

It should be noted that Art. 12*a*(1) AMRO does not preclude the business relationship from being terminated **at the client's initiative**. This follows *a con-* 20 3

trario from the wording " on his own initiative" in Art. 12*a*(1) OBA and from the distinction the law makes between the prohibition on terminating the business relationship and the obligation to freeze funds.

20 4 During the analysis conducted by MROS, the financial intermediary must **continue to execute orders** from clients relating to assets reported pursuant to Art. 9(1)(a) of the Anti-Money Laundering Act (AMLA) (see Art. 9a(1) of the AMLA) . The purpose of this provision is to prevent the client from being indirectly alerted that a report has been filed with MROS. However, the objective of discretion sought by this provision is not absolute, as the financial intermediary may execute client orders involving significant assets only in a manner that allows law enforcement authorities to trace them (Art. 9*a*, para. 2, AMLA). If this condition is not met, the financial intermediary will have no choice but to refuse to execute the client's instructions, which could alert the client to the possibility that a report has been filed with MROS.

20 5 From the perspective of supervisory law, a financial intermediary subject to the OBA-FINMA must also **notify FINMA or the supervisory authority** of any reports filed when they concern business relationships involving significant assets. In particular, the financial intermediary must provide such notification when there is reason to believe, given the circumstances, that the matter giving rise to the report will have consequences for the reputation of the financial intermediary or the financial center (Art. 22*a*, para. 1, OBA-FINMA). It should be noted that certain self-regulatory organizations (SROs) require their members to inform them immediately of any report filed.

20 6 A key rule for ensuring the eventual forfeiture of assets linked to money laundering is the **freezing of assets**. Indeed, as soon as MROS notifies the financial intermediary that it is forwarding the information to a criminal prosecution authority, the financial intermediary must freeze the assets entrusted to it that are linked to the information reported pursuant to pursuant to Art. 9(1)(a) of the Anti-Money Laundering Act (AMLA) (Art. 10(1) AMLA). By contrast, assets entrusted to the financial intermediary that are linked to information reported pursuant to Art. 9(1)(c) of the AMLA—that that is, a match with a terrorist list, must be frozen immediately upon notification to MROS (Art. 10(1)^{bis} AMLA). The freeze on the assets must remain in effect until a decision is received from the competent criminal prosecution authority, but for no more than five business days from the time MROS notifies the financial intermediary that it has forwarded the information to a criminal prosecution authority

in the case of Art. 9(1)(a) of the Anti-Money Laundering Act (AMLA), or from the time the financial intermediary has informed MROS in the case of Art. 9(1)(c) of the AMLA (Art. 10(2) of the AMLA).

In addition, the sector-specific ordinances require persons subject to them to **retain a copy of the reports** filed (Art. 74(1)(f) OBA-FINMA; Art. 23(1(f) OBA-DFJP; Art. 45(1)(f) OBA-OFDF; see Art. 21(2)(g) OBA-CFMJ). 207

It is also worth noting the**obligation to provide additional information to MROS**. On the one hand, Art. 11*a*(1 of the Anti-Money Laundering Act (AMLA) provides that the financial intermediary that filed the report must provide MROS, upon request and within the timeframe set by MROS, with all available information necessary for the assessment of the suspicions. On the other hand, the question arises as to whether the financial intermediary (or any other person subject to the AMLA) is required to voluntarily submit new information to MROS without a prior request. In the absence of a clear legal basis basis, the answer must be in the negative. However, the financial intermediary is, in principle, free to send MROS information related to a report that has already been submitted. If the initial report has been processed by MROS and MROS has already informed the financial intermediary of its decision, MROS considers that any information or document submitted constitutes a new report, for which the financial intermediary must conduct an in-depth analysis and provide the usual attachments; a simple reference to the initial report is not sufficient. Conversely, if MROS has not yet completed its review of the initial report and the new information concerns exactly the same individuals and the same set of facts, MROS does not consider this to be MROS, this does not constitute a new report. MROS treats this information as a supplement to the initial report, in which case a simple reference to the latter is sufficient. Finally, if the new information does not concern the same facts or the same individuals, but is related to the initial report, it must be the subject of a new report; a reference to the previous report seems appropriate in this case. 208

C. Exclusion of Liability in the Case of Reports Made in Good Faith

A report to MROS fundamentally conflicts with the obligations of loyalty and confidentiality that a person subject to the Anti-Money Laundering Act (AMLA) owes to their client. Furthermore, even if the suspicions reported to 209

MROS are later found to be unfounded, the report may require the client concerned to take costly steps and may cause the client losses, particularly due to financial transactions the client was unable to carry out or due to the inconvenience suffered as a result of the criminal proceedings initiated following the report. This raises the question of potential civil claims against the person subject subject to the Anti-Money Laundering Act (AMLA). To prevent these risks from influencing their decision regarding a potential report, Art. 11(1) AMLA provides for **an exemption from criminal and civil liability**. More specifically, according to Art. 11(1) AMLA, anyone who makes a report in good faith may not be prosecuted for breach of official secrecy, professional secrecy, or business secrecy, nor held liable for breach of contract.

VIII. CONSEQUENCES OF A BREACH OF THE REPORTING OBLIGATION

210 A **breach of the reporting obligation** entails various consequences, both administrative and/or criminal.

211 From a theoretical perspective, three main scenarios may constitute a violation of Art. 9 of the Anti-Money Laundering Act (AMLA). First, if the report is **not made at all**, even though the required conditions are met. Second, a **late report** may also constitute a violation of Art. 9 of the Anti-Money Laundering Act (AMLA), bearing in mind that the report must be made immediately according to the wording of the provision. Third, Art. 9 AMLA is also violated in the event of a **report that is (manifestly) incomplete or does not comply with the prescribed form**. It has already been noted above that this scenario should be applied only with restraint (see *supra* N. 183) .

212 These three scenarios may first and foremost be subject to criminal penalties. Article 37 of the Anti-Money Laundering Act (AMLA) imposes a fine of up to 500,000 francs on anyone who intentionally violates the reporting obligation and a fine of 150,000 francs in the case of a negligent violation. This constitutes a in its purest form, which can only be committed by a person subject to Art. 9 of the Anti-Money Laundering Act (AMLA). Pursuant to Art. 6 DPA, criminal liability within a company lies with the natural persons who acted (para. 1) or with their superiors (para. 2) (see supra N. 167 et seq.). The company may be held liable under the subsidiary liability provisions of Art. 49 of the Financial Market Supervision Act (LFINMA).213 On the administrative or pru-

dential level as well, several consequences may result from non-compliance with Art. 9 of the Anti-Money Laundering Act (AMLA). For example, FINMA may order the restoration of compliance with the law (Art. 31 of the FINMA Act) or issue a decision finding a serious violation, as well as carry out enforcement by substitution (Art. 32 FINMA Act). If FINMA finds a serious violation of supervisory law, it may prohibit the perpetrator from holding a management position in a regulated institution (Art. 33 FINMA Act; see Art. 9(2) AML-FINMA -FINMA), as a violation of anti-money laundering rules may call into question the guarantee of sound business practices required of the financial intermediary (Art. 9(1) AML-FINMA). FINMA may also prohibit the person from engaging in trading in financial instruments or providing client advisory services (Art. 33a FINMA Act). In addition, it may resort to naming and shaming (Art. 34 FINMA Act) and confiscate the proceeds acquired by a regulated entity or a person holding a management position who has seriously violated supervisory law (Art. 35 FINMA Act; see Art. 9(2) OBA-FINMA). Finally, it may revoke a regulated entity's operating license, recognition, authorization, or registration if the entity no longer meets the required conditions or if it seriously violates supervisory law (Art. 37 FINMA Act).

BIBLIOGRAPHY

Baumann Florian, Commentaire de l'art. 70/71 CP, in: Niggli Marcel/Wiprächtiger Hans (édit.), Basler Kommentar Strafrecht, Bâle 2019

Borsodi Benjamin/Goumaz Charles, Défaut de vigilance en matière d'opérations financières et droit de communication (art. 305ter CP), in: Mazou Miriam/Jeanneret Yvan (édit.), Le procès pénal, Bâle 2025

Cassani Ursula, Evolutions législatives récentes en matière de droit pénal économique: blanchiment d'argent et corruption privée, ZStrR 2018 p. 179

Cassani Ursula/Villard Katia, Commentaire de l'art. 305bis CP, in: Macaluso Alain/Moreillon Laurent/Queloz Nicolas (édit.), Commentaire romand – Code pénal II, 2 éd., Bâle, 2025

Cassani Ursula/Villard Katia, Droit pénal économique. Eléments de droit suisse et transnational, 2e éd., Bâle 2025 (cit. Droit pénal économique)

Chappuis Benoît, Avis de droit à l'intention du Département fédéral des finances sur le projet de loi sur la transparence des personnes morales et l'iden-

tification des ayants droit économiques (LTPM) et les modifications de la LBA sous l'angle du secret professionnel de l'avocat, 23 avril 2024 (cit. Avis de droit)

Chappuis Benoît/Burgener Fabio, Commentaire de l'art. 2 LBA, in: Cassani Ursula/Bovet Christian/Villard Katia (édit.), Commentaire romand – Loi sur le blanchiment d'argent, Bâle 2022

- Commentaire de l'art. 8a LBA, in: Cassani Ursula/Bovet Christian/Villard Katia (édit.), Commentaire romand – Loi sur le blanchiment d'argent, Bâle 2022

Chappuis Benoît/Gurtner Jérôme, La profession d'avocat, Zurich 2021

De Capitani Werner, Kommentar zu Art. 9 GwG, in: Niklaus Schmid (édit.), Kommentar Einziehung, Organisiertes Verbrechen, Geldwäscherei, t. II, Zurich 2002

Delnon Vera/Hubacher Marc, Geldwäscherei und Teilkontamination, ZStR 3/2016, p. 326

Egger Tanner Christine, Die strafrechtliche Erfassung der Geldwäscherei: ein Rechtsvergleich zwischen der Schweiz und der Bundesrepublik Deutschland, Zürich 1999

Fellmann Jeremias, Meldepflicht und Schweigerecht, Banken, Art. 9 Abs. 1 GwG und «nemo tenetur», in: Magister, Editions Weblaw, Bern 2013

Fingerhuth Thomas, Finanzmarktstrafrecht, Zurich 2025 (cit. OFK Finanzmarktstrafrecht)

Garbarski Andrew/Conti Yann, Système de communication MROS: quo vadis?, in: Macaluso Alain/Moreillon Laurent/Lombardini Carlo/Garbarski Andrew (édit.), Développements récents en droit pénal de l'entreprise III, Berne 2022

Garbarski Andrew/Macaluso Alain, Commentaire de l'art. 37 LBA, in: Cassani Ursula/Bovet Christian/Villard Katia (édit.), Commentaire romand – Loi sur le blanchiment d'argent, Bâle 2022

Hohl-Chirazi Catherine, Blanchiment d'argent, infraction préalable et *in dubio pro reo*, in: Mazou Miriam/Jeanneret Yvan (édit.), Le procès pénal, Bâle 2025

Hohler Christoph/Schmid Niklaus, Die Stellung der Banken und ihrer Mitarbeiter unter besonderer Berücksichtigung der Verantwortlichkeit der Bank nach StGB Art. 100quater f., PJA 5/2005, p. 515

Hutzler Doris, Kommentar zu Art. 9 GwG, in: Ackermann Jürg-Beat (édit.), Kriminelles Vermögen – Kriminelle Organisationen, 2 tomes, Zurich/Bâle/Genève 2018

Ivell Katrin, Kommentar zu Art. 9 GwG, in: Hsu Peter Ch./Flühmann Daniel (édit.), Basler Kommentar zum Geldwäschereigesetz, Bâle 2021

Julen Berthod Anne Valérie/Lecouturier Alizée, Droits et obligations des intermédiaires financiers, in: Giroud Sandrine/Rordorf-Braun Héloïse (édit.), Droit suisse des sanctions et de la confiscation internationales, Bâle 2020

Kunz Michael, Umsetzung der GAFI-Empfehlungen 2012, Die Geldwäschereiprävention verlässt den Finanzsektor, Jusletter du 23 février 2015

Lombardini Carlo, Banques et blanchiment d'argent, 3 éd., Zurich 2016

Luchsinger Roland, Kommentar zu Art. 9 GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (édit.), Geldwäschereigesetz (GwG) – Stämpflis Handkommentar, Berne 2017

Lutz Peter/Kern Martin, Geldwäscherei und das qualifizierte Steuervergehen von Art. 305 bis Ziff. 1 bis StGB, SJZ 113 (2017), p. 97

Macaluso Alain/Garbarski Andrew, Communication de soupçons de blanchiment après la fin de la relation d'affaires, PJA 10 (2016), p. 1318

Mariani Giulia, Buts, effets et limites des recommandations du GAFI. Avec un regard sur le droit suisse et comparé de la lutte contre le blanchiment d'argent, Bâle 2021

Matthias Kuster, Zur Abgrenzung des Melderechts nach Art. 305ter Abs. 2 StGB von der Meldepflicht nach Art. 9 GwG, in: Jusletter vom 6. Juni 2017 (cit. Abgrenzung)

Mauron Benoît, La valeur patrimoniale sujette à confiscation ou à restitution en procédure pénale, État des lieux de la jurisprudence et défis actuels, AJP 2018 p. 1364 ss

Mooser Michel, Droit notarial, Berne 2025

Niggli Marcel/Muskens Louis, Commentaire de l'art. 11 CP, in: Niggli Marcel/Wiprächtiger Hans (édit.), Basler Kommentar Strafrecht, Bâle 2019

Niggli Marcel/Riedo Christof/Fiolka Gerhard/Muskens Louis, Strafrecht BT, Bâle 2023

Polli Natacha, Commentaire de l'art. 6 LBA, in: Cassani Ursula/Bovet Christian/Villard Katia (édit.), Commentaire romand – Loi sur le blanchiment d'argent, Bâle 2022

Reinle Michael, Die Meldepflicht im Geldwäschereigesetz – Die Banken im Spannungsfeld zwischen Geldwäschereibekämpfung und Vertrauensverhältnis zum Bankkunden, Zurich/St-Gall 2007

Schauwecker Marc-André, Steuerdelikte als Vortaten zur Geldwäscherei und deren Konsequenzen für Finanzintermediäre, Berne 2016

Schinkelshoek Martin, Anwendungsbereich von Art. 9 Abs. 1 lit. b Geldwäschereigesetz (GwG) – Wann besteht für den Finanzintermediär eine Meldepflicht bei Abbruch von Verhandlungen zur Aufnahme einer Geschäftsbeziehung, PJA 3 (2015), p. 481 (cit. PJA 3 (2015), p. 481)

Strasser Othmar, Aufsichts- und verwaltungsstrafrechtliche Verantwortlichkeit bei Gremienentscheidungen in der Geldwäschereibekämpfung von Banken, SJZ 118 (2022), p. 691

- Die Verantwortlichkeit in Banken für Meldungen bei Geldwäschereiverdacht, EF 8/19, p. 607

- Verbrecherischer Erlös nach Geldwäschereigesetz – Was heisst "aus einem Verbrechen herrühren" nach Art. 9 Abs. 1 lit. a Ziff. 2 GwG?, ST 9/10, p. 614

Suter Christoph/Remund Cédric, Neue Vortaten zur Geldwäscherei im Steuerstrafrecht: welche Konsequenzen für Finanzintermediäre?, ASA 82 (2014), p. 589

Suter Christoph/Remund Cédric/Lumengo Paka Nina, Steuervortaten zur Geldwäscherei, GesKR 2019 p. 522

Tanner André/von Rotz Madeleine, Kommentar zu Art. 305ter StGB, in: Lehmkuhl Marianne/Wenk Jan, Onlinekommentar zum schweizerischen Strafgesetzbuch, Version: 13.8.2024

Thelesklaf Daniel, Kommentar zu Art. 9 GwG, in: Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano (édit.), GwG Kommentar, 3e éd., Zurich 2019

Villard Katia, Commentaire de l'art. 9 LBA, in: Cassani Ursula/Bovet Christian/Villard Katia (édit.), Commentaire romand – Loi sur le blanchiment d'argent, Bâle 2022

Autorité fédérale de surveillance des marchés financiers (FINMA), Circulaire 2011/1, Activité d'intermédiaire financier au sens de la LBA Précisions concernant l'ordonnance sur le blanchiment d'argent (OBA), Berne 2010

- Ordonnance de la FINMA sur le blanchiment d'argent (OBA-FINMA), Rapport explicatif sur la révision partielle de l'OBA-FINMA, Berne 2017 (cit. Rapport explicatif sur la révision partielle de l'OBA-FINMA)

- Ordonnance de la FINMA sur le blanchiment d'argent (OBA-FINMA), Rapport de la FINMA sur les résultats de l'audition relative à la révision partielle de l'OBA-FINMA, qui a eu lieu du 4 septembre au 16 octobre 2017, Berne 2018 (cit. Rapport sur les résultats de l'audition relative à la révision partielle de l'OBA-FINMA)

- Révision partielle de l'ordonnance de la FINMA sur le blanchiment d'argent (OBA-FINMA), Commentaires, Berne 2022 (cit. Commentaires sur la révision partielle de l'OBA-FINMA, 27.10.2022)

- Révision partielle de l'Ordonnance de la FINMA sur le blanchiment d'argent (OBA-FINMA), Rapport explicatif, Berne 2022 (cit. Rapport explicatif sur la révision partielle de l'OBA-FINMA, 8.3.2022)

Bureau de communication en matière de blanchiment d'argent (MROS), Rapport annuel 2002, Berne 2003

- Rapport annuel 2007, Berne 2008

- Rapport annuel 2008, Berne 2009

- Rapport annuel 2009, Berne 2010

- Rapport annuel 2010, Berne 2011

- Rapport annuel 2011, Berne 2012

- Rapport annuel 2012, Berne 2013

- Rapport annuel 2013, Berne 2014

- Rapport annuel 2014, Berne 2015

- Rapport annuel 2015, Berne 2016

- Rapport annuel 2016, Berne 2017

- Rapport annuel 2017, Berne 2018

- Rapport annuel 2018, Berne 2019

- Rapport annuel 2020, Berne 2021

- Rapport annuel 2021, Berne 2022

- Rapport annuel 2024, Berne 2025

- Rapport annuel 2025, Berne 2026

- Typologies négatives, Berne 2025

Conseil fédéral, Message concernant la loi sur la transparence des personnes morales, FF 2024 1607

- Message concernant la loi sur la transparence des personnes morales du 22 mai 2024, FF 2024 1607

- Message concernant la mise en œuvre des recommandations du Groupe d'action financière (GAFI), révisées en 2012, du 13 décembre 2013, FF 2014 585

- Message concernant la modification de la loi sur le blanchiment d'argent du 16 juin 2019, FF 2019 5237

- Message concernant la modification du code pénal suisse et du code pénal militaire (Révision du droit de la confiscation, punissabilité de l'organisation criminelle, droit de communication du financier) du 30 juin 1993, FF 1993 III 269

- Message relatif à la loi fédérale concernant la lutte contre le blanchissage d'argent dans le secteur financier du 17 juin 1996, FF 1996 III 1057

- Message relatif à la loi sur les valeurs patrimoniales d'origine illicite du 21 mai 2014, FF 2014 5121

- Message relatif à l'arrêté fédéral portant approbation et mise en œuvre de la Convention du Conseil de l'Europe pour la prévention du terrorisme et de son Protocole additionnel et concernant le renforcement des normes pénales contre le terrorisme et le crime organisé du 14 septembre 2018, FF 2018 6469

- Message sur la mise en œuvre des recommandations révisées du Groupe d'action financière (GAFI) du 15 juin 2007, FF 2007 5919

Département fédéral des finances (DFF), Rapport explicatif concernant l'ordonnance sur le blanchiment d'argent (OBA) – mise en œuvre des recommandations du GAFI, 11 novembre 2015 (cit. Rapport OBA 2015)

Groupe d'action financière (GAFI), 4ème Rapport de suivi renforcé & réévaluation de notations de conformité technique Suisse, 2023

- Les Quarante Recommandations Du Groupe D'action Financière Sur Le Blanchiment De Capitaux, 1990 (cit. Recommandations 1990)

- Les Quarante Recommandations, 1996 (cit. Recommandations 1996)

- Les Quarante Recommandations, 2003 (cit. Recommandations 2003)

- Mandate of the Financial Action Task Force, 2019

- Rapport d'évaluation mutuelle Suisse, 2016

- Rapport d'évaluation mutuelle Suisse, Synthèse, 2005

- Recommandations du GAFI, 2025 (cit. Recommandations 2012)

Office fédéral de la police (Fedpol), Révision partielle de l'ordonnance sur le Bureau de communication en matière de blanchiment d'argent, Commentaires, Berne 2019

Secrétariat d'État aux questions financières internationales (SFI), Consultation relative à la modification de la loi fédérale concernant la lutte contre le blanchiment d'argent et le financement du terrorisme (loi sur le blanchiment d'argent), Rapport de résultats, 26 juin 2019 (cit. Rapport de résultats de la consultation relative à la modification de la LBA)

- Mise en œuvre des recommandations du Groupe d'action financière, révisées en 2012, Rapport explicatif destiné à la consultation, 27 février 2013 (cit. Rapport explicatif sur la mise en œuvre des recommandations du GAFI)

- Modification de la loi fédérale concernant la lutte contre le blanchiment d'argent et le financement du terrorisme, Rapport explicatif sur le projet soumis à consultation, 1 juin 2018 (cit. Rapport explicatif sur la modification de la LBA)

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 11 AMLA

A commentary by Massimo Chiasera

SUGGESTED CITATION

Massimo Chiasera, Commentary of art. 11 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Chiasera, art. 11 AMLA N. XXX

Art. 11 Exclusion of criminal and civil liability

[1] Any person who in good faith files a report under Article 9 of this Act or who freezes assets in accordance with Article 10 may not be prosecuted for a breach of official, profession or trade secrecy or be held liable for breach of contract.

[2] This exclusion of prosecution and liability also applies to:

a. financial intermediaries that file a report under Article 305ter paragraph 2 of the SCC;

b. audit firms that file a report under Article 15 paragraph 5;

c. supervisory organisations in accordance with Article 43*a* of the FINMASA that file a report under Article 16 paragraph 1;

d. self-regulatory organisations that file a report under Article 27 paragraph 4.

CONTENT

I. Basis and purpose of the provision 362
II. Material scope of the exclusion of criminal liability and liability 363
A. Reporting pursuant to Art. 9 AMLA 363
B. Freezing of assets pursuant to Art. 10 AMLA 363
III. Personal scope of application of the exclusion of criminal liability and liability .. 364
IV. Requirement of good faith 365
V. Legal consequences 366
Bibliography 366
Materials 368

I. BASIS AND PURPOSE OF THE PROVISION

1 The exclusion of criminal liability and liability pursuant to Art. 11 AMLA is found in the second section of the second chapter under the heading "Obligations in the event of suspected money laundering." Despite the systematic classification of this provision, it does not establish any additional obligations. Rather, it is a **protective or exonerating provision** in favor of persons, companies, or authorities that are required to report money laundering or freeze assets for the purpose of combating money laundering. Although the provision on the exclusion of liability generally refers to the activities of financial intermediaries, the use of the word "who" suggests that the provision applies not only to financial intermediaries themselves, but also to their organs, employees, and auxiliary persons.

2 Art. 11 AMLA is intended to ensure that financial intermediaries who comply with their obligation to report suspicious assets within the meaning of Art. 9 AMLA or exercise their right to report under Art. 305ter para. 2 SCC do **not face any civil liability for damages and/or criminal consequences**. Art. 11 AMLA implements the protection required by the FATF Recommendations with regard to financial intermediaries that make reports or implement asset freezes.

3 According to Art. 14 SCC, the law cannot prescribe or permit the same conduct and at the same time make it a criminal offense. Provided that the conditions for a report or a freezing of assets are met, Art. 14 SCC thus offers the financial intermediary **protection** from prosecution, as the latter fulfills a legal obligation or exercises a legal right by filing a money laundering report. In other words, in view of Art. 14 SCC, the additional protection of Art. 11 AMLA would not have been necessary to exclude the risk of criminal liability.

4 Art. 11 AMLA also has a certain **signaling effect** within the legal framework, especially since the inclusion of this provision in the Anti-Money Laundering Act sends a strong signal in favor of financial intermediaries and underscores the legislature's commitment to a trustworthy financial center.

II. MATERIAL SCOPE OF THE EXCLUSION OF CRIMINAL LIABILITY AND LIABILITY

A. Reporting pursuant to Art. 9 AMLA

Reporting refers to the transmission of suspicious transactions or business relationships to the Money Laundering Reporting Office (MROS). Art. 11 para. 1 AMLA refers to reports pursuant to Art. 9 AMLA, i.e. reports within the scope of the **statutory reporting obligation**. Art. 11 para. 2 AMLA additionally clarifies that the same protection applies if a financial intermediary exercises its right to report pursuant to Art. 305ter para. 2 SCC. 5

Reports to **foreign reporting offices** and the disclosure of information to third parties are excluded from the scope of Art. 11 AMLA. The justification provided in Art. 11 AMLA is also limited to reporting to the Money Laundering Reporting Office (MROS). In particular, Art. 11 AMLA does not release the financial intermediary from its overriding duty to maintain banking secrecy. Due to general confidentiality obligations, the financial intermediary is therefore prohibited from disclosing to third parties any suspicious circumstances or other details relating to customer relationships and/or any reports of money laundering. Finally, the financial intermediary is subject to the prohibition on disclosure pursuant to Art. 10a AMLA. 6

B. Freezing of assets pursuant to Art. 10 AMLA

The suspicious activity report represents both the temporal or chronological and the systematic starting point for the freezing of assets. This covers the **immediate freezing** ordered by the financial intermediary on the basis of its own investigations, which is provided for in the context of a report pursuant to Art. 9 para. 1 lit. c GwG and is also limited to five working days. Furthermore, the subsequent freezing of assets is also covered, which takes effect as soon as the reporting office informs the financial intermediary that it has forwarded the reported information to a criminal prosecution authority. This provision significantly reduces the financial intermediary's liability risk. It is therefore hardly conceivable that the financial intermediary could be held liable on the basis of a criminal procedural freeze ordered by the law enforcement authorities. Since the financial intermediary must in principle comply with such an order, civil liability is ruled out from the outset. In these situa- 7

tions, Article 11 AMLA therefore constitutes at most an additional, but fundamentally dispensable, defense argument.

III. PERSONAL SCOPE OF APPLICATION OF THE EXCLUSION OF CRIMINAL LIABILITY AND LIABILITY

8 According to the wording of Art. 11 para. 1 AMLA, the exclusion of criminal liability and liability applies to persons who make a report in accordance with Art. 9 AMLA or freeze assets in accordance with Art. 10 AMLA. The **group of addressees** of this provision is therefore determined by the group of persons obliged to act under Articles 9 and 10 AMLA.

9 Art. 11 AMLA covers all persons who are in any way **involved in** making the report or freezing the assets. This includes, in particular, organs, employees, and auxiliary persons whom the financial intermediary has called upon to perform its tasks. The protection therefore extends not only to the financial intermediary itself, but also to its organs, employees, and auxiliary persons, regardless of their function, position, or respective tasks. It therefore makes sense that the scope of protection should cover all persons who are legally obliged or authorized to make a report or to act on behalf of such a person.

10 Since February 1, 2009, **self-regulatory organizations** that submit reports in accordance with Art. 27 para. 4 AMLA have also been expressly covered by the scope of Art. 11 AMLA. Since January 1, 2016, financial intermediaries who disclose information in good faith on the basis of a lawful request for disclosure pursuant to Art. 11a para. 1 AMLA or Art. 11 para. 2 AMLA are also covered by the exemption from criminal liability and liability pursuant to Art. 11 AMLA. If, based on the analysis of information originating from a **foreign reporting office**, it becomes apparent that financial intermediaries subject to this Act are or were involved in a transaction or business relationship in connection with this information, then, since July 1, 2021, pursuant to Art. 11a para. 2bis AMLA, the financial intermediaries involved must also disclose all related information to the reporting office upon request, insofar as they have such information at their disposal. However, Art. 11 AMLA does not apply to persons who are neither subject to the reporting obligation under the Anti-Money Laundering Act nor entitled to exercise the right to report under Art. 305ter para. 2 SCC.

IV. REQUIREMENT OF GOOD FAITH

The exclusion of prosecution and liability requires that the report or the freezing of assets was made in good faith. The requirements for **good faith** must not be set too high in order to preserve the preventive purpose of the Anti-Money Laundering Act and thus not jeopardize the credibility of the measures to combat money laundering. It is irrelevant whether the report or the suspicions that prompted the financial intermediary to report were actually justified, whether the report was effectively forwarded, whether criminal proceedings were initiated, and/or whether a conviction was ultimately handed down in any subsequent criminal proceedings. In other words, the exclusion of criminal prosecution and liability does not only apply in cases where all the conditions set out in Art. 9 or 10 AMLA are met. The exclusion of criminal prosecution and liability is also justified if this was not the case. This applies if, at the time of the report or the freezing of assets, the financial intermediary assumed or could reasonably assume that the conditions were met. 11

Art. 11 AMLA thus also provides protection in cases where it subsequently transpires that the assets do not originate from a crime. Cases where the legal opinions are unclear or disputed and the financial intermediary applied a stricter standard than the Money Laundering Reporting Office or the criminal prosecution authorities are also protected. However, **not too high requirements** should be imposed on the financial intermediary's good faith. 12

Art. 11 AMLA is not only relevant for determining whether a report or a freeze could have been ordered at all, but also for assessing how the financial intermediary justified the suspicion when filing the report. Provided that the financial intermediary has clarified the suspicious circumstances to the best of its knowledge and belief or **with due care** and recorded them in the report, it cannot be held against the financial intermediary if these ultimately prove to be incorrect or if the report was not forwarded to the competent law enforcement authorities or if the subsequent criminal prosecution comes to nothing. 13

The Federal Supreme Court assesses the degree of attention required in this context based on an **average level of attention** that a reasonable person would normally exercise in the circumstances, taking into account the customary practice in the industry concerned. In assessing whether the financial intermediary has exercised the required degree of care, it is necessary to take into account not only the legal framework applicable at the time of the report 14

or the freezing of assets, but also the customary practice in the financial sector or supervisory requirements.

15 Good faith must exist at the **time of the report** or the freezing of assets. If good faith ceases to exist after the report has been submitted or after the freezing of assets has been lifted, this is generally irrelevant. The exclusion of liability nevertheless applies. In connection with Art. 11 AMLA, the judge must place himself in the *ex ante* situation of the financial intermediary, i.e. he must only take into account the information available to the financial intermediary at the time of the report.

V. LEGAL CONSEQUENCES

16 Art. 11 AMLA exempts persons who make reports pursuant to Art. 9 AMLA or freeze assets pursuant to Art. 10 AMLA from **civil and criminal liability**, as these persons "cannot be prosecuted for violations of official, professional, or business secrecy" or "held liable for breach of contract."

17 It has not been conclusively clarified whether the exclusion of punishment under Art. 11 AMLA also applies to Art. 173/174 SCC (defamation offenses), Art. 303 SCC (false accusation) and Art. 304 SCC (obstruction of justice). However, criminal liability is also unlikely to arise in this regard, provided that the financial intermediary exercises the **due diligence** required when making the report and does not deliberately include defamatory and false information in its report. In this context, the financial intermediary should also be able to invoke the justification provided by Art. 14 SCC: According to this provision, anyone who acts in accordance with a federal law shall not be punished. Too narrow a restriction of the applicability of Art. 11 AMLA to confidentiality obligations would be contrary to the purpose of Art. 11 AMLA. Accordingly, a financial intermediary acting in good faith in fulfilling its reporting obligation under Art. 9 GwG should be exempt from criminal liability for defamation, false accusation, and offenses against the administration of justice on the basis of Art. 11 GwG.

BIBLIOGRAPHY

Herren C. Nicolas, L'obligation de communiquer: Les "soupçons fondés" de l' art. 9 LBA, SJ 2019 II, S. 107 ff.

Hürlimann-Kaup Bettina, Die Rechtsprechung des Bundesgerichts zum Einleitungstitel des ZGB in den Jahren 2014 bis 2017 (2/2), ZBJV 155 (2029), S. 110 ff.

Hutzler Doris, Art. 11 Straf- und Haftungsausschluss, in: Ackermann, Jürg-Beat (Hrsg.), Kommentierung zu Kriminelles Vermögen – Kriminelle Organisation – Band II, Zürich 2018 (zit. KV-KO-Hutzler).

Lengauer Daniel/Ruckstuhl Lea, Recht für die Praxis, Compliance, Zürich 2017, S. 301 ff.

Luchsinger Roland J, Kommentierung zu Art. 11 GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Geldwäschereigesetz, Stämpflis Handkommentar, Bern 2017.

Naef Francesco/Calvarese Daniele, I chiarimenti complementari nella lotta antiriciclaggio, NF 9 (2022), S. 488 ff.

Niggli Marcel/Carola Göhlich, Kommentierung zu Art. 14 StGB, in: Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Strafgesetzbuch und Jugendstrafgesetz, Basel 2021.

Porpiglia Gianni/Kunz Oliver M., Kommentierung zu Art.11 GwG, in: Peter Ch. Hsu/Daniel Flühmann (Hrsg.), Basler Kommentar zum Geldwäschereigesetz, Basel 2021 (zit. BSK-Porpiglia/Kunz).

Schären Simon, Die Vermögenssperre als Instrument der Geldwäschereibekämpfung, GesKR 2018, S. 322 ff.

Strasser Othmar, Aufsichts- und verwaltungsstrafrechtliche Verantwortlichkeit bei Gremienentscheidungen in der Geldwäschereibekämpfung von Banken, SJZ 118 (2022), S. 691 ff.

Strasser Othmar, Die Geldwäscherei-Strafbestimmung von Art. 305bis StGB als Schutznorm für geschädigte Anleger? in: Cavallo Angela et al. (Hrsg.), Liber Amicorum für Andreas Donatsch: Im Einsatz für Wissenschaft, Lehre und Praxis, Zürich 2012, S. 867 ff.

Thelesklaf Daniel, Kommentierung zu Art. 11 GwG, in: Thelesklaf Daniel/Wyss Ralph/Van Thiel Mark/Ordolli Stiliano (Hrsg.), GwG/AMLA, Orell Füssli Kommentar, 3. Aufl., Zürich 2019.

MATERIALS

Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG) vom 17.6.1996, BBl 1996 III 1101 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1996/3_1101_1057_993/de, besucht am 11.7.2025 (zit. Botschaft GwG 1996).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 14 AMLA

A commentary by Caroline Kindler

SUGGESTED CITATION

Caroline Kindler, Commentary of art. 14 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Kindler, art. 14 AMLA N. XXX

Art. 14 Affiliation to a self-regulatory organisation

[1] Financial intermediaries within the meaning of Article 2 paragraph 3 must be affiliated to a self-regulatory organisation.

[2] A financial intermediary within the meaning of Article 2 paragraph 3 is entitled to affiliate to a self-regulatory organisation if:

a. the financial intermediary guarantees compliance with its duties in accordance with this Act by means of its internal regulations and organisation

b. the financial intermediary enjoys a good reputation and guarantees compliance with its duties in accordance with this Act

c. the persons responsible for its administration and management also meet the requirements of letter b; and

d. its qualified participants enjoy a good reputation and guarantee that their influence is not detrimental to prudent and sound business operations.

[3] The self-regulatory organisation may make affiliation conditional on the financial intermediary operating in specific sectors.

CONTENT

I. Financial intermediaries' duty to join an SRO (para. 1) 372
A. Financial intermediaries under Art. 2 para. 3 AMLA 372
B. Self-regulatory organization 372
C. Affiliation requirement 372
II. The financial intermediary's right of affiliation (para. 2), substantive requirements 373
A. Internal regulations and operational organization (lit. a) 373
B. Guarantee and good reputation of the financial intermediary (lit. b) 375
C. Guarantee and good reputation of the most senior management (lit. c) 377
D. Requirement for qualified participants (let. d) 377
III. Right of the financial intermediary to affiliation (para. 2), legal consequence 377
IV. Industry-specific restrictions of the SRO (para. 3) 379
Bibliography 380
Materials 381

I. FINANCIAL INTERMEDIARIES' DUTY TO JOIN AN SRO (PARA. 1)

1 When FinIA entered into force on January 1, 2020, the dual control system of the AMLA, which offered a choice between direct supervision by FINMA and affiliation to an SRO, was replaced by an exclusive **SRO control system**. The duty of financial intermediaries under Art. 2 para. 3 AMLA to join a self-regulatory organization (SRO) was enshrined in Art. 14 para. 1 AMLA.

A. Financial intermediaries under Art. 2 para. 3 AMLA

2 Financial intermediaries in accordance with Art. 2 para. 3 AMLA are persons who professionally accept, hold or assist in the investment or transfer of assets belonging to third parties. Examples of such **financial intermediaries** can be found in Art. 2 para. 3 let. a–c, f and g. The definition of such a financial intermediary is specified in the AMLO and in FINMA Circular 2011/1.

B. Self-regulatory organization

3 This refers to the **self-regulatory organization** under Art. 24 AMLA.

C. Affiliation requirement

4 Art. 14 para. 1 AMLA establishes the **obligation for** financial intermediaries as defined in Art. 2 para. 3 AMLA to join a self-regulatory organization (SRO). Such membership is mandatory: When commencing professional activity as a financial intermediary in accordance with Art. 2 para. 3 AMLA, the application for admission to an SRO must be submitted within two months (Art. 11 para. 1 let. b AMLO). Until they are affiliated, these financial intermediaries are prohibited from taking any action other than that which is strictly necessary to safeguard the assets (Art. 11 para. 2 AMLO). If a financial intermediary leaves or is excluded from an SRO, it must also apply to join another SRO within two months (Art. 12 para. 1 AMLO). It may continue its activities until it is admitted to the new SRO, but only within the framework of existing business relationships (Art. 12 para. 2 AMLO).

5 *E contrario*, a financial intermediary within the meaning of Art. 2 para. 3 AMLA is prohibited from operating without being affiliated to an SRO, subject

to the deadlines set out in Art. 11 para. 2 and Art. 12 para. 2 AMLO. Violation of the duty to join an SRO constitutes illegal activity as a financial intermediary, which can be punished with a custodial sentence of up to three years or a monetary penalty in the case of intent, or a fine of up to CHF 250,000 in the case of negligence (Art. 44 FINMASA). In addition, FINMA may take supervisory measures against the financial intermediary in accordance with Art. 29–37 FINMASA or order its dissolution (Art. 20 AMLA).

An **SRO** is not prohibited from admitting financial intermediaries that it knows or must assume have violated the two-month time limit in accordance with Art. 11 para. 1 let. b or Art. 12 para. 2 AMLO and are therefore already operating illegally. In such cases, however, the SRO is subject to an immediate reporting obligation to FINMA, which must contain all relevant information known to it. 6

II. THE FINANCIAL INTERMEDIARY'S RIGHT OF AFFILIATION (PARA. 2), SUBSTANTIVE REQUIREMENTS

Art. 14 para. 2 AMLA sets out the conditions under which a financial intermediary is entitled to affiliate with an SRO. These conditions must be met **cumulatively**. 7

A. Internal regulations and operational organization (lit. a)

Art. 14, para. 2, let. a AMLA requires sufficient internal regulations and an appropriate operational organization to ensure compliance with the obligations under the AMLA. 8

The requirements that the internal regulations and the operational organization must meet are based on the **regulations** of the SRO applicable to the respective financial intermediary in accordance with Art. 25 AMLA, which specify the legal obligations. AMLO-FINMA is not directly applicable to financial intermediaries in accordance with Art. 2 para. 3 AMLA. Nevertheless, FINMA bases its approval of SRO regulations on the key parameters of AMLO-FINMA (Art. 1 para. 2 AMLO-FINMA). This means that although SRO regulations may contain deviations from AMLO-FINMA, these deviations must be clearly identified (Art. 1 para. 3 AMLO-FINMA). 9

10 In the sense of this "indirect" applicability of AMLO-FINMA to financial intermediaries in accordance with Art. 2 para. 3 AMLA, the points listed under Art. 26 para. 2 AMLO-FINMA provide at least some indications of what should be regulated by the financial intermediaries. Accordingly, the following points should be set out in an **internal directive** on combating money laundering and terrorist financing:

a. the criteria for identifying higher-risk business relationships in accordance with Art. 13 AMLO-FINMA;

b. the criteria for identifying higher-risk transactions in accordance with Art. 14 para. 1 and 2 AMLO-FINMA;

c. the principles of transaction monitoring in accordance with Art. 20 AMLO-FINMA;

d. the cases in which the internal anti-money laundering unit must be consulted and the most senior management body must be informed;

e. the principles of staff training;

f. the business policy for dealing with politically exposed persons;

g. the responsibility for reporting to the Money Laundering Reporting Office;

h. the modalities by which the financial intermediary records, limits and monitors increased risks;

i. the amount limits in accordance with Article 13 para. 2 e) and f) and Article 14 para. 2 a) AMLO-FINMA;

j. the criteria for the involvement of third parties in accordance with Art. 28 AMLO-FINMA;

k. the internal allocation of tasks and competencies between the anti-money laundering unit and the other business units responsible for the application of the duties of due diligence;

l. the updating of client documentation.

11 In order to implement these provisions, the financial intermediary must have an appropriate **operational structure**. For the interpretation of the concept of operational structure, Art. 8 AMLA in connection with Art. 23 ff. AMLO-FINMA – subject to the applicable SRO regulations. In particular, the finan-

cial intermediary must set up an office specializing in money laundering, consisting of one or more qualified persons (Art. 24 para. 1 AMLO-FINMA), which performs the tasks set out in Art. 24 f. AMLO-FINMA. The SRO regulations may stipulate that the anti-money laundering unit of a financial intermediary only has to fulfill the tasks specified in Article 24 AMLO-FINMA (or in the corresponding provision of the SRO regulations) if the financial intermediary has a staff complement of five or fewer full-time employees or an annual gross income of less than CHF 2 million and pursues a business model without increased risks (*by analogy* with Art. 75 para. 1 AMLO-FINMA). In any case, the SRO may require that the anti-money laundering unit also fulfill the tasks according to Art. 25 AMLO-FINMA (or according to the corresponding provision of the SRO regulations), if this is necessary to combat money laundering and terrorist financing (*by analogy* with Art. 75 para. 2 AMLO-FINMA).

Regarding the formal scope of the **documentary evidence** that a financial intermediary must submit to the SRO as part of the application for affiliation as proof of compliance with the conditions of article 14, para. 2, letter a, it is recommended that the SRO should request not only the AMLA directive but also the organizational regulations, the statutes, an organizational chart and, where applicable, contracts for the delegation of tasks in the area of the AMLA. 12

B. Guarantee and good reputation of the financial intermediary (lit. b)

The **guarantee requirement** was originally enshrined in the Banking Act (Art. 3 para. 2 let. c BankG) to ensure that a bank is "managed by reliable and professionally capable persons". In the meantime, the guarantee requirement can be found in most financial market laws. It is an indeterminate legal concept. It is debatable whether the practice developed in banking and stock exchange law can be used for interpretation, since the concept of "guarantee" according to Art. 14 AMLA differs from that in BankG: Pursuant to Art. 14 para. 2 let. b and c AMLA, the financial intermediary must only offer "guarantee of fulfilment of the obligations under the AMLA" and not, as in banking and stock exchange law, "guarantee of proper business conduct" in general. The latter guarantee requirement demands not only compliance with the relevant laws, but also, in general, compliance with the entire legal system. In 13

view of the clear wording of Art. 14 AMLA, according to the Federal Supreme Court, it cannot be assumed that the guarantee requirement in the AMLA is to be interpreted in the same way as in banking and stock exchange law. Different treatment is also justified by the different purposes of the laws: The banking and stock exchange legislation is primarily aimed at protecting customers and investors, while the AMLA is primarily intended to combat money laundering. Despite these relativizing remarks, the Federal Supreme Court concludes that the requirement of "guarantee" under Art. 14 AMLA, in the sense of a person's "ability to comply with the law", can be called into question if a financial intermediary violates provisions other than those of the AMLA under Art. 2 para. 3 AMLA. However, a certain level of seriousness is required for violations of the law to be assumed to mean that the guarantee of compliance with the AMLA is no longer fulfilled. Such seriousness is deemed to exist in particular if the violations and the conduct of the financial intermediary in this context indicate that the financial intermediary "is not willing or able to comply with the obligations arising from the Anti-Money Laundering Act or the corresponding orders of the supervisory authority".

14 Compliance with the requirement for proper business conduct must be assessed on a **case-by-case basis**, based on the specific tasks and functions and with regard to the financial intermediary's specific legal obligations.

15 Pursuant to Article 1a of the FINMA Data Ordinance, FINMA includes data on persons whose proper business conduct is in doubt or cannot be guaranteed in a **data collection** (para. 1). This data collection, known as the "watchlist", serves to ensure that only persons who can guarantee proper business conduct are entrusted with the administration or management of supervised institutions (para. 2 let. a) or hold a significant interest in the supervised institution (para. 2 let. b). The watchlist is registered with the Federal Data Protection and Information Commissioner (FDPIC), but is not publicly accessible and is intended for internal use only. It may only contain corroborated and reliable data on a person, such as information on criminal and administrative, supervisory and disciplinary proceedings. Unsubstantiated suspicions, accusations or allegations may not be included.

16 In addition to the requirement to provide guarantees, it is also assumed that the financial intermediary has a **good reputation**. In contrast to the requirement to provide guarantees, which is based on the applicable legal system, the assessment of good reputation is linked to moral conditions: a good reputa-

tion encompasses characteristics such as respect, esteem and trustworthiness, whereby particular attention is paid to integrity, honesty, conscientiousness and diligence. Nevertheless, the two legal concepts overlap in many areas.

To assess the guarantee and good reputation, **SROs** usually require extracts from the criminal and debt collection registers, as well as written confirmations that no criminal, civil or administrative proceedings are pending. In addition, they require proof of educational qualifications, employment references and CVs with references. 17

C. Guarantee and good reputation of the most senior management (lit. c)

The guarantee requirement concerns not only the "depersonalized" guarantee of the financial intermediary but also the **most senior management**, i.e. the persons entrusted with administration and management. This includes not only the formal bodies but also, in principle, all persons who have a decisive influence on the financial intermediary's key strategic or operational decisions. It is not the job title that is important, but the function actually exercised. The interpretation described in the commentary on Article 14, para. 2, let. b AMLA can also be applied accordingly to the requirements for natural persons in accordance with Article 14, para. 2, let. c AMLA. 18

D. Requirement for qualified participants (let. d)

The **holders of qualified participations** in a financial intermediary are also subject to a duty to provide a guarantee, which is, however, limited to their good reputation and their influence on business activities. The threshold for a qualified participation is generally 10% of the capital or votes. An exception is the SRO PolyReg, which sets the threshold at 20%. The SRO Leasingverband requires, in addition to the disclosure of all shareholders or partners with a holding of more than 10%, the disclosure of the financial intermediary's controlling persons, analogous to the definition in Art. 2a para. 3 AMLA. 19

III. RIGHT OF THE FINANCIAL INTERMEDIARY TO AFFILIATION (PARA. 2), LEGAL CONSEQUENCE

Art. 14 para. 2 AMLA stipulates that the financial intermediary has a **legal right** to join an SRO if he cumulatively fulfils the conditions of para. 2, letters 20

a to d. This legal right is subject only to the sector-specific restrictions which may be determined by the SRO in accordance with Art. 14 para. 3 AMLA. If the financial intermediary meets the membership requirements, the SRO is in principle obliged to accept him.

21 According to the Federal Court, self-regulatory organizations perform a state function in the fight against money laundering and are therefore bound by the **fundamental rights** under Article 35, para. 2 FC. The admission procedure must therefore comply with the principle of equality before the law (Art. 8 FC) and the prohibition of arbitrariness (Art. 9 FC), both with regard to the statutes and regulations and with regard to the specific admission decisions. Admission decisions that treat financial intermediaries willing to join the scheme differently despite the same conditions, or rejection decisions that are not based on any objective reasons, are not permitted. In addition, the financial intermediary willing to join the scheme must be granted the right to a legal hearing (Art. 29 para. 2 FC), which includes in particular the right to a reasoned decision.

22 A rejected financial intermediary may request that FINMA review the refusal of affiliation. Since FINMA is obliged under Art. 31 FINMASA to restore order in the event of violations of the law or other abuses, it would have to enforce the financial intermediary's affiliation in the event of an unlawful **refusal of affiliation** on the part of the SRO. Pursuant to Art. 53 FINMASA, FINMA would also be entitled to issue a formal ruling in terms of Art. 5 para. 1 (a) APA: since admission to an SRO is formally a matter of private law, it cannot be ordered by decree. However, FINMA is able to issue a declaratory decision stating that the refusal of admission was unlawful and that only the admission of the financial intermediary can restore compliance with the regulations.

23 It should be noted that the **legal classification** of admission to an SRO as a purely private matter has recently been challenged by case law. In its judgment of November 21, 2023, the Federal Administrative Court ruled that the SRO VQF's decision not to accept an applicant was a ruling that fell under public law. In general, when assessing the legal relationship between the SRO and its members, there appears to be a tendency towards a weighting in favour of public law, which has been supported not least by the introduction of the supervisory organizations under Art. 43a FINMASA. In its judgment 2C_887/2017 of March 23, 2021, the Federal Supreme Court confirmed the private-law character of the sanctioning mechanism of the SRO PolyReg, but

emphasized that due to the development of the fight against money laundering in Switzerland in recent decades – from an initial purely private self-regulation to an essential public task – it is possible that in the future the Federal Supreme Court could qualify sanctions under money laundering law as public law.

IV. INDUSTRY-SPECIFIC RESTRICTIONS OF THE SRO (PARA. 3)

Art. 14 para. 3 AMLA allows self-regulatory organizations to make affiliation dependent on the activity in certain areas. This entitles SROs to limit their membership to financial intermediaries from a particular **professional group**. In order to meet the requirements of an admission procedure that complies with fundamental rights, the definition of these areas must be based on objective and factually comprehensible criteria that can stand up to independent judicial review. As of the cut-off date (July 1, 2024), the following SROs were authorized by FINMA: 24

- AOOS - Swiss Company for Supervision (AOOS);
- ASSOCIATION ROMANDE DES INTERMEDIAIRES FINANCIERS (ARIF);
- Organisme de Surveillance pour Intermédiaires Financiers & Trustees SO-FIT (Supervisory Organization for Financial Intermediaries & Trustees SO-FIT);
- Organismo di Autodisciplina dei Fiduciari del Cantone Ticino (OAD FCT);
- PolyReg General Self-Regulation Association;
- Swiss Leasing Association (SRO SLV);
- Self-regulatory organization of the Swiss Bar Association and the Swiss Association of Notaries (SRO SAV/SNV);
- Self-regulatory organization of the Swiss Insurance Association (SRO-SVV);
- Self-regulatory organization of the Swiss Association of Investment Companies (SRO SVIG);
- SRO-Treuhand Suisse;

- VQF Financial Services Standards Association (SRO VQF).

Classic industry SROs, which link their membership to a specific profession, are the SRO SLV, SRO SAV/SNV, SRO-SVV, SRO SVIG and SRO Treuhand Suisse. The OAD FCT, SRO PolyReg and SRO VQF are cross-industry SROs.

25 AOOS and SO-FIT have both an authorization as an SRO and an authorization as a **supervisory organization** under Article 43a FINMASA. Affiliation with the AOOS and SO-FIT self-regulatory organizations was open to asset managers and trustees until the end of the transitional period under Article 74 para. 2 FinIA, i.e. until December 31, 2022. Since that date, asset managers and trustees have been required to apply to FINMA for a license as an asset manager (pursuant to Art. 17 para. 1 FinIA) and/or as a trustee (pursuant to Art. 17 para. 2 FinIA) and to be subject to the supervision of a supervisory organization in accordance with Art. 43a FINMASA.

BIBLIOGRAPHY

Amadò Flavio/Molo Giovanni, Kommentierung zu Art. 11 FINIG, in: Amadò Flavio/Molo Giovanni (Hrsg.), FIDLEG. Bundesgesetz über die Finanzdienstleistungen, Verhaltens-, Organisations- und Verfahrensnormen des FIDLEG sowie ausgewählter Bestimmungen des FINIG. Praxiskommentar, Zürich/St. Gallen 2022.

Blatter Manuel, Rechtsstaatliche Garantien im Enforcementverfahren der FINMA, Ausgewählte Aspekte in der Institutaufsicht und in Unterstellungssachen, Zürich 2019.

Emmenegger Susan, Zulässigkeit eines SRO-Anschlusszwangs für Finanzintermediäre im Sinne von Art. 2 Abs. 3 GwG, Rechtsgutachten zuhanden des Eidg. Finanzdepartements, Bern 2013.

Frigo Patrick/Jain Vivien, Kommentierung zu Art. 14 GwG, in: Peter Ch. Hsu/Daniel Flühmann (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Vogel Alexander/Heiz Christoph/Luthiger Reto, Kommentierung zu Art. 11 FINIG, in: Vogel Alexander/Heiz Christoph/Luthiger Reto (Hrsg.), Orell Füssli Kommentar, Bundesgesetz über die Finanzdienstleistungen und Bundesgesetz über die Finanzinstitute und weiteren Erlassen, Zürich 2020.

Wyss David, FINMA-Bussenkompetenz – ein wirksames Mittel zur Abschreckung?, GesKR 2024, S. 129 ff.

Wyss Ralph, Kommentierung zu Art. 14 GwG, in: Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell Füssli Kommentar, Geldwäschereigesetz, 3. Aufl., Zürich 2019.

MATERIALS

Association romande des intermédiaires financiers (ARIF), (nicht datiertes) Selbstregulierungsreglement, abrufbar unter https://arif.ch/IMG/pdf/reglementoar_d.pdf, besucht am 23.8.2024 (zit. Selbstregulierungsreglement ARIF).

Botschaft des Bundesrates an die Bundesversammlung über die Revision des Bankengesetzes vom 13. Mai 1970, BBl 1970 1144, abrufbar unter https://www.fedlex.admin.ch/eli/fga/1970/1_1144__/de, besucht am 23.8.2024 (zit. Botschaft BankG 1970).

Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG) vom 17.6.1996, BBl 1996 III 1101, abrufbar unter https://www.fedlex.admin.ch/eli/fga/1996/3_1101_1057_993/de, besucht am 23.8.2024 (zit. Botschaft GwG 1996).

Botschaft zum Finanzdienstleistungsgesetz (FIDLEG) und zum Finanzinstitutsgesetz (FINIG) vom 4.11.2015, BBl 2015 8901, abrufbar unter https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2015/2141/de/pdf-a/fedlex-data-admin-ch-eli-fga-2015-2141-de-pdf-a.pdf, besucht am 23.8.2024 (zit. Botschaft FIDLEG/FINIG 2015).

Eidgenössische Finanzmarktaufsicht (FINMA), Rundschreiben 2008/17 Informationsaustausch zwischen den SRO und der FINMA betreffend Anschlüsse, Ausschlüsse und Austritte von Finanzintermediären vom 20.11.2008, abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2008-17.pdf?sc_lang=de&hash=71FFD4758724C36DBC692710A9C8477B, besucht am 23.8.2024.

Eidgenössische Finanzmarktaufsicht (FINMA), Rundschreiben 2011/1 Tätigkeit als Finanzintermediär nach GwG, Ausführungen zur Geldwäschereiverordnung (GwV) vom 20.10.2010, abrufbar unter https://www.finma.ch/de/~/media/

finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2011-01-01-01-2017.pdf?la=de, besucht am 23.8.2024.

Geschäftsbericht 2021 des Bundesgerichts vom 17.2.2022, abrufbar unter https://www.eidgenoessischegerichte.ch/de/files/geschaeftsberichte/GB_2021_d.pdf, besucht am 23.8.2024 (zit. Geschäftsbericht 2021 des Bundesgerichts).

Liste der von der FINMA anerkannten Selbstregulierungsorganisationen (SRO), abrufbar unter https://www.finma.ch/de/bewilligung/selbstregulierungsorganisationen-sro/, besucht am 23.8.2024.

Organisme de Surveillance pour Intermédiaires Financiers & Trustees (SO-FIT), Règlement relatif aux obligations des affiliés à l'organisme d'autorégulation du 1.10.2020, abrufbar unter https://so-fit.ch/wp-content/uploads/2021/02/Re%CC%80glement-daffiliation.OAR_.SO-FIT.2021.pdf, besucht am 23.8.2024 (zit. Reglement SO-FIT).

Organismo di Autodisciplina dei Fiduciari del Cantone Ticino (OAD FCT), Statuti dell'organismo di autodisciplina dei fiduciari del cantone Ticino del 1.1.2020, abrufbar unter https://oadfct.ch/Regolamenti/, besucht am 23.8.2024 (zit. Statuten OAD FCT).

PolyReg Allg. Selbstregulierungs-Verein, Aufnahmegesuch, abrufbar unter https://www.polyreg.ch/uploads/Dokumente/de/Aufnahmegesuch.pdf, besucht am 23.8.2024 (zit. Aufnahmegesuch SRO PolyReg).

PolyReg
Allg. Selbstregulierungs-Verein, Statuten vom 1.7.2023, abrufbar unter https://www.polyreg.ch/uploads/Polyreg_Statuten.pdf, besucht am 23.8.2024 (zit. Statuten SRO PolyReg).

Schweizer Verband der Investmentgesellschaften (SVIG), Reglement zur SRO-Zugehörigkeit vom 1.1.2016, abrufbar unter https://www.svig.org/sites/default/files/downloads/reglement%201-9%2C%20v01.01.2016.pdf, besucht am 23.8.2024 (zit. Reglement SRO-Zugehörigkeit SRO SVIG).

Schweizerische Aktiengesellschaft für Aufsicht (AOOS), Anschlussvertrag an die Selbstregulierungsorganisation nach Geldwäschereigesetz, abrufbar unter https://www.aoos.ch/dataset/file/9018-aoos-sro-anschlussvertrag-pdf, besucht am 23.8.2024 (zit. Anschlussvertrag AOOS).

Selbstregulierungsorganisation des Schweizerischen Anwaltsverbandes und des Schweizer Notarenverbandes (SRO SAV/SNV), Reglement vom 27.6.2023, abrufbar unter https://sro-sav-snv.ch/rechtliche-grundlagen/regelwerke, besucht am 23.8.2024 (zit. Reglement SRO SAV/SNV).

Selbstregulierungsorganisation des Schweizerischen Leasingverbandes SRO/SLV, Anschlussantrag, abrufbar unter https://www.leasingverband.ch/cms/upload/fullsearch_documents/Administrator/Anschlussantrag.pdf, besucht am 23.8.2024 (zit. Anschlussantrag SRO/SLV).

Selbstregulierungsorganisation des Schweizerischen Leasingverbandes SRO/SLV, Reglement für Anschluss, Austritt und Ausschluss von Finanzintermediären vom 15.12.1999 (Fassung vom 13.1.2016), abrufbar unter https://www.leasingverband.ch/cms/upload/fullsearch_documents/Administrator/Reglement_fuer_Anschluss_Austritt_und_Ausschluss_von_Finanz-intermediaeren.pdf, besucht am 23.8.2024 (zit. Anschlussreglement SRO/SLV).

Selbstregulierungsorganisation des Schweizerischen Leasingverbandes SRO/SLV, Selbstregulierungsreglement SRO/SLV vom 15.12.1999 (Fassung vom 19.1.2023), abrufbar unter https://www.leasingverband.ch/cms/upload/Selbstregulierungsreglement_SRR_12._Fassung_vom_19._Januar_2023_gltig_ab_01.04.2023.pdf, besucht am 23.8.2024 (zit. Selbstregulierungsreglement SRO/SLV).

Selbstregulierungsorganisation Schweizerischer Treuhandverband (SRO-Treuhand|Suisse), Statuten vom 1.7.2021, abrufbar unter https://sro-treuhand-suisse.ch/fileadmin/Aktuelles/Finanzintermediaer/Regelwerke_der_SRO/SRO_Statuten_gueltig_ab_01072021.pdf, besucht am 23.8.2024 (zit. Statuten SRO-Treuhand|Suisse).

Verein Selbstregulierungsorganisation des Schweizerischen Versicherungsverbandes (SRO-SVV), Statuten vom 21.8.2020, abrufbar unter https://www.sro-svv.ch/images/pdf/de_regelwerk/Statuten_SRO-SVV.pdf, besucht am 23.8.2024 (zit. Statuten SRO-SVV).

VQF Verein zur Qualitätssicherung von Finanzdienstleistungen (SRO VQF), Statuten vom 1.7.2023, abrufbar unter https://www.vqf.ch/de/vqf-downloads, besucht am 23.8.2024 (zit. Statuten SRO VQF).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 15 AMLA

A commentary by Thomas Nagel

SUGGESTED CITATION

Thomas Nagel, Commentary of art. 15 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Nagel, art. 15 AMLA N. XXX

Art. 15 Dealers' duty to verify

[1] Dealers with duties of due diligence under Article 8*a* must appoint an audit firm to verify whether they are complying with their duties under Chapter 2.

[2] Audit firms under Article 6 of the Auditor Oversight Act of 16 December 2005 which have the required expertise and experience may be appointed as an audit firm.

[3] The dealers must provide the audit firm with all the information and documents required to conduct the audit.

[4] The audit firm shall verify compliance with the duties under this Act and prepare a report thereon for the attention of the responsible management bodies of the dealer audited.

[5] If a dealer fails to comply with its duty to report, the audit firm shall immediately file a report with the Reporting Office if it has reasonable grounds to suspect that:

a. an offence under Article 260ter or 305bis SCC has been committed;

b. assets are the proceeds of a felony or an aggravated tax misdemeanour under Article 305bis number 1bis SCC;

c. assets are subject to the power of disposal of a criminal or terrorist organisation; or

d. assets serve the financing of terrorism (Art. 260^{quinquies} para. 1 SCC).

CONTENT

I. General 388
II. Scope of the obligation 388
III. Requirements for the audit and the audit firm 389
IV. Scope and period of the audit 390
V. Auditing procedures 391
VI. Reporting obligation of the auditing company 392
VII. Legal consequences of violating the audit requirement 392
Bibliography 393
Materials 393

I. GENERAL

1 The term "dealer" includes natural and legal persons who **trade in goods and accept cash in payment** (Art. 2 para. 1 let. b AMLA). Unlike financial intermediaries, dealers are not subject to any state supervision or supervision by self-regulatory organizations. Since they are not financial market players, supervision is not the responsibility of FINMA. Art. 15 AMLA is intended to ensure and verify compliance with AMLA obligations by dealers by obliging dealers to commission an audit firm to audit the dealer's compliance with the obligations under Chapter 2 of AMLA. It is confusing that the term "auditing body" was still used in the original version of Art. 15 AMLA (in force until December 31, 2022). In corporate law, an "auditing body" refers to a body within a company with special rights and duties, whose main purpose is to audit the statutory annual financial statements. Its task is thus essentially to audit the accounts. However, monitoring compliance with due diligence obligations is an activity of the regulatory audit. The term was thus replaced by "audit firm" as of January 1, 2023, and is also consistently used in this commentary. However, the adjustment was forgotten in Art. 22 AMLO, where the incorrect term "auditing body" is still used.

II. SCOPE OF THE OBLIGATION

2 Art. 15 para. 1 AMLA is explicitly linked to the **scope of application of Art. 8a**. This means that dealers who have to fulfill the obligations under Art. 8a AMLA are subject to the audit requirement. Accordingly, only dealers who accept more than CHF 100,000 in at least one trading transaction must commission an audit firm to carry out an audit in accordance with Art. 15 para. 1 AMLA. It is sufficient if one trading transaction exceeds the aforementioned amount. In other words, the scope of application of Art. 15 AMLA is the same as that of Art. 8a AMLA. For the scope of application of the dealer concept and the obligations, see the comments on Art. 2 para. 1 AMLA and Art. 8a AMLA.

III. REQUIREMENTS FOR THE AUDIT AND THE AUDIT FIRM

The obligation under Article 15 AMLA to appoint an audit firm applies to dealers regardless of the obligation to have the annual and, if applicable, the consolidated financial statements audited (Article 22 para. 1 AMLO; see Article 727 and Article 727*a* CO for ordinary and limited audits). A dealer who has both the invoice in accordance with CO and compliance with the AMLA obligations audited by the same audit firm should demand a separate engagement letter and declaration of completeness, as the AMLA audit is a separate audit subject. **Audit firms** that have the necessary **specialist knowledge** and **experience** can be commissioned (Art. 15 para. 2 AMLA). The audit firm itself must assess whether it is competent to carry out the audit. According to the legislator, the company or person conducting the audit (lead auditor) is competent to do so if they are licensed by the Federal Audit Oversight Authority (FAOA) or a self-regulatory organization to conduct audits under financial market laws or the AMLA (Art. 9*a.* AOA or Art. 24 para. 1 let. d AMLA). 3

If the dealer does not have an audit firm, the **board of directors or the board of management** shall commission an audit firm in accordance with Article 6 AOA to carry out the audit (Article 15, para. 2 AMLA in conjunction with Article 22, para. 2 AMLO). This duty can be delegated, but not the responsibility for it. The statutory auditors (regardless of whether or not they also perform the AMLA audit of the dealer), if required, must list the results of the AMLA audit in the audit report. The impact of violations on the financial statements (e.g. impending fines that would lead to a future outflow of funds) must be taken into account, for example by checking whether appropriate provisions have been created and whether the annual financial statements give a true and fair view. 4

The mandated audit firm must be licensed by the Federal Audit Oversight Authority (FAOA). An audit firm is licensed in accordance with Art. 6 AOA if the majority of the members of the supreme governing body and the management body are appropriately licensed; at least one-fifth of the individuals who participate in providing audit services have the appropriate license; it is ensured that all persons who direct audit services have the appropriate license and the management structure ensures that the individual mandates are sufficiently monitored (Art. 6 para. 2 AOA). In addition, according to Art. 6 para. 2 AOA, 5

public financial auditors may also be licensed as audit firms if they meet the requirements of Art. 6 para. 1 AOA. Until December 31, 2022, it was possible to commission a natural person to carry out the audit (see Art. 15 paras. 1 and 2 AOA, Art. 5 AOA in conjunction with Art. 4 paras. 2 and 3 AOA). This was adjusted as of January 1, 2023, because it is not common or contrary to the system in the area of regulatory audit – a natural person may only provide legally required audit services on a self-employed basis if they are registered in the commercial register as a sole proprietorship and they themselves, as well as their sole proprietorship, are appropriately licensed by the supervisory authority (Art. 8 AOO).

6 Dealers must **provide the audit firm with** all the information and **documents required** for the audit (Art. 15 para. 3 AMLA). The audit firm has full discretion to request any documents and information necessary for the execution of the mandate. The audit firm is subject to professional secrecy by law, but this is overridden in the event of a reporting obligation under Art. 15 para. 2 AMLA.

IV. SCOPE AND PERIOD OF THE AUDIT

7 The audit firm shall audit compliance with the **AMLA obligations** applicable to the dealer to be audited and shall draw up a **report** on this for the attention of the audited dealer's responsible body (Art. 15 para. 4 AMLA). This includes all the due diligence requirements applicable to dealers mentioned in Art. 8a AMLA (identification of the contracting party, determination of the beneficial owner, documentation requirement and special duty of clarification) and the reporting requirement pursuant to Art. 9 para. 1bis AMLA. Compliance with the prohibition on information (Art. 10*a* para. 5 AMLA) cannot be meaningfully verified.

8 The audit firm shall check whether there are any indications that the list of cash transactions is incomplete or that the applicable duties of care have not been complied with in this regard. If the list is incomplete, the firm shall request the merchant to complete it immediately; if this is no longer possible, this fact shall be included in the report. The audit firm's audit is based on the **documentary evidence** prepared in accordance with Art. 8a para. 1 let. c in conjunction with Art. 7 AMLA. This documentation must be designed in such a way that it can be verified by the audit firm, in such a way that all the information contained in Art. 21 para. 1-3 AMLO is visible. The documentation

must be kept for at least ten years (Art. 21 para. 4 AMLO). The audit firm takes a risk-based approach to its audit, i.e. it must, at its own discretion, deepen (e.g. if there are indications of misconduct) or relax (e.g. by selecting samples from a large number of transactions in excess of CHF 100,000) certain aspects, while observing the principle of proportionality.

From a time perspective, the audit period for compliance with the AMLA provisions may, for practical reasons, coincide with the financial year. In exceptional cases, a shorter or longer **audit period** may also be chosen by the dealer's senior management or board of directors. There is no legal requirement for dealers to be audited annually. What is clear is that the duty to audit is triggered in principle by a cash transaction in excess of CHF 100,000. However, it is not clear by when the audit obligation must be fulfilled. A separate audit for each individual purchase transaction would not be practical. Accordingly, it may be difficult in practice to accuse a merchant of violating Art. 15 AMLA – in my opinion, it is unclear when this violation begins. Wyss and EXPERTsuisse are of the opinion that the audit should be carried out at the latest when the merchant would have to have an audit of the annual financial statements carried out if he were required to do so under the Swiss Code of Obligations. This would mean that, for example, the audit of a joint-stock company would have to be carried out within six months of the end of the financial year (in line with Art. 699 para. 2 CO). Even if this view is logically sound in my opinion, there is no clear legal basis for it. In my opinion, this is tricky, especially when imposing a penalty for a violation of this duty (*nulla poena sine lege,* Art. 1 SCC) (see OK-Nagel/Parvex, Art. 38 AMLA N. 7). 9

It must be possible to audit all cash payments for goods in excess of CHF 100,000 made during an audit period. The dealer must submit a written **letter of representation**. In doing so, payments that are interrelated in terms of time or economic context must be considered together (Art. 8a para. 3 AMLA), which can be difficult in practice. 10

V. AUDITING PROCEDURES

The auditing company's audit procedures are divided into **three audit steps**: risk analysis, audit of the completeness of the documentation and audit of compliance with the due diligence and reporting obligations. There are no provisions for test purchases or other forms of monitoring the business conduct of dealers. 11

VI. REPORTING OBLIGATION OF THE AUDITING COMPANY

12 According to Art. 9, para. 1bis AMLA, the **primary reporting obligation lies with the dealer**. If a merchant fails to comply with the reporting requirement under Art. 9 para. 1bis AMLA, the **audit firm** shall report the matter to the Money Laundering Reporting Office Switzerland (MROS) without delay in accordance with Art. 15 para. 4 AMLA (**subsidiary reporting requirement**) if it has reasonable grounds to suspect that: a criminal offence under Art. 260ter or 305bis SCC (a) a criminal offence under Article 260ter or 305bis SCC The audit firm also has a reporting obligation if, during the audit, it comes across new facts or itself has a reasonable suspicion without the dealer having come to this conclusion himself. In the literature, the view is put forward that the audit firm should set a short deadline for the trader who has failed to report, within which the trader can make the report himself. This approach makes sense even if it is not provided for by law, which requires the audit firm to report "without delay".

13 The reporting requirement also applies if the dealer withdraws the audit firm's mandate after the latter becomes aware of facts that require reporting, or if the audit firm itself resigns the mandate. It should be noted that the audit firm itself has no independent obligation to report – it merely reports on behalf of the defaulting dealer, in the sense of a **substitute performance**, who has failed to do so in breach of duty. The audit firm is not criminally liable under Art. 37 AMLA, but the audit firm may be criminally liable under Art. 305bis in conjunction with Art. 25 SCC). Even if the audit firm makes the report, the dealer may still be liable to prosecution, especially if the report was not made "promptly" within the meaning of Art. 9 para. 1bis AMLA.

14 If an audit firm makes a report in good faith within the meaning of Art. 15 para. 5 AMLA, it shall not be held liable under Art. 11 para. 1 and 2 let. b AMLA under either criminal or civil law (**exclusion of criminal liability and liability**). The prohibition on tipping off also applies to the auditors in accordance with Art. 10*a*, para. 5 AMLA.

VII. LEGAL CONSEQUENCES OF VIOLATING THE AUDIT REQUIREMENT

15 Dealers who accept more than CHF 100,000 in cash as part of a commercial transaction without commissioning an audit firm to audit compliance with the

due diligence and reporting requirements are subject to prosecution under Art. 38 AMLA. The offense begins and is simultaneously completed as soon as the audit firm should have been commissioned in accordance with Art. 15 AMLA in order to ensure a proper and timely audit. Regarding the criminal liability and other possible consequences of a violation of Art. 15 AMLA, please refer to the commentary on Art. 38 AMLA.

BIBLIOGRAPHY

Burckhardt Peter/Hösli Andreas, Neue strafrechtliche Risiken für Händler bei Barzahlungen über CHF 100‘000, in: Jusletter vom 1.2.2016 (zit. Burckhardt/Hösli, Jusletter 1.2.2016).

Hagi Andreas Lukas/Tschabold Stephan, Kommentierung zu Art. 15, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar zum Geldwäschereigesetz (GwG), Bundesgesetz vom 10.10.1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Bern 2017 (zit. SHK-Hagi/Tschabold, Art. 15 GwG).

Nagel Thomas, Der persönliche und sachliche Geltungsbereich des schweizerischen Geldwäschereigesetzes: Mit rechtsvergleichenden Hinweisen zu internationalen Standards, dem Recht der Europäischen Union und dem deutschen Recht, Zürich et al. 2020 (zit. Nagel).

Ramelet Nicolas, Kommentierung zu Art. 15, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz, Basel 2021 (zit. BSK-Ramelet, Art. 15 GwG).

Wyss Ralph, Kommentierung zu Art. 15, in: Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Geldwäschereigesetz mit weiteren Erlassen (GwG), 3. Aufl., Zürich 2019 (zit. OFK-Wyss, Art. 15 GwG).

MATERIALS

Botschaft zur Änderung des Geldwäschereigesetzes vom 26.6.2019, BBl 2019 5451 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2019/1932/de, besucht am 31.8.2024 (zit. Botschaft GwG 2019).

Erläuterungsbericht zur Geldwäschereiverordnung (GwV) – Umsetzung der GAFI-Empfehlungen vom 11.11.2015, abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/41723.pdf, besucht am 31.8.2024 (zit. Erläuterungsbericht GwV 2015).

EXPERTsuisse, Ausgewählte Fragen und Antworten zu den Auswirkungen der Anpassungen des Geldwäschereigesetzes auf die Prüfung von Händlerinnen und Händlern, 23.6.2016 (zit. EXPERTsuisse).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 20 AMLA

A commentary by Marc Mauerhofer / Tabea Oberhänsli

SUGGESTED CITATION

Marc Mauerhofer/Tabea Oberhänsli, Commentary of art. 20 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Mauerhofer/Oberhänsli, art. 20 AMLA N. XXX.

Art. 20 Activity without affiliation to a self-regulatory organisation

[1] FINMA may take supervisory action in accordance with Articles 29 to 37 of the FINMASA against financial intermediaries who fail to comply with the duty to be affiliated to a recognised self-regulatory organisation in accordance with Article 14 paragraph 1.

[2] It may order the liquidation of legal entities and general and limited partnerships, and the deletion of sole proprietorships from the commercial register.

CONTENT

I. Introduction 397
A. Background 397
B. Purpose 397
C. International standard and division of responsibilities in Switzerland 398
II. Reference to the supervisory instruments under Art. 29–37 FINMASA (para. 1) .. 398
A. Registered financial intermediaries 398
B. Use of supervisory instruments against AMLA violations 399
1. As part of preliminary clarifications 399
2. In enforcement proceedings 400
3. After enforcement proceedings 403
III. Order of dissolution or deletion from the commercial register (para. 2) 403
A. (Complete) liquidation vs. partial liquidation 403
B. Supervisory liquidation vs. bankruptcy 404
C. Waiver of liquidation 405
Bibliography 406
Materials 408

I. INTRODUCTION

A. Background

Until the FinIA and the FinSA came into force on January 1, 2020, financial intermediaries within the meaning of Article 2, para. 3 AMLA had the choice of joining a recognized self-regulatory organization or obtaining a license from FINMA to carry out their activities (Article 14 of the old AMLA). Financial intermediaries that opted for the latter were directly supervised by FINMA (directly subordinated financial intermediaries, so-called DSFI). With the **entry into force** of the FinIA and the FinSA, the DSFI status was abolished. Art. 20 of the old AMLA, which regulated the consequences of the withdrawal of a license, was also repealed. The previous option of either joining a recognized self-regulatory organization or being directly supervised by FINMA was replaced by the obligation to join a recognized self-regulatory organization (Art. 14 para. 1 AMLA). 1

In contrast to financial intermediaries under other financial market laws, who require a license from FINMA to carry out their activities, financial intermediaries under Art. 2 para. 3 AMLA are not supervised entities within the meaning of Art. 3 FINMASA. Article 20 AMLA, which has been in force since January 1, 2023, therefore expressly states that FINMA may take the **supervisory measures** provided for in FINMASA against financial intermediaries in accordance with Article 2 para. 3 AMLA who violate their duty to join a recognized self-regulatory organization in accordance with Article 14 para. 1 AMLA. This makes it clear that even after the abolition of DSFI status, FINMA still has the authority to take action against financial intermediaries that do not require a license from FINMA but operate without being affiliated to a self-regulatory organization as required by supervisory law. 2

B. Purpose

The supervisory instruments applicable under Article 20 AMLA supplement Article 44 FINMASA, which makes the unauthorized practice of an activity on the financial markets a criminal offense. By enabling FINMA to take supervisory measures under FINMASA against financial intermediaries within the meaning of Article 2 para. 3 AMLA, the proper state of affairs should be restored and a level playing field ensured in the financial markets. Art. 20 AMLA 3

thus ensures that unlicensed financial intermediaries can be **effectively prosecuted**, even if they are not supervised persons or entities in accordance with Art. 3 FINMASA.

C. International standard and division of responsibilities in Switzerland

4 The **FATF Recommendations** require that state authorities take action against providers of money or value transfer services (MVTS) that operate without a license: "Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions." The relevant finance ministries or supervisory authorities therefore have corresponding powers in many countries.

5 The solution chosen by **Switzerland** is in line with the international standard. On the one hand, FINMA, as the supervisory authority, takes action under supervisory law against unauthorized providers based on Article 20 of the AMLA. This approach aims to restore compliance and prevent the risk of recurrence. For example, unauthorized providers are to cease their activities (Art. 31 FINMASA) or be liquidated (Art. 20 para. 2 AMLA), and the public is to be warned about unauthorized providers (Art. 34 FINMASA). Since operating without a license or without being affiliated to a self-regulatory organization also constitutes a criminal offense under Article 44 FINMASA, FINMA files a criminal complaint at the end of its investigation or proceedings (Art. 38 para. 3 FINMASA). The Federal Department of Finance (FDF) is the prosecuting authority in such cases (Art. 50 FINMASA). The FDF then conducts administrative penalty proceedings. Thus, in addition to the procedure under supervisory law, the responsible persons are also penalized for the past unauthorized activity in order to prevent and restore the proper state of affairs.

II. REFERENCE TO THE SUPERVISORY INSTRUMENTS UNDER ART. 29–37 FINMASA (PARA. 1)

A. Registered financial intermediaries

6 The provision of Article 20 AMLA applies to **financial intermediaries** who violate the duty to join a recognized self-regulatory organization in accordance with Article 14, para. 1 AMLA. Article 14, para. 1 AMLA refers in this re-

gard to Article 2, para. 3 AMLA. The provision thus applies to persons who, on a professional basis, accept or hold assets belonging to third parties or assist in the investment or transfer of such assets without the required SRO affiliation.

In practice, payment service providers, e.g. persons who carry out money transfers for third parties, such as operators of a local payment system or a hawala system, as well as debt reschedulers, are likely to be included as typical **examples of** this. It also includes payment instrument issuers, e.g. issuers of payment tokens in an ICO or issuers of local currencies. Other examples could be creditors who exceed the professional threshold, commodity dealers acting on behalf of third parties or money changers. 7

The scope of application of Art. 20 AMLA **does not include** other persons to whom the Anti-Money Laundering Act applies. In particular, Art. 20 AMLA does not apply to dealers in accordance with Art. 2 para. 1 let. b AMLA. It also does not apply to advisors who may be subject to an SRO affiliation requirement in the future. Financial intermediaries as defined in Art. 2 para. 2 AMLA are also excluded, i.e. in particular all those subject to prudential supervision. However, an analogous provision applies to these in the relevant financial market law. 8

B. Use of supervisory instruments against AMLA violations

1. As part of preliminary clarifications

According to the wording of Article 31 FINMASA, FINMA is obliged to restore compliance with the law if someone "violates" financial market legislation, e.g. carries out an activity requiring a license without the appropriate license. As long as there is insufficient evidence, FINMA may deploy its resources in a needs- and risk-oriented manner within the framework of general constitutional and administrative principles and the **principle of discretion**. It can further investigate such suspicious circumstances in (preliminary) clarifications. 9

Clarification is an informal administrative act, i.e. the rights and obligations of the Administrative Procedure Act, in particular the right to inspect files or the obligation to bear costs, do not apply. However, the **duty to provide information and report** under Article 29 FINMASA already applies, since FINMA 10

can also use the supervisory instruments against persons whose subordination requirement is still disputed. The option of demanding information about their business activities from persons who may be subject to an SRO affiliation requirement enables FINMA to investigate the suspicion in the first place. Anyone who refuses to provide information despite suspicion of unlawful activity risks being placed on the public FINMA warning list in accordance with Article 22 para. 2 FINMASA.

11 If the suspicions are confirmed but the **restoration of** compliance with the law pursuant to Article 31 FINMASA is achieved during the investigation, FINMA may decide not to initiate proceedings. In practice, these cases are by far the most common and require the cooperation of the party concerned: For example, the proper state of affairs can be restored by the financial intermediary joining a self-regulatory organization or permanently and credibly ceasing the activity requiring authorization. However, this restoration of the proper state of affairs does not alter the fact that the previous activity was carried out without a license or without affiliation to a self-regulatory organization, which is punishable under Article 44 FINMASA.

2. In enforcement proceedings

12 Under Article 30 FINMASA, FINMA is entitled to **open formal** proceedings if there are indications of a violation of supervisory law. It will do so if the proper state of affairs cannot be restored in the clarifications or if a serious violation has occurred (in particular with high levels of assets involved or with numerous clients).

13 The restoration of compliance with the law pursuant to Article 31 FINMASA can also take place as part of enforcement proceedings rather than as part of the clarifications (see above N. 9 ff.). In such cases, FINMA can order the cessation of the activity. It usually does this with respect to the natural persons involved or responsible, while such an order only makes sense with respect to a legal entity if it is not liquidated at the same time (see below N. 18). This **cease-and-desist order** is often combined with a penalty under Art. 48 FINMASA.

14 Finally, it is also conceivable that the party itself restores compliance during the proceedings, for example by permanently and credibly ceasing the activity only at this stage. In such situations, FINMA can issue a **declaratory ruling**

pursuant to Art. 32 FINMASA. However, mere declaratory rulings are rare after an unlicensed activity, since an injunction (see above N. 13) is practically always necessary to prevent repetition.

15 If there has been a serious breach of supervisory provisions, which is generally to be assumed in the case of unauthorized activities, FINMA may publish its ruling in accordance with Article 34 FINMASA. The **publication of** a ruling in accordance with the wording of the law takes place after it has become legally enforceable (i.e. the suspension of the suspensive effect is not permitted). It may contain personal data and is to be ordered in the ruling itself. In practice, the instrument of publication is used almost exclusively for proceedings against natural persons who have themselves acted unlawfully or who are responsible for the unlawful actions of a legal entity. Typically, it is not the entire order that is published, but only the operative part of the cease-and-desist order (see above, N. 13), with a time limit being set for the publication. The purpose of the publication is to warn against this person. This should also enable contractual partners, such as banks when opening an account, to recognize that this person has already been involved in unauthorized activities. Such publication is to be distinguished from publications under Art. 22 FINMASA: If there are reasons under Art. 22 FINMASA, i.e. in particular a public interest, FINMA may inform the public outside of an injunction. Publication under Art. 34 FINMASA and publication under Art. 22 FINMASA occur at different points in time: While publication under Art. 34 FINMASA may only occur after the ruling has become legally enforceable, publication under Art. 22 FINMASA is not tied to any particular point in time and usually occurs shortly after the conclusion of proceedings. Occasionally, FINMA has combined publication and disclosure, which is permissible if the requirements of both provisions are met.

16 Pursuant to Art. 35 FINMASA, FINMA may **confiscate the profits made** by a supervised person or entity or a responsible person in a managerial position as a result of a serious violation of supervisory law. This provision can in principle be used in enforcement proceedings against unlicensed persons. If a person not authorized under the AMLA would have been able to join an SRO, then the (small) saving on the SRO affiliation fee is the only profit that can be causally attributed to the violation of supervisory law. If the AMLA violator is not eligible for a license, however, e.g. because he was involved in a fraud-like construct, the profits from the business activity can also be confiscated. One

possibility in the case of legal entities is therefore to order the liquidation under supervisory law (see below N. 18) and to order the confiscation of profits in the event of and in the amount of the liquidation surplus. In the case of responsible persons in a managerial position, the confiscation can be up to the amount of the salary or other remuneration received. However, here too it must be determined whether the unlawful gain is limited to the savings made by joining the SRO. Finally, the confiscation of profits must remain proportionate, which, according to the Federal Council Dispatch, could be the case if it would lead to (private) bankruptcy. In published practice, the confiscation of profits from unlicensed individuals has so far been the exception.

17 Due to the general reference to the supervisory measures of the FINMASA in Article 20 AMLA, **professional and activity bans** under Article 33 and 33*a* FINMASA against individuals who are responsible for an unlicensed activity are also possible. However, there are no known cases of this in published practice. This is probably because people operating without a license often have little chance of finding a new job in the licensed sector. These prospects are further diminished by any publication in accordance with Art. 34 FINMASA (see above N. 15).

18 Finally, the reference in Article 20 para. 1 AMLA also includes the provision of Article 37 FINMASA. This allows FINMA to order the **liquidation** of unlicensed actors under supervisory law. This is explained in more detail in para. 2 of Article 20 AMLA (see the comments below N. 22 et seq.).

19 The measures described here can, in principle, be **combined.** However, it must always be checked whether the overall proportionality is maintained.

20 As part of the proceedings, FINMA can appoint an **investigating agent**. In accordance with Art. 36 FINMASA, it can determine that the investigating agent should act in place of the governing bodies of a company. The appointment of an investigating agent is therefore an effective instrument, particularly in the case of unlicensed actors, which allows control over a business activity to be taken despite the lack of coercive measures in administrative proceedings. The provision can also be applied analogously to a sole proprietorship. FINMA will make use of the instrument of the investigating agent in particular when an assessment of a possible unauthorized activity requires an in-depth investigation of the facts or when the funds at hand are to be secured by means of the investigating agent's position. The appointment of the investigat-

ing officers is a precautionary measure that often takes place superprovisionally, i.e. without hearing the affected party. If the investigating officer determines during their work that the company is over-indebted and they have been appointed as an organ, they submit the notice of over-indebtedness to the competent civil court in accordance with Art. 725*b* para. 3 CO. Once bankruptcy proceedings have been initiated, the enforcement proceedings continue, with the bankruptcy taking precedence over a liquidation under supervisory law by FINMA in accordance with Article 37 FINMASA.

3. After enforcement proceedings

21 After the enforcement proceedings have been legally concluded, FINMA **enforces the** measures ordered in accordance with Article 32 para. 2 FINMASA in conjunction with Article 39 APA. For the typical measures for unauthorized actors, it can carry out the enforcement actions directly: for example, it publishes relevant excerpts from the order or begins the liquidation (see also N. 25). The enforcement of the confiscation of profits takes place, if necessary, by way of SchKG. Finally, a cease-and-desist order (see above N. 13) cannot be enforced in the strict sense: if it is violated and it was issued under threat of a penalty pursuant to Art. 48 FINMASA, FINMA will file a criminal complaint with the FDF and may again open enforcement proceedings (and, if necessary, order more severe measures than in the first proceedings).

III. ORDER OF DISSOLUTION OR DELETION FROM THE COMMERCIAL REGISTER (PARA. 2)

A. (Complete) liquidation vs. partial liquidation

22 Art. 20 para. 2 AMLA stipulates that FINMA can order the dissolution of legal entities and general and limited partnerships and the deletion of sole proprietorships from the commercial register. Art. 20 para. 2 AMLA provides an explicit legal basis for the **most serious measure** FINMA can take in the event of a violation of the affiliation requirement under Art. 14 para. 1 AMLA. Before FINMA orders the dissolution or deletion in the commercial register, it must, in application of the principle of proportionality (Art. 5 para. 2 FC), examine whether the restoration of the proper state of affairs can be achieved by less drastic measures (see above N. 9 et seq.). Dissolution or deletion in the commercial register is the ultima ratio.

23 If it is not possible to restore the proper state of affairs, e.g. because the unlicensed financial intermediary does not permanently and credibly cease its activities, behaves uncooperatively and refuses to join a recognized self-regulatory organization or cannot join one because it does not meet the requirements of Art. 14 para. 2 AMLA, FINMA orders the **dissolution of** or deletion from the commercial register. In particular, FINMA is not required to give the unauthorized financial intermediary the opportunity to convert the unauthorized activity into an activity that is unobjectionable under financial market law in order to avert liquidation.

24 If liquidation is the consequence of the violation of the affiliation requirement, FINMA must regulate the **scope of** the liquidation by means of a ruling. In this context, the principle of proportionality requires that the liquidation does not exceed what is necessary to restore compliance with the law. This means that in cases in which the financial intermediary also carries out an activity that is unobjectionable under financial market law in addition to the unlawful activity, only the part relating to the unlawful activity needs to be liquidated. However, a partial liquidation is only possible under the following conditions: on the one hand, the partial liquidation must be technically possible. On the other hand, it must be possible to carry out the activity that is unobjectionable under financial market law independently. Furthermore, no financial resources that cannot be distinguished in accounting terms and that were generated by the unauthorized activity may have flowed into the activity that is unobjectionable under financial market law. Finally, it must be possible to assume that there will be no relevant risk of the unauthorized activity being carried out again in the future. If no positive prognosis can be made, which is usually the case in practice with less than reputable business models, a full liquidation is unavoidable.

B. Supervisory liquidation vs. bankruptcy

25 FINMA itself carries out a supervisory liquidation that has been ordered or – which is more usual in practice – appoints a **liquidator** for this purpose. If an over-indebtedness situation already exists during the proceedings, the investigating agent appointed by FINMA as an official can file a notice of over-indebtedness with the competent civil court (see above N. 20). However, if no bankruptcy proceedings are initiated during the proceedings and FINMA subsequently orders the liquidation under supervisory law, it is conceivable that

an over-indebtedness situation may arise after the liquidation has been opened. In this case, the liquidator appointed by FINMA can submit the over-indebtedness report to the competent civil court, which is responsible for opening bankruptcy proceedings and liquidation in the case of financial market participants operating without a license (Art. 173*b* para. 2 SchKG). If the unlicensed financial intermediary is a sole proprietorship, FINMA may order its deletion from the commercial register in accordance with Article 20 para. 2 AMLA. This order also results in a liquidation under supervisory law. However, it cannot lead to (private) bankruptcy.

C. Waiver of liquidation

26 According to the Federal Supreme Court's case law on Art. 37 para. 2 and 3 FINMASA in conjunction with the relevant financial market law (e.g. Art. 23^{quinquies} para. 1 BankG), liquidation is in principle the **mandatory and only legal consequence** of an activity carried out without a license in the financial markets. As the authority applying the law, FINMA has no discretion in choosing the legal consequence. However, it must apply the principle of proportionality and regulate the extent of the liquidation by order (see above N. 24) or, if necessary, waive the liquidation (see below N. 27 f.).

27 The wording of individual provisions in the financial market laws already indicates that FINMA has discretion in deciding whether liquidation is to be carried out. In the area of collective investment schemes, for example, the provision of Article 134 CISA is formulated as an "optional" provision. In contrast, Art. 23^{quinquies} para. 1 BankG, Art. 52 VAG, Art. 66 para. 1 FinIA and Art. 87 para. 2 FinMIA, which also regulate the consequences of the withdrawal of a license, are not formulated as "optional" provisions. However, the Federal Supreme Court has already teleologically reduced Art. 20 AACA, which provided for dissolution or deletion from the commercial register as a consequence of the withdrawal of the DSFI license by FINMA, to the effect that **no liquidation** is carried out if the company or sole proprietorship does not engage in any financial intermediary activities or only to a limited extent. This interpretation corresponds to the original version of this provision from 1998, which expressly stipulated that the legal consequence of liquidation would only apply if the company or sole proprietorship "predominantly acts as a financial intermediary". The idea behind this proviso was to take into account the principle of proportionality. The Federal Court justified the teleological

reduction of Art. 20 aGwG by stating that there were no indications in the materials as to why this reservation had been deleted, and that it should not be readily assumed that the reformulation of this provision is intended to displace the principle of proportionality as a formative principle of the Swiss constitutional order. (

28 Like Art. 134 CISA, Art. 20 para. 2 AMLA is currently formulated as a **"discretionary" provision**. Violation of the requirement to affiliate with a recognized self-regulatory organization therefore does not necessarily have to lead to dissolution or deletion from the commercial register and liquidation. Rather, the wording of Art. 20 para. 2 AMLA explicitly leaves room for considerations of proportionality. FINMA may thus refrain from liquidation in individual cases. According to the case law on Art. 20 aGwG (see above N. 27), a waiver of liquidation for reasons of proportionality is possible if the company or sole proprietorship has only carried out a minor financial intermediary activity. However, cases in which liquidation is waived for reasons of proportionality are rare in practice.

In this article, the authors express only their personal views.

BIBLIOGRAPHY

Amez-Droz Laura, Finanzmarktenforcement und Kommunikation: Zum Kommunikationsverhalten der FINMA hinsichtlich einzelner Enforcementverfahren, SZW 2024, S. 188–207.

Ammann Fritz, Verwaltungsstrafverfahren des Finanzdepartements, in: Zulauf Urs/Wyss David (Hrsg.), Finanzmarktenforcement, 3. Aufl., Bern 2022, S. 625–674.

Bertschinger Urs, Das Finanzmarktaufsichtsrecht vom vierten Quartal 2015 bis ins vierte Quartal 2016, SZW 2016, S. 620–639 (zit. Bertschinger, Finanzmarktaufsichtsrecht).

Bertschinger Urs, Zur Abwicklung unbewilligter Finanzaktivitäten, SZW 2013, S. 519–528 (zit. Bertschinger, Abwicklung).

Brunnhofer Michaela/Leimgruber Dominik, Kommentierung zu Art. 20 GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar, Geldwäschereigesetz, Bern 2017.

Emmenegger Susan, Zulässigkeit eines SRO-Anschlusszwangs für Finanzintermediäre im Sinne von Art. 2 Abs. 3 GwG, Rechtsgutachten zuhanden des Eidg. Finanzdepartements, Bern 2013.

Eymann Patric, Eröffnung des Verfahrens und Kriterien dazu, in: Zulauf Urs/Wyss David (Hrsg.), Finanzmarktenforcement, 3. Aufl., Bern 2022, S. 105–107.

Friedmann Oliver/Kuhn Christoph/Schönknecht Florian, Enforcement, in: Sester Peter/Brändli Beat/Bartholet Oliver/Schiltknecht Reto (Hrsg.), Finanzmarktaufsicht und Finanzmarktinfrastrukturen, Zürich et al. 2018, S. 469–510.

Frigo Patrick/Jain Vivien, Kommentierung zu Art. 14 GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Grodecki Stéphane, Kommentierung zu Art. 20 GwG, in: Cassani Ursula/Bovet Christian/Villard Katia (Hrsg.), Commentaire Romand, Loi sur le blanchiment d'argent, Basel 2022.

Hsu Peter Ch./Bahar Rashid/Flühmann Daniel, Kommentierung zu Art. 34 FINMAG, in: Watter Rolf/Vogt Nedim Peter (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

Kuhn Christoph, Massnahmen der FINMA, in: Zulauf Urs/Wyss David (Hrsg.), Finanzmarktenforcement, 3. Aufl., Bern 2022, S. 351–420.

Maurenbrecher Benedikt/Terlinden André, Kommentierung zu Art. 36 FINMAG, in: Watter Rolf/Vogt Nedim Peter (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

Meyer Patrick K./Ryhner Samuel, Kommentierung zu Art. 134 KAG, in: Bösch René/Rayroux François/Winzeler Christoph/Stupp Eric (Hrsg.), Basler Kommentar, Kollektivanlagengesetz, 2. Aufl., Basel 2016.

Roth Pellanda Katja/Kopp Lara, Kommentierung zu Art. 31 und 37 FINMAG, in: Watter Rolf/Bahar Rashid (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

Schönknecht Florian, Vorabklärungen im FINMA-Enforcement, in: Zulauf Urs/Wyss David (Hrsg.), Finanzmarktenforcement, 3. Aufl., Bern 2022, S. 65–92.

Truffer Roland, Kommentierung zu Art. 29 FINMAG, in: Watter Rolf/Vogt Nedim Peter (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

MATERIALS

Botschaft zum Bundesgesetz über die Eidgenössische Finanzmarktaufsicht vom 1.2.2006, BBl 2006 2829 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2006/303/de, besucht am 22.12.2024 (zit. Botschaft FINMAG 2006).

Botschaft zur Änderung des Geldwäschereigesetzes vom 26.6.2019, BBl 2019 5451 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2019/1932/de, besucht am 22.12.2024 (zit. Botschaft GwG 2019).

FATF Recommendations, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF 2012, letztmals aktualisiert im November 2023, www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html, besucht am 22.12.2024.

Jahresbericht 2019, FINMA 2019, https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/geschaeftsbericht/20200402_finma_jahresbericht_2019.pdf, besucht am 22.12.2024 (zit. FINMA, Jahresbericht 2019).

Leitlinien zum Enforcement, FINMA 2014, https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/3durchsetzung/leitlinien-zum-enforcement.pdf, besucht am 22.12.2024.

Mutual Evaluation Report Singapore, Anti-money laundering and counter-terrorist financing measures, FATF 2016, https://www.fatf-gafi.org/en/publications/mutualevaluations/documents/mer-singapore-2016.html, besucht am 22.12.2024.

Mutual Evaluation Report Switzerland, Anti-money laundering and counter-terrorist financing measures, FATF 2016, www.fatf-gafi.org/publications/mutualevaluations/documents/mer-switzerland-2016.html, besucht am 22.12.2024.

Mutual Evaluation Report United Kingdom, Anti-money laundering and counter-terrorist financing measures, FATF 2018, https://www.fatf-gafi.org/en/

publications/mutualevaluations/documents/mer-united-kingdom-2018.html, besucht am 22.12.2024.

Mutual Evaluation Report United States, Anti-money laundering and counter-terrorist financing measures, FATF 2016, https://www.fatf-gafi.org/en/publications/mutualevaluations/documents/mer-united-states-2016.html, besucht am 22.12.2024.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 23 AMLA

A commentary by Anton Brönnimann

SUGGESTED CITATION

Anton Brönnimann, Commentary of art. 23 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Brönnimann, art. 23 AMLA N. XXX.

Section 4 Money Laundering Reporting Office Switzerland (the Reporting Office)

Art. 23

[1] The Federal Office of Police shall manage the Money Laundering Reporting Office Switzerland (the Reporting Office).

[2] The Reporting Office shall examine and analyse the reports received. If necessary, it shall obtain additional information in accordance with Article 11*a*.

[3] It shall maintain its own information system to combat money laundering and its predicate offences, organised crime and terrorist financing.

[4] It must notify the responsible prosecution authority immediately if it has reasonable grounds to suspect that:

a. an offence as defined in Articles 260ter Number 1, 305bis or 305ter SCC has been committed;

b. assets are the proceeds of a felony or an aggravated tax misdemeanour under Article 305bis number 1bis SCC;

c. assets are subject to the power of disposal of a criminal or terrorist organisation; or

d. assets serve the financing of terrorism (Art. 260^{quinquies} para. 1 SCC).

[5] If it transmits the information reported by a financial intermediary under Article 9 paragraph 1 letter a of this Act or under Article 305ter paragraph 2 of the SCC to a prosecution authority, it shall inform the financial intermediary thereof, provided the financial intermediary has not terminated the business relationship in accordance with Article 9*b*.

[6] ....

CONTENT

I. Introduction 414
II. Influence of international requirements 415
A. General 415
B. FATF Recommendation 29 – Financial Intelligence Unit 416
C. Membership in the Egmont Group and compliance with the Egmont Principles 417
D. Relationship between soft law and national law 417
III. Content of the regulation 419
A. Organization – The Reporting Office as part of fedpol (para. 1) 419
1. Integration of the Reporting Office in fedpol 419
2. Implementation of international requirements in national law 422
B. Analysis of suspicious activity reports – "Intelligence" (para. 2) 422
1. Principle 422
2. Analytical tools – MROS toolbox 424
a. Information from financial intermediaries 425
b. Access to police and judicial databases 426
c. Information from international administrative assistance 426
d. Information from national administrative assistance 427
e. OSINT and other information sources 428
3. Risk-based approach 428
C. Information system (para. 3) 429
1. Use of the software application "goAML" 429
2. Processing principles 430
D. Reporting to the law enforcement agencies (para. 4) 431
E. Notification of the financial intermediary (para. 5) 432
Bibliography 434
Materials 435

I. INTRODUCTION

1 The Money Laundering Reporting Office Switzerland MROS (hereafter: "Reporting Office" or "MROS") is the central reporting office for suspected cases of money laundering and terrorist financing in Switzerland and performs the duties of a **Financial Intelligence Unit (FIU)**. FIU is the internationally accepted term for government agencies that are responsible for investigating financial transactions in the fight against money laundering and terrorist financing. The reporting office plays an important role in the fight against crime – it tracks down incriminated assets and follows the principle of "follow the money". In doing so, it makes a significant contribution to the credibility of Switzerland's anti-money laundering system and thus also protects the reputation of the Swiss financial center.

2 The **tasks and competencies** of MROS are derived from the Anti-Money Laundering Act (AMLA), the Ordinance on the Money Laundering Reporting Office Switzerland (MROSO), the MROS/fedpol internal regulations, the international recommendations of the Financial Action Task Force (FATF) and the obligations to the Egmont Group. Accordingly, MROS's core tasks include: (1) **"Intelligence":** MROS receives reports from financial intermediaries and other persons subject to the AMLA, which are filed in accordance with the Anti-Money Laundering Act and the Swiss Criminal Code. MROS adds further information and conducts its own analysis. MROS then decides in each individual case whether or not the information obtained should be forwarded to a law enforcement agency in the form of a criminal complaint. (2) **"Cooperation":** MROS exchanges information with other national authorities and with foreign FIUs in the context of mutual administrative assistance in operational and strategic matters. (3) **"Prevention":** MROS contributes to the assessment of the national risks of money laundering and terrorist financing. It conducts strategic analysis (identification of patterns and trends) and shares the knowledge gained with authorities, the financial industry and the public.

3 Art. 23 AMLA forms the **legal basis** of MROS. It addresses the principles of organization, analysis of suspicious activity reports, and the conditions for reporting and sharing information with law enforcement authorities. However, Art. 23 cannot be viewed in isolation – it is closely linked to Art. 9, 11a, 29–32, 35 and 35a AMLA, as well as the international recommendations of the FATF and the principles of the Egmont Group. At least the core of Article 23 AMLA

has not been revised in the past 25 years – in some cases, however, international and technical developments have rendered its wording obsolete. The practice followed by the reporting office and the interpretation of the applicable period of Article 23 AMLA are therefore of central importance.

II. INFLUENCE OF INTERNATIONAL REQUIREMENTS

A. General

The national system for combating money laundering is heavily influenced by **international standards**. Switzerland is a member of the Financial Action Task Force (FATF), which was founded in 1989. The FATF is the most important international body for combating and preventing money laundering, terrorist financing and proliferation financing. It sets standards in this area – a total of 40 recommendations define uniform rules of conduct and benchmarks that apply to the entire financial sector and to all persons and professional groups involved. The FATF regularly adopts various interpretative documents, in particular guidance and best practice papers. The FATF promotes the worldwide dissemination of these standards and reviews their implementation in its member states. 4

The World Bank, the International Monetary Fund and the UN Security Council have recognized the FATF recommendations as international standards, although they are not directly binding and thus only have the status of soft law. More than 180 countries worldwide have committed to adopting the FATF recommendations. 5

In order to comply with the changes in the standard, the AMLA has been fundamentally revised several times over the past 25 years. MROS has also been significantly affected by such **amendments,** especially since various recommendations, mainly Recommendation 29, but also Recommendations 1 (risk assessment), 2 (national cooperation and coordination), 20 and 23 (suspicious activity reports), 31 (prosecution and investigation authorities), 33 (keeping statistics) and 40 (international cooperation), deal with deal with the role and activities of the FIU or refer to them directly or indirectly. 6

B. FATF Recommendation 29 – Financial Intelligence Unit

7 FATF Recommendation 29 deals exclusively with the **function of the FIU** and is expressed in the Interpretative Note on the organization and scope of tasks and their performance. The FATF standard requires that each country has a central reporting office for suspicious activity reports – a Financial Intelligence Unit (FIU). The FIU is responsible at the national level for receiving and analyzing suspicious activity reports regarding money laundering, its predicate offenses and terrorist financing. It forwards its findings from the analysis to the competent authorities, either spontaneously or upon request.

8 To **fulfill its tasks**, an FIU must be able to obtain additional information from the reporting bodies. It should also have access to relevant information from the authorities (public prosecutor, police, supervisory authorities, other administrative authorities, etc.), which should be as direct and comprehensive as possible. It should also have access to public sources and, if necessary, to commercially available databases.

9 A FIU must also be operationally **autonomous**, i.e. it must be able to act independently and without instructions in its core activities – receiving reports, prioritizing and triaging, gathering information, analyzing and using the results of the analysis, managing data, forwarding and exchanging information, and cooperating with other authorities. An essential feature of autonomy is that the FIU is provided with adequate financial, human and technical resources to enable it to carry out its tasks. Operational independence does not mean that an FIU must necessarily be an independent authority. It can be part of an already existing authority – but in this case it must be ensured that the core tasks of the FIU are separate from those of the other authority. The same also applies to the handling of data. The FIU must ensure that the security of the data received is guaranteed and that only FIU employees can access the corresponding data processing systems and IT applications.

10 Finally, FATF Recommendation 29 also requires that the FIU apply the Egmont Group's principles for international information sharing. The FATF standard thus effectively requires the FIU to maintain **permanent membership** in the Egmont Group.

C. Membership in the Egmont Group and compliance with the Egmont Principles

Since 1998, MROS has been a member of the Egmont Group, which was founded in 1995 and currently brings together 177 FIUs worldwide. This organization enables the international, secure, rapid and legally permissible **exchange of information** in the fight against money laundering. Membership of the Egmont Group is essential for a financial center the size and importance of Switzerland's, and there is no alternative. Admission and continued membership are subject to strict qualification criteria. Membership provides a FIU with a kind of quality seal and guarantees a secure and standardized exchange of information at the international level. Membership is now also part of the FATF standards. Furthermore, certain FIUs are only willing to exchange information via the Egmont Secure Web – a secure electronic information system – which requires membership of the Egmont Group. 11

In 2018, the Egmont Group published a document entitled *'Understanding FIU Operational Independence and Autonomy'*. The characteristics of an independent FIU are described in chapter 6. In essence, the Egmont Group's requirements regarding operational autonomy go further than FATF Recommendation 29. In particular, the Egmont Standard requires the FIU to be physically separate from other state authorities. There are also more restrictive rules on the appointment of staff, budget authority and the ability to travel on official business, which should be decided at FIU level. Likewise, the appointment and dismissal of the head of the FIU is subject to special criteria that do not necessarily correspond to the personnel law requirements of the respective jurisdiction. The Egmont Group provides a checklist with the relevant criteria for self-assessment of operational independence and autonomy. 12

FIUs that no longer sufficiently comply with and/or violate the constantly evolving principles of the Egmont Group are subject to a so-called **non-compliance procedure** due to non-compliance with the principles, which, if the identified deficits are not remedied, provides for warnings, suspensions and, as a last resort, exclusion from the Egmont Group. 13

D. Relationship between soft law and national law

Soft law is characterized by the fact that it does not originate from one of the formal sources of international law mentioned in Art. 38 of the ICJ Statute and 14

is therefore not legally binding. Rather, it is **legal support or legal supplement**. The non-binding nature of soft law means that its disregard does not trigger any international legal responsibility on the part of the state concerned and that reprisals are inadmissible under international law. Meanwhile, retorsions or listings remain permitted. Manifestations of soft law can be, for example, resolutions, declarations, recommendations and codes of conduct of international organizations, standards, best practice, principles and legally non-binding agreements (e.g. memorandum of understanding). One important indication of the existence of soft law is the existence of a monitoring procedure (so-called follow-up procedures) for compliance with the requirements contained in the relevant set of rules.

15 The FATF is not an international organization in the sense of public international law, but a purely political body, which is why its recommendations and publications have no direct binding effect on the participating states and thus only represent "soft law". However, the FATF and its member states clearly expect their recommendations to be followed. The FATF ensures that its recommendations are taken seriously and adhered to by means of annual self-assessments by member countries and periodic mutual evaluations by assessors from other member states. Three times a year, the **FATF publishes lists** of countries that show strategic deficits in the fight against money laundering and terrorist financing or do not comply with the recommendations. The so-called "blacklist" includes all jurisdictions that pose a risk to the international financial system and also hamper or even prevent international efforts in the fight against money laundering and terrorist financing. Meanwhile, all those jurisdictions that have not made sufficient progress in remedying the deficits or have not committed to a plan of action developed jointly with the FATF are placed on the so-called "gray list".

16 Being on the blacklist has no direct consequences for the country in question – the FATF cannot impose any immediate harsh measures. However, it calls on its member states and other jurisdictions to take **countermeasures** against these countries in order to protect the international financial system from the risks of money laundering and terrorist financing. With regard to the countries on the gray list, the FATF calls on its member states to take into account the risks posed by the identified deficiencies. These calls are enshrined in FATF Recommendation 19, and are thus part of the FATF standard and therefore

subject to regular review by the FATF. With its own recommendation, the FATF has a strong means of coercion to force member countries to comply.

The FATF's "sanction system" is based on the principle of **"naming and shaming"**. Those who do not comply with the FATF recommendations are pilloried and have to expect countermeasures or harassment from the other member states. The same applies to the Egmont Group. Non-compliance with the Egmont Principles can lead to exclusion from the Egmont Group, which also affects FATF Recommendation 29, i.e. there is a violation of the FATF standard. 17

Switzerland is one of the world's leading financial centers. The financial sector accounts for one-seventh of Switzerland's gross value added. Around ten percent of all jobs in Switzerland are directly or indirectly dependent on the financial sector. The Swiss financial center is an important cornerstone of the Swiss economy. The attractiveness of the Swiss financial center is based on a smoothly functioning range of financial services and an impeccable reputation. Any countermeasures taken by other countries would have a negative impact on the Swiss financial center and thus on the Swiss economy. Violations of the FATF standards and the Egmont principles must therefore be avoided. In the interest of a functioning and credible financial center, Switzerland is thus **de facto forced to** transform soft law into national law in the area of financial market regulation. 18

III. CONTENT OF THE REGULATION

A. Organization – The Reporting Office as part of fedpol (para. 1)

1. Integration of the Reporting Office in fedpol

Based on its tasks and competencies, the Reporting Office is an **administrative authority** with special tasks, although it has no police powers – specifically, no powers of coercion. Its competencies lie in the analysis and assessment of reported and obtained information. The Reporting Office is neither a police nor a judicial authority, but it is affiliated to fedpol. 19

According to para. 1, the Reporting Office for Money Laundering is managed by the Federal Office of Police fedpol. In the French translation of the law, it is "gérer", which has more the meaning of "manage". What is meant by **"man-** 20

age" or **"gérer"** is not further explained in the law and ordinance. The question of subordination and thus the degree of independence of the reporting office is relevant. Essentially, an FIU must be independent in its core operational processes and, when analyzing cases, it must decide independently whether and what to forward to law enforcement and other national and international authorities. Likewise, the protection of the reporting parties must be guaranteed at all times. A corresponding separation or emancipation from fedpol and the rest of the central administration is therefore necessary.

21 In its report of December 20, 2021, the SFAO states: The question of independence should **not be interpreted too absolutely**. Ultimately, it makes sense for MROS and the other fedpol divisions to work closely together to combat money laundering. This was also the legislator's intention when MROS was assigned to the former BAP (Federal Office for Police, now fedpol). The Reporting Office can benefit from fedpol's infrastructure. This model is more cost-effective than maintaining an administratively independent unit. MROS receives from fedpol the financial and human resources it needs to carry out its core processes. Meanwhile, the SFAO recommended that fedpol and the reporting office draw up internal rules of procedure similar to those of the internal auditors of the departments and offices and provide a definitive answer to the question of what "managing" MROS by fedpol in accordance with Art. 23 para. 1 AMLA entails.

22 fedpol and MROS implemented the SFAO's recommendation in 2022 and issued **internal regulations**. MROS's annual report for 2022 states: *"The challenge was to define the division of tasks between fedpol and MROS as precisely as possible in order to best meet the requirements of the FATF and the Egmont Group." On the other hand, the general administrative organization, or the organizational and hierarchical integration of MROS in fedpol, which is clearly anchored in the law, could not be undermined by a regulation. In other words, a set of rules of procedure/regulations must fit within the framework of the general administrative organization.* The rules of procedure that came into force on November 1, 2022, are based on four central pillars:

23 no. 1 – **Organizational structure**: MROS is organizationally and hierarchically attached to the Crime Prevention and Justice Division (KPR). The head of MROS exercises leadership, control and supervision over the operational management of MROS. As part of fedpol, MROS is subject to all organization-

al, personnel and administrative regulations and directives of the general federal administration, the FDJP and fedpol.

no. 2 – **Operational tasks of the Reporting Office**: The main task is the reporting system – receiving reports of suspicion, analyzing them and passing the information on to the competent law enforcement authorities, as well as national and international mutual assistance. In addition, MROS is a member of the Egmont Group, and as such exercises the associated rights and duties, i.e. it participates in the necessary meetings, working groups and expert panels, maintains active relationships with FIUs abroad and is authorized to independently conclude Memoranda of Understanding (MoUs) with foreign partner offices. Furthermore, MROS is the specialist unit for combating money laundering and terrorist financing and is dedicated to a range of preventive tasks (raising awareness among financial intermediaries, participating in expert groups, conducting training and further education, etc.). It conducts strategic analysis and shares and publishes its findings with other authorities, the financial sector and third parties. MROS maintains its own data processing system. 24

no. 3 – Reporting Office's **operational independence**: The Reporting Office decides independently on the manner in which it fulfills and prioritizes the tasks defined in Art. 2. It decides on the deployment of the human resources made available to it. It also independently sets thematic priorities (triage, prioritization, etc.). With regard to the topic of financial and human resources, the rules of procedure point out that fedpol provides these for the tasks to be fulfilled by the reporting office, whereby the organizational and budgetary requirements of the federal administration must be adhered to. Other points covered by these regulations concern the topics of employee recruitment, information protection and travel. 25

no. 4 – **Assessment of operational independence**: Finally, the internal regulations contain provisions on review and escalation. According to these provisions, the Financial Inspectorate of the General Secretariat of the Federal Department of Justice and Police (FISP) periodically reviews the operational independence of MROS, prepares a report on the matter and, if necessary, makes recommendations. Furthermore, FISP also acts as an assessment authority in cases of ambiguity regarding independence issues. 26

27 The adoption of the internal regulations has provided MROS and fedpol with **clear demarcation criteria** regarding MROS's activities. The adoption of the internal regulations was deemed positive in an Egmont Group audit that took place in 2022.

2. Implementation of international requirements in national law

28 The FATF assessed Switzerland for the fourth time in 2016 and conducted a follow-up in 2020. In both reports, the FATF stated that MROS is **compliant with** Recommendation 29 on operational independence. The SFAO also came to a similar conclusion in its report: *"MROS is appropriately integrated into fedpol's structures and processes. The SFAO did not identify any situation in which fedpol violated the necessary operational independence of MROS."*

29 Only the Egmont Group expressed a **certain criticism** of MROS's independence in its on-site review conducted in 2022. Although it also concluded that MROS was compliant with the relevant Egmont principles, However, it also stated that the lack of budget authority for the reporting office, the lack of clear allocation of human resources in favor of the reporting office, and the lack of specific rules for the appointment and dismissal of the head of the reporting office should be considered problematic from the point of view of the independence of an FIU. This harbors a notorious potential for conflict between the reporting office and fedpol.

30 The question of independence will be on the agenda again during the upcoming fifth FATF mutual evaluation, which will be carried out from the end of 2026 to the end of 2028. In contrast to the last mutual evaluation in 2016, the focus will not only be on the technical implementation of Recommendation 29 in national law, but also on its **effective implementation**. Operational independence will therefore be measured by the activities of the reporting office, in particular the free interaction of the reporting office with other national authorities, foreign partner agencies and the financial industry.

B. Analysis of suspicious activity reports – "Intelligence" (para. 2)

1. Principle

31 The core task of the reporting office is the **analysis of** the incoming suspicious activity reports. Financial intermediaries under Art. 2 AMLA, the supervisory authorities entrusted with the fight against money laundering and ter-

rorist financing (FINMA, FGB, FOCG, SFAMA) and para-statal supervisory bodies (SROs and supervisory organizations) as well as dealers under Art. 2 para. 1 let. b in conjunction with 8a AMLA and their auditing bodies (see Art. 1 para. 2 lit. a MGwV). The group of reporters is therefore limited. There is no reporting option for third parties (e.g. concerned citizens, companies, media, etc.) – the reporting office is not authorized to accept reports from such parties and to deal with their content.

Switzerland has a **qualitative reporting system**, i.e. a report is based on reasonable suspicion and not on quantitative thresholds that trigger an automatic transmission to the reporting office when they are exceeded. The financial intermediaries and other reporting agents are an integral part of the suspicious activity reporting system in that they check, evaluate and process potentially suspicious transactions before passing them on to the reporting office. The Reporting Office should not be inundated with insufficiently substantiated SARs. It can therefore be assumed that the reporting persons have complied with the minimum formal requirements according to Art. 3 and 3a MLO and that the facts submitted are substantiated to a certain extent (see Art. 3 para. 1 let. h MLO). MROS rejects formally flawed and unfounded reports for improvement. It confirms receipt of a report only after receiving all the information and documents required by Art. 3 and 3a MGwV – a report is therefore only considered to have been submitted once the acknowledgement of receipt has been issued by MROS. 32

The primary goal of MROS's analysis work is to clarify whether or not the suspicions that led to the report are substantiated. In addition, MROS is tasked with supporting the downstream prosecuting authorities by providing concise analysis reports and thus generating **added value** – financial intelligence. In this so-called operational analysis, available and obtainable information is used to identify specific targets (e.g. persons, assets, criminal networks and associations), to follow up leads on certain activities or transactions and to establish connections between these targets and possible proceeds of crime, money laundering, predicate offences or terrorist financing. The starting point is always a report from a financial intermediary or a report (spontaneous information or request) from an international partner office (foreign FIU). This means that a **triggering piece of information** is needed. MROS has no authority to act on its own initiative – for example, on the basis of media reports. 33

34 If trigger information is available, MROS can take up the **"red thread"**, use the information available in its own data processing system goAML and use the tools to obtain further information. The options under Article 11a AMLA to obtain additional information from the reporting financial intermediary and from third-party institutions that are presumably involved are central here. In addition, there are other instruments for gathering information, such as national administrative assistance, retrieving information from judicial and police databases, obtaining information via the Egmont Network and OSINT (see no. III.B.2 below).

35 The FATF standard requires that MROS conduct **strategic analysis** in addition to operational analysis. In strategic analysis, available and obtainable information, including data that can be provided by other authorities, is used to identify trends, methods and patterns related to money laundering and terrorist financing. This information is then used to identify threats and vulnerabilities in the defense mechanism and to trigger countermeasures. The benefits are not limited to MROS alone – the information obtained should equally serve the other authorities and the financial industry.

36 Strategic analysis is enshrined in Art. 1 para. 2 let. f of the Financial Intelligence Act. Until the Financial Intelligence Act was amended on January 1, 2016, neither the AMLA nor the Financial Intelligence Act contained an explicit reference to strategic analysis. Today, MROS conducts strategic analysis primarily in the area of preparing **sectoral and national risk analyses**. Furthermore, it also addresses specific phenomena. One example is the "Alert" on terrorist financing that MROS addressed to the financial sector in late fall/winter 2023. Starting in January 2025, MROS plans to make anonymized case constellations available to the financial sector by means of a public and web-based typology database. Another field of activity for strategic analysis is the public-private partnership (PPP), which began operating under the name "Swiss FIPPP" in November 2024. The latter is geared towards exchanging information on trends, methods and typologies.

2. Analytical tools – MROS toolbox

37 In order to provide as complete a picture as possible of the transactions and networks involved in a case, MROS needs to have access to as much **additional information** as possible, in addition to the report that triggered its analysis. MROS can access certain additional information in two ways. Firstly,

it has access to several databases. Secondly, it can request information from financial intermediaries and from domestic and foreign authorities under certain conditions.

a. Information from financial intermediaries

In addition to the initial information – the SAR – other key elements of a transaction analysis include further **financial information** which MROS can request from the reporting financial intermediary and third-party intermediaries under Art. 11a AMLA. Today, criminal networks are present internationally with complex structures and across institutions. In order to create a complete picture, it is essential for MROS to access the complete information available from the financial intermediaries and to take it into account in its analysis. MROS can now obtain information from financial intermediaries in **three ways**: 38

Art. 11a para. 1 AMLA allows MROS to request additional information from the **reporting institution**. The duty to produce information extends to all information that MROS requires for its analysis and that is available at the **financial intermediary**. The information available is deemed to be that which is available or can be obtained in the entities of an undertaking that are subject to Swiss jurisdiction. In the opinion presented here, MROS's right to demand disclosure extends beyond simply requesting additional information from reports that have been submitted incompletely. This is already clear from the wording of the legal provision and from FATF Recommendation 29, which speaks of "additional information from reporting entities". In addition, however, it must be possible for MROS to request additional information from the reporting institution based on an analysis it has initiated, which then also includes information from other sources and not only information from the SAR. Any other interpretation would run counter to MROS's task of conducting in-depth analyses. 39

Art. 11a para. 2 AMLA stipulates that MROS can also demand information from the **third-party intermediary** if the analysis shows that the third-party intermediary is or was involved in the transaction or business relationship under investigation in some way. The prerequisite is that the indication that the third-party intermediary is affected comes from a suspicious activity report received by MROS. The scope of the disclosure obligation in para. 2 corresponds to that in para. 1. 40

41 Art. 11a para. 2bis AMLA finally stipulates that the reporting office may also demand information from financial intermediaries on the basis of information from its **foreign partner authorities**. In this context, it is irrelevant whether the information from the foreign FIU is a request or spontaneous information. It is also irrelevant whether a report has already been submitted to MROS by a reporting person in the same context. The scope of the duty to disclose is also the same for para. 2bis as for para. 1 and para. 2.

b. Access to police and judicial databases

42 For the operational analysis of suspicious activity reports, the reporting office primarily relies on its own data application goAML, i.e. it searches its own data for links and further clues, which then lead to further analysis steps and queries. In addition, the Reporting Office also has access rights to various **official databases** in order to check whether the natural and legal persons mentioned in the information received are already known to the authorities.

43 Art. 35a para. 1 AMLA authorizes the Reporting Office to access the following police and judicial databases in **retrieval procedures** and to check whether the persons in question are listed ("hit/no hit"): (1) National Police Index; (2) Central Migration System (ZEMIS); (3) Automated Criminal Records (VOSTRA); (4) State Security Information System (ISIS – transferred to IASA INDEX [NDB]); (5) Personal, File and Business Management System in the Area of Legal Assistance in Criminal Matters (TROVA).

44 Art. 35 para. 2 AMLA allows the Reporting Office **further access** to the information systems mentioned in para. 1, insofar as the provisions applicable to the respective information system provide for this. For example, the Reporting Office can access all the information contained in the police index. For ZEMIS and VOSTRA, IASA INDEX (NDB) and TROVA, specific or different rights of access apply, i.e. only part of the data can be accessed in each case.

45 MROS can also access other information systems on the basis of **special legal provisions** (e.g. RUMACA). At present, MROS has varying degrees of access to 15 police and judicial databases.

c. Information from international administrative assistance

46 An important source of information for MROS's operational analyses are its foreign partner FIUs. A large proportion of the reports of suspicious activity

have an international connection. MROS can make **requests to foreign FIUs**. MROS also benefits from spontaneous information and requests from abroad, which often contain valuable clues and information that can advance an analysis already in progress. The exchange of information between MROS and its foreign counterparts is governed by Art. 30 AMLA and the Egmont Principles. In all cases, the exchange of information must be in line with the principles of specialty (for analysis purposes only), reciprocity and confidentiality. Furthermore, the information received is subject to a dissemination proviso, i.e. the foreign authority determines to whom the information may be forwarded.

d. Information from national administrative assistance

Information from national administrative assistance can also complete the picture of an analysis or make it possible in the first place. MROS has seen a steady increase in the amount of information received in this regard since 2020. In principle, information can be **exchanged with any Swiss authority** provided the conditions set out in Art. 29, 29a and 29b AMLA are met. 47

Art. 29 para. 1 and 29b AMLA govern national administrative assistance between MROS and the various **supervisory authorities and bodies**. The authorities named in the law can provide each other with "all information" that they require for the "application of the AMLA". This is an **optional provision**. The authority concerned by the request from the reporting office decides independently whether to provide the requested information. 48

Art. 29 para. 2 AMLA stipulates that the reporting office can obtain information from **all Swiss authorities** that it needs for analyses in the context of money laundering, its predicate offences, organized crime or terrorist financing. In addition to financial information, this also includes information relating to criminal, administrative penal and administrative proceedings, including those from pending proceedings. In contrast to para. 1, there is an obligation to **release information** here on the part of the requested authorities. In practice, however, cantonal and municipal authorities in particular are very reluctant to release information. They are not very familiar with Art. 29 para. 2 AMLA. 49

Art. 29a AMLA finally requires that the prosecuting authorities forward to the Reporting Office all rulings issued on the basis of a report filed under Art. 23 para. 4 AMLA. The provision also requires that the Reporting Office be in- 50

formed of pending proceedings and that it be sent **judgments and discontinuation orders**, together with the reasons for them, provided that there is a connection to money laundering, its predicate offenses, organized crime or terrorist financing.

e. OSINT and other information sources

51 In the context of the global and continuously increasing availability of data and its networking, transaction and network analyses of open source intelligence (OSINT) are becoming more and more important. OSINT involves the collection, analysis and dissemination of information from **publicly accessible sources**, with a view to a specific question or analysis. OSINT sources include: traditional media, social media, websites, dark web, commercially available databases, official registers, archives, published statistics from authorities and private individuals, etc. Today, MROS also makes targeted use of OSINT information. In principle, MROS can use any publicly available information and data. The data protection requirements and restrictions that apply to MROS also apply to OSINT.

3. Risk-based approach

52 MROS's modus operandi has changed considerably in recent years. Due to the drastic increase in the number and volume of reports, MROS can no longer analyze and process all the information in the same level of detail. The Reporting and Analysis Office sets **priorities and focuses**. Since the introduction of the goAML data application on 1 January 2020, the Reporting and Analysis Office has been taking a '**risk-based approach**' to receiving and processing suspicious activity reports: the incoming suspicious activity reports are categorized by risk using a '**triage matrix**', prioritized and then analyzed to varying degrees based on this classification. MROS focuses on combating serious crime, with a particular emphasis on organized crime, terrorist financing and certain forms of economic crime. In doing so, MROS also aligns itself with the strategies of the law enforcement authorities, operates in a success-oriented manner and takes into account potential reputational risks for the Swiss financial center.

53 In 2023, one in five reports was **thoroughly analyzed**. The remaining 80% of the suspicious activity reports were processed in stages or with holistic analysis procedures (e.g. clustering methods). Some of the reports were already

sorted out upon receipt, so-called "filtered". This means that the report and the information it contains are no longer followed up, but are available for later use in the goAML data application. In its 2023 annual report, the reporting office states that its analyses tend to contain more information than in the past, i.e. they are composed of various suspicious activity reports and additional information obtained, which has also increased their complexity. Likewise, suspicious activity reports that had already been filtered at an earlier stage could be reactivated due to information added later. The risk-based approach means that the Reporting Office is moving away from the traditional processing approach of "one report equals one report to the prosecution authorities" towards active **"intelligence"** and the networking of existing information. It is no longer the report of suspicion as such, but rather its information content that is the focus of the analysis.

C. Information system (para. 3)

1. Use of the software application "goAML"

To fulfil its tasks, the Reporting Office is obliged to operate its own data processing system. The **software application goAML**, developed by UNODC, has been in use since 1 January 2020, replacing the previous GEWA system. The goAML application is a fully integrated software solution developed specifically for use by FIUs and is now in use in over 60 countries worldwide. The application is continuously being developed and new features are being added by UNODC in collaboration with the FIUs. The Reporting Office switched to version 5.2 in 2023; a transitional period is currently in effect for financial intermediaries until the end of 2024 at the latest to make the necessary adjustments to their interfaces and processes. 54

goAML allows the **electronic receipt of suspicious activity reports**. Financial intermediaries have three different transmission options: (1) fully automatic transmission via XML file, (2) a semi-automatic solution in which only the accounts and transactions are transmitted via XML file and the remaining information is entered via a web interface, and (3) fully manual entry of the data via the web interface. Around 60% of reports are submitted entirely via XML. This method of submission is less prone to errors than the others. 75% of the reports rejected by MROS upon receipt are due to manual input errors. Requests in accordance with Art. 11a AMLA can also be processed entirely via 55

goAML. MROS can also communicate with the authorities via goAML. All reports in accordance with Art. 23 para. 4 AMLA, including the transmission of analysis reports to the prosecuting authorities, as well as a large proportion of outgoing spontaneous information in accordance with Art. 29 AMLA, are now transmitted via the goAML channel.

2. Processing principles

56 The use of an information system is **not an end in itself**, but is based on the list of tasks and the competencies of the reporting office and should enable and facilitate it in fulfilling its tasks. Accordingly, the information system can be used for the three core tasks of intelligence, cooperation (national and international administrative assistance) and prevention (Art. 14 MGwV). The data stored in the information system comes from the information sources that the reporting office can access. These are mainly the reports of suspicious activity and the information from the inquiries based on Art. 11a AMLA. However, it also contains all information that comes from national and international administrative assistance, as well as the clarifications and analyses of the reporting office as such (Art. 15 MGwV).

57 MROS processes **particularly sensitive data** within the meaning of Art. 3 FADP. This involves processing personal data in connection with suspicious transactions and natural and legal persons suspected of money laundering, their predicate offences, organized crime or terrorist financing (Art. 16 para. MGwV). Furthermore, information on third parties may also be entered into the information system if it is relevant to the purpose of the reporting office (Art. 16 para. 2 MGwV).

58 Access to the information system is reserved exclusively for **employees of the reporting office** and, for system-related reasons, for maintenance personnel (Art. 20 MGwV). This is in line with the consistent implementation of the requirement for independence in accordance with the FATF and the Egmont Group.

59 The data stored in the information system is kept for a maximum of 10 years from the date of entry by the reporting office and then individually deleted (Art. 28 para. 1 MGwV). The same applies to the clarifications and analyses prepared by MROS.

D. Reporting to the law enforcement agencies (para. 4)

If, on the basis of its analysis, the Reporting Office comes to the conclusion that there is a suspicion of money laundering, its predicate offences, organized crime, terrorist financing or a lack of due diligence in financial transactions, it is obliged to report the matter immediately to the **competent law enforcement authority**. 60

The term "law enforcement authorities" refers to authorities as defined in Art. 12 of the Swiss Criminal Procedure Code (CrimPC). This means that reports can be made to both the public **prosecutor's office and the police**. As a rule, MROS reports to the public prosecutor's office, as only they have the authority to extend the legal freeze period in accordance with Art. 10 AMLA. In this regard, the police authorities are dependent on the cooperation of the public prosecutor's office. In view of the short decision period of only five days, the police authorities are hardly in a position to decide in good time whether to uphold the asset freeze. 61

The **material jurisdiction** is based on Art. 22 et seq. CrimPC. Cantonal jurisdiction is the rule, with federal jurisdiction the exception. The offenses subject to federal jurisdiction are listed in Art. 23 para. 1 and Art. 24 CrimPC. These include the classic state security offenses, i.e. offenses that are primarily directed against the federal government or that strongly affect its interests. It also includes complex intercantonal or international cases of organized crime, including terrorism and its financing, money laundering and corruption. As part of an optional federal authority, economic crime with a national or international dimension also falls under the federal authority. 62

MROS decides **independently and conclusively** which prosecuting authority to forward its analysis reports or complaints to. Based on practical considerations, MROS has long based its decisions on the location of the business relationship, since the place where the money laundering offence was committed is the main factor. Furthermore, information from different reports relating to the same facts are processed in an analysis report and sent to the same public prosecutor. This gives the prosecutor a better overview of the extended facts, which can serve as a basis for assessing whether to open proceedings. 63

The Reporting Office **does not withdraw any reports or parts thereof.** This procedure could lead to practical problems in connection with the freez- 64

ing of assets in accordance with Article 10, para. 1 AMLA and with the notifications to the financial intermediaries in accordance with Article 23, para. 5 AMLA. If a prosecution authority considers itself to be not competent to prosecute a report from MROS, it refers the matter to the public prosecutor's office that it considers to be competent, in application of Art. 39 para. 1 CrimPC, for the initiation of a court of jurisdiction procedure.

65 The act of reporting an offence in accordance with Article 23, para. 4 AMLA is generally **one-time and one-sided**. Once a report has been made, any further exchange with the prosecuting authorities in the same matter is based on Article 29 AMLA. In particular, the public prosecutor's requests may then only be answered according to the principles of national administrative assistance. MROS may exchange information orally with the prosecuting authorities before filing a report in order to clarify any questions of jurisdiction and transmission modalities or to consider whether a transmission makes sense at all.

66 Regarding the scope of the report to the prosecuting authorities, Art. 8 para. 1 MGwV states that the information transmitted by MROS must not contain any information identifying the person who filed the report or provided the information. This provision came into force on January 1, 2020, as part of the partial revision of the MLLCA, after the last country evaluation criticized the MROS's **protection of sources** as insufficient. As a result of this restriction, MROS no longer explicitly comments on the degree of involvement of the financial intermediary when a report is sent to the law enforcement authorities. Although this does not prevent conclusions from being drawn about the person submitting the report or providing the information, the prosecution authorities need a minimum of context in order to be able to start their investigations and take the necessary action, in particular to freeze the accounts. The protection of sources should therefore not be understood as absolute, but is limited to the fact that MROS must disclose the necessary information to the competent prosecution authority so that it can even begin its work.

E. Notification of the financial intermediary (para. 5)

67 Para. 5 stipulates that the Reporting Office informs the reporting financial intermediary when it transmits the reported information to a prosecuting authority. This applies to both mandatory reporting (Art. 9 AMLA) and voluntary reporting (Art. 305ter para. 2 SCC). In both cases, the information to the financial intermediary triggers a **legal freeze** of the reported assets for five work-

ing days, in accordance with Art. 10 para. 1 AMLA, which is to be carried out by the financial intermediary.

Para. 5 in its current form came into force on January 1, 2023. Previously, para. 5 was linked to a 20-day processing period, during which the reporting office had to report to the reporting financial intermediary under Art. 9 para. 1 let. a AMLA (reporting obligation) whether or not it was forwarding the report to a law enforcement agency. MROS thus had to inform the financial intermediary of the **fate of his report.** The revision of Art. 5 was necessary for several reasons: 68

Due to the increasing number of reports, MROS had **no longer been able to meet the 20-day processing deadline for several years.** There was not enough time, especially for reports that required in-depth analysis and entailed requests for information from foreign FIUs or further financial intermediaries in accordance with Art. 11a para. 2 AMLA. 69

Furthermore, the observance of the processing period was no longer appropriate in view of the intelligence approach applied by MROS. It was only the abolition of the processing period that gave the reporting office the necessary **leeway** to triage suspicious activity reports, prioritize or defer them and treat them with varying degrees of depth and focus. 70

Ultimately, the systematic information as to whether or not the information was forwarded to the prosecution authorities was also not very helpful, as it could be misinterpreted and lead the financial intermediary to draw **false conclusions**. For example, a financial intermediary could conclude from the non-transmission that his report was unfounded or that the reported assets were of lawful origin. Such information could also play a role for a financial intermediary when considering whether or not to maintain the reported business relationship. However, it is wrong to draw certain conclusions from MROS's decision not to forward information from a report to a law enforcement agency. It is not uncommon for MROS to forward information to a foreign reporting office. In such cases, a report is not necessarily forwarded to a Swiss law enforcement agency. Furthermore, information contained in a report may only later, in combination with other information, give rise to a suspicion and thus justify a report to a law enforcement agency. In accordance with the intelligence approach adopted by the Reporting Office, it is not the report as such that is crucial but the information contained in it. Financial in- 71

termediaries should therefore not draw any false conclusions from a non-transmission, neither regarding the appropriateness of their report nor regarding the lawful origin of the reported assets.

72 With the **revision of** para. 5, para. 6 was also deleted. The duty of MROS to provide information to the financial intermediaries was thereby standardized and the reports according to Art. 9 AMLA and Art. 305ter para. 2 SCC were placed on an equal footing.

BIBLIOGRAPHY

Ackermann Jürg-Beat/Zehnder Stephanie, in: Ackermann Jürg-Beat (Hrsg.), Kommentar Kriminelles Vermögen – Kriminelle Organisationen: Einziehung, Kriminelle Organisationen, Finanzierung des Terrorismus, Geldwäscherei, Band II, Zürich/Basel/Genf 2018 (zitiert KV-KO-Ackermann/Zehnder).

BAK Economics, Volkswirtschaftliche Bedeutung des Schweizer Finanzsektors – Studie im Auftrag der Schweizerischen Bankiervereinigung SBVg und des Schweizerischen Versicherungsverbandes SVV, Ergebnisse 2024, abrufbar unter https://www.svv.ch/sites/default/files/202411/BAK_Economics_Bedeutungsstudie_Finanzsektor_2024.pdf (zitiert BAK Economics).

Berger Corinne, Kommentierung zu Art. 23 GwG, in: Hsu Ch. Peter/Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz (GwG), Basel 2021.

Beuret Arnaud, Kommentierung zu Art. 29 GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar (SHK) Geldwäschereigesetz (GwG), Bern/Zürich 2017.

Derungs Corsin/Gmünder Eliane, Kommentierung zu Art. 23 GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar (SHK) Geldwäschereigesetz (GwG), Bern/Zürich 2017.

Gaul Caroline/Isler Michael/Vasella David, Kommentierung zu Art. 35a GwG, in: Hsu Ch. Peter/Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz (GwG), Basel 2021.

Hutzler Doris, in: Ackermann Jürg-Beat (Hrsg.), Kommentar Kriminelles Vermögen – Kriminelle Organisationen: Einziehung, Kriminelle Organisationen, Finanzierung des Terrorismus, Geldwäscherei, Band II, Zürich/Basel/Genf 2018 (zitiert KV-KO-Hutzler).

International Monetary Fund & World Bank, Financial Intelligence Units – An Overview, Washington D.C. 2004, abrufbar unter https://doi.org/10.5089/9781589063495.069 (zitiert IMF/WB, FIUs – An Overview).

Luchsinger Roland J., Kommentierung zu Art.11a GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar (SHK) Geldwäschereigesetz (GwG), Bern/Zürich 2017.

Naef Franceso, Soft Law und Gewaltenteilung – Über die Kunst der Legiferierung durch die Katzenklappe, AJP 2015, S. 1109–1121.

Naegeli Vera, Kommentierung zu Art. 11a GwG, in: Hsu Ch. Peter/Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz (GwG), Basel 2021.

Naegeli Vera, Kommentierung zu Art. 29 GwG, in: Hsu Ch. Peter/Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz (GwG), Basel 2021.

Ordolli Stiliano, § 34 Die Schweizerische Meldestelle für Geldwäscherei und ihre Tätigkeit, in: Sester Peter/Brändli Beat/Bartholet Olivier/Schildknecht Reto (Hrsg.) Finanzmarktaufsicht und Finanzmarktinfrastrukturen: St. Galler Handbuch zum Schweizer Finanzmarktrecht, Zürich 2017.

Taube Tamara, Die Schwarze Liste der FATF – was droht der Schweiz wirklich?», recht 2014, S. 210–217.

Thelesklaf Daniel, Kommentierung zu Art. 11a GwG, in: Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell-Füssli-Kommentar GwG/AMLA, 3. Aufl., Zürich 2019.

Thelesklaf Daniel, Kommentierung zu Art. 23 GwG, in: Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell-Füssli-Kommentar GwG/AMLA, 3. Aufl., Zürich 2019.

Thürer Daniel, «Soft Law» – eine neue Form von Völkerrecht?, Zeitschrift für Schweizerisches Recht (ZSR) 104 I, S. 429–453.

MATERIALS

Bericht der Eidgenössischen Finanzkontrolle: Prüfung der Aufgabenerfüllung der Meldestelle für Geldwäscherei, 20.12.2021, abrufbar unter https://www.efk.admin.ch/wpcontent/uploads/publikationen/berichte/sicher-

heit_und_umwelt/justiz_und_polizei/20146/20146be-endgueltige-fassung-v04.pdf, besucht am 30.11.2024 (zitiert Bericht EFK).

Botschaft zum Bundesgesetz über die Sperrung und die Rückerstattung unrechtmässig erworbener Vermögenswerte ausländischer politisch exponierter Personen vom 21.5.2014, BBl 2014 5265 ff. abrufbar unter https://www.fedlex.admin.ch/eli/fga/2014/1134/de, besucht am 30.11.2024 (zitiert Botschaft SRVG 2014).

Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG) vom 17.6.1996, BBl 1996 III 1101 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1996/3_1101_1057_993/de, besucht am 30.11.2024 (zitiert Botschaft GwG 1996).

Botschaft zur Änderung des Geldwäschereigesetzes vom 26.6.2019, BBl 2019 5451 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2019/1932/de, besucht am 30.11.2024 (zitiert Botschaft GwG 2019).

Botschaft zur Änderung des Geldwäschereigesetzes vom 27.6.2012, BBl 2012 6941 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2012/1031/de, besucht am 30.11.2024 (zitiert Botschaft GwG 2012).

Botschaft zur Genehmigung und zur Umsetzung des Übereinkommens des Europarats zur Verhütung des Terrorismus mit dem dazugehörigen Zusatzprotokoll sowie zur Verstärkung des strafrechtlichen Instrumentariums gegen Terrorismus und organisierte Kriminalität vom 14.9.2018, BBl 2018 6427 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2018/2301/de, besucht am 30.11.2024 (zitiert Botschaft Verhütung Terrorismus 2018).

Botschaft zur Umsetzung der 2012 revidierten Empfehlungen der Groupe d'action financère (GAFI) vom 13.12.2013, BBl 2014 605 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2014/100/de, besucht 30.11.2024 (zitiert Botschaft GwG 2014).

Egmont Group of Financial Intelligence Units Charter, 2013 (revised 2023), abrufbar unter https://egmontgroup.org/wp-content/uploads/2021/09/Egmont-Group-Charter-Revised-July-2023-Abu-Dhabi-UAE.pdf, besucht am 30.11.2024 (zitiert Egmont Charter).

Egmont Group of Financial Intelligence Units, Support and Compliance Process, 2014, abrufbar unter https://egmontgroup.org/wpcontent/uploads/

2021/09/
Egmont_Group_of_Financial_Intelligence_Units_Support_and_Compliance_Process.pdf, besucht am 30.11.2024 (zitiert Egmont Compliance Process).

Egmont Group of Financial Intelligence Units: Understanding FIU Operational Independence and Autonomy, Toronto (CAN) 2018, abrufbar unter https://egmontgroup.org/wp-content/uploads/2021/09/2018_Understanding_FIU_Operational_Independence_and_Autonomy.pdf, besucht am 30.11.2024 (zitiert Understanding FIU Operational Independence and Autonomy).

Egmont Group, Principles for information exchange between financial intelligence units, October 2013 (revised April 2023), abrufbar unter https://egmontgroup.org/wp-content/uploads/2022/07/2.-Principles-Information-Exchange-With-Glossary_April2023.pdf, besucht am 30.11.2024 (zitiert Egmont Principles Exchange).

Erläuterungen zur Teilrevision der MGwV, 27.11.2019, abrufbar unter https://www.ejpd.admin.ch/dam/fedpol/de/data/kriminalitaet/geldwaescherei/vo-anpassung/erlaeuterungen-mgwv-d.pdf.download.pdf/erlaeuterungen-mgwv-d.pdf, besucht am 30.11.2024 (zitiert Erläuterungen Teilrevision MGwV 2019).

Fourth Mutual Evaluation Report on Anti-Money Laundering and counter-terrorist financing measures, Switzerland, December 2016, abrufbar unter https://www.fatf-gafi.org/content/dam/fatf-gafi/images/mer/mer-switzerland-2016.pdf, besucht am 30.11.2024 (zitiert MER 2016).

Geschäftsordnung fedpol/MROS vom 1.11.2022, abrufbar unter https://www.fedpol.admin.ch/dam/fedpol/de/data/kriminalitaet/geldwaescherei/geschaeftsordnung-mros.pdf.download.pdf/geschaeftsordnung-mros-d.pdf, besucht am 30.11.2024.

International Standards on Combating Money laundering ans the Financing of Terrorism and Proliferation – The FATF Recommendations, Paris 2012 (revised November 2023), abrufbar unter fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF Recommendations 2012.pdf.coredownload.inline.pdf, besucht am 30.11.2024 (zitiert FATF-Empfehlung[en]).

Jahresberichte der Meldestelle für Geldwäscherei (MROS), abrufbar unter https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/

publikationen.html, besucht am 30.11.2024 (zitiert Jahresbericht MROS, jeweiliges Jahr)

Strategie MROS 2024–2027, abrufbar unter https://www.fedpol.admin.ch/dam/fedpol/de/data/kriminalitaet/geldwaescherei/strategie-mros.pdf.download.pdf/strategie-mros-d.pdf, besucht am 30.11.2024.

Third Enhanced Follow-up Report & Technical Compliance Re-Rating, January 2020, abrufbar unter https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fur3-switzerland-2020.html, besucht am 30.11.2024 (zitiert FUR 2020).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 24 AMLA

A commentary by Caroline Kindler

SUGGESTED CITATION

Caroline Kindler, Commentary of art. 24 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Kindler, art. 24 AMLA N. XXX

Section 5 Self-Regulatory Organisations

Art. 24 Recognition

[1] Organisations are recognised as self-regulatory organisations if they:

a. have regulations in accordance with Article 25;

b. supervise their affiliated financial intermediaries with regard to compliance with their duties in terms of Chapter 2; and

c. provide the guarantee of irreproachable business conduct and ensure that the persons and audit firms they instruct to carry out inspections:

possess the required specialist knowledge,
provide the required guarantees that inspections will be carried out properly, and

are independent of the management and administration of financial intermediaries being inspected;

d. ensure that the audit firms they instruct to carry out inspections and lead auditors fulfil the requirements under Article 24*a*.

[2] The self-regulatory organisations of the licensed transport undertakings under the Public Transport Act of 20 March 2009 must be independent of their respective managements.

CONTENT

I. Self-regulatory organization 442
A. Concept of self-regulation 442
B. The significance of self-regulation in the AMLA 442
C. Organization 443
II. Recognition: Concept and Legal Nature 443
III. Conditions (Para. 1) 443
A. Regulations in accordance with Art. 25 AMLA (let. a) 443
B. Supervision of affiliated financial intermediaries (lit. b) 444
C. Guarantee, expertise and independence (c) 444
1. Guarantee 445
2. Expertise 446
3. Independence 446
D. Ensuring compliance with Art. 24a AMLA (lit. d) 447
IV. SROs of licensed transport companies (para. 2) 447
Bibliography 448
Materials 448

I. SELF-REGULATORY ORGANIZATION

A. Concept of self-regulation

1 **Self-regulation** refers to the direct or indirect establishment and enforcement of rights, duties and responsibilities by private individuals in the exercise of a legally granted area of autonomy. A distinction is made between voluntary (genuine) and state-directed (fake) self-regulation: Voluntary (genuine) self-regulation occurs when private individuals, in the exercise of their economic freedom and on the basis of private autonomy, issue statutes, such as rules of professional ethics, or conclude contracts. In the case of state-directed (pseudo) self-regulation, on the other hand, the state lays down the foundations for private self-regulation in a legal enactment. Voluntary or genuine self-regulation is generally considered to be a private autonomous (industry) agreement. By contrast, state-directed (pseudo) self-regulation raises questions of demarcation, particularly with regard to its classification as a private-law agreement or as an actual legislative act of public or private law based on delegated legislative powers.

B. The significance of self-regulation in the AMLA

2 The concept of self-regulation in the fight against money laundering originated in the banking sector: the Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CDB), which has been in force since 1977, is regularly cited as an example of voluntary (genuine) self-regulation. When the Anti-Money Laundering Act was drafted, the legislator relied "heavily on the proven" CDB. In the message on the Anti-Money Laundering Act, it was stated that the law "[...] is based on the principle of self-regulation" and "[...] is characterized by the idea of self-regulation". Nevertheless, the concept that the legislator introduced for monitoring compliance by financial intermediaries with the duties under the second chapter of the Anti-Money Laundering Act is an application of **state-controlled (pseudo) self-regulation**: FINMA grants and withdraws recognition of self-regulatory organizations (SROs) by law, supervises them and approves their self-regulatory regulations. In addition, FINMA ensures that the SROs effectively enforce the statutory and regulatory requirements with respect to their affiliated financial intermediaries. As the public role of self-regulation and the public interest as-

sociated with combating money laundering have become increasingly important over the past few decades, the fight against money laundering in Switzerland has developed from its initial form of purely private self-regulation into an essential public duty.

C. Organization

The law does not prescribe any particular **legal form** for SROs: they are not even required to be a separate legal entity. As of July 1, 2024 (cut-off date), eleven SROs were authorized by FINMA, which are either organized as an association under Art. 60 et seq. CC or form an organizational unit within an industry association. 3

II. RECOGNITION: CONCEPT AND LEGAL NATURE

The term "authorization" is generally used for the power to exercise an activity granted by the FINMA. However, the legislator uses the term "recognition" in this instance, presumably because it is not only about the permission to exercise an operational activity, but also about the transfer of supervisory powers. Nevertheless, "recognition" is indisputably a **police authorization**, and as such an order in accordance with Art. 5 APA. If the conditions of Art. 24 are met, the SRO is therefore entitled to recognition. An appeal may be lodged with the Federal Administrative Court against the corresponding decision of FINMA (Art. 44 APA). 4

III. CONDITIONS (PARA. 1)

An SRO is entitled to recognition if the conditions set out in para. 1 let. a-d are met **cumulatively**. 5

A. Regulations in accordance with Art. 25 AMLA (let. a)

Art. 24, para. 1, let. a AMLA requires that an SRO has **regulations** in accordance with Art. 25 AMLA: these regulations must define the duties of due diligence of the affiliated financial intermediaries in accordance with Art. 3–11a AMLA and specify how these are to be fulfilled (Art. 25, para. 2 AMLA). In addition, the regulations must (a) define the conditions for the admission and exclusion of financial intermediaries, (b) specify how compliance with the obligations under Art. 3–11a AMLA is to be monitored and (c) set out appropriate 6

sanctions (Art. 25 para. 3 AMLA). As part of the recognition procedure, FINMA is therefore obliged to check compliance with the conditions set out in Article 25 AMLA and to approve the regulations.

B. Supervision of affiliated financial intermediaries (lit. b)

7 Pursuant to Art. 24 para. 1 let. b AMLA, as part of the recognition procedure an SRO must demonstrate that it is able to supervise the affiliated financial intermediaries to ensure that they comply with their duties under Art. 3–11a AMLA. Since recognition by FINMA is constitutive for an SRO, it cannot carry out any supervisory activities before it is recognized. The examination of the guarantee of supervision is therefore initially carried out hypothetically as part of the recognition procedure. Compliance with the conditions is only examined in practice after the point of recognition. From the perspective of doctrine, the **guarantee of supervision** includes adequate organization, sufficient personnel and sufficient financial resources.

C. Guarantee, expertise and independence (c)

8 Article 24, para. 1, let. c AMLA requires that both the SRO and the persons entrusted with the control and the audit companies offer a **guarantee of** irreproachable business and auditing activities. The persons entrusted with the control and the audit companies must also have the necessary expertise and be independent.

9 Regarding the **addressees of** these requirements, the applicable provision makes it clear that the SRO itself must also guarantee proper business conduct. It is assumed in legal doctrine that this was already implicit in the previous wording, so that the adapted formulation merely represents a clarification. "Audit firms" refers to those within the meaning of Art. 24a AMLA. The term "persons entrusted with control" encompasses all persons who are formally or materially entrusted with control. These include, among others, those who assess the admission of supervised persons, commission the audit, accept audit reports or order and carry out measures and/or sanction proceedings, as well as those who can impose sanctions up to and including exclusion. Persons who carry out purely administrative activities are not included. It should not be assumed that the term "persons entrusted with control" is interpreted broadly.

1. Guarantee

Art. 24 para. 1 let. c AMLA requires that the SRO itself provides "guarantees of proper business conduct" and that the persons and audit firms entrusted with the control provide "guarantees of proper auditing conduct". The **guarantee requirement** was originally enshrined in the Banking Act (Art. 3 para. 2 let. c BankG) to ensure that a bank is managed by "reliable and professionally competent persons". In the meantime, the guarantee requirement can be found in most financial market laws. It is an indeterminate legal concept. It is questionable whether the practice developed in banking and stock exchange law can be used for interpretation: the wording of Art. 24 para. 1 let. c AMLA requires that the SRO generally provides "guarantee of proper business conduct", in contrast to Art. 14 para. 2 lit. b and c AMLA, which only requires financial intermediaries to 'guarantee the fulfillment of their obligations under the AMLA'. However, since an SRO does not carry out any "business activity" in the sense of a commercial activity, but rather performs a sovereign supervisory function, the scope of the SRO's guarantee requirement is limited to "guaranteeing compliance with legal obligations". This was already provided for in the message on the AMLA. Consequently, the guarantee requirement imposed on the SRO is to be interpreted by analogy with Art. 14 AMLA: according to the Federal Court, the guarantee requirement in terms of a person's "ability to comply with the law" can be called into question if regulations other than those of the AMLA are violated. However, serious violations of the law are required in order to assume that the guarantee of compliance with the AMLA is no longer fulfilled. In contrast to the guarantee requirement imposed on the SRO, the guarantee requirement for the persons entrusted with the control and audit companies is limited to "proper auditing". The scope of this requirement must therefore be interpreted narrowly and refers exclusively to the area of auditing. According to legal doctrine, the persons entrusted with the control activity, in particular the lead auditors, must meet increased legal and ethical requirements. In contrast to the guarantee requirement for SROs, however, "serious legal violations" can only cast doubt on the guarantee of these persons if there is a connection between these violations and their professional activity, i.e. AMLA audit activity. 10

2. Expertise

11 The persons and audit firms entrusted with the audit must have the necessary **specialist knowledge**. According to the dispatch, it is not possible to provide a general answer as to what requirements are to be set in this regard. From a teaching point of view, the persons entrusted with the audit must have knowledge of Swiss financial market law, in particular in the area of the Anti-Money Laundering Act (AMLA), as well as in-depth knowledge of the industry. In particular, industry SROs require specific knowledge and skills in the respective industry, while cross-industry SROs need the broadest possible technical coverage.

12 However, the necessary professional expertise and **industry proximity** sometimes conflict with the requirement for independence. Since industry-specific knowledge can generally only be acquired through activities in the respective industry, a certain degree of industry proximity is inevitable. The legislator has stipulated that the recruitment of persons associated with affiliated financial intermediaries is not prohibited in principle; however, it must be ensured that the usual recusal requirements are adhered to. In case of doubt, however, FINMA regularly places more emphasis on independence than on industry-specific knowledge. The requirements for the expertise of audit firms are set out in Art. 24a AMLA.

3. Independence

13 The persons and audit firms entrusted with the audit must be **independent of** the management and administration of the financial intermediaries to be audited. This is to ensure that the auditors can act with as little influence as possible from the interests of the supervised financial intermediaries and concentrate on the aspects of the audit. Therefore, any constellation that could restrict the freedom of decision should be avoided. According to doctrine, the requirement of independence encompasses legal, personnel and economic aspects. Independence prohibits the controllers, for example, from accepting mandates from supervised financial intermediaries or from holding direct or larger indirect participations in such financial intermediaries. This requirement of independence applies only to the "financial intermediaries to be controlled"; there are no restrictions on financial intermediaries supervised by another SRO.

However, complete, unconditional independence – both formal and material – of the control persons is not always possible. The **vested interests** of the members of the SRO's board of directors, who may be dismissed or not re-elected by the supervised financial intermediaries, are unavoidable. Even if, as proposed by Neese, board members refrain from operational activities and appoint a managing director, there remains an unavoidable residual influence on the employed supervisors due to the relationship of subordination and the obligation to follow instructions. Furthermore, it is in line with the legislator's intention not to demand absolute independence: the message does not require "the recruitment of persons who are not associated with any of the affiliated financial intermediaries in every case. It must merely be ensured that the usual duties of confidentiality are maintained". While the increasing independence requirements in FINMA's supervisory practice are understandable from a corporate governance perspective, there is a risk that these requirements will outweigh the expertise and industry experience that the system of self-regulation is actually intended to ensure. 14

D. Ensuring compliance with Art. 24a AMLA (lit. d)

Art. 24 para. 1 let. d AMLA requires for the recognition of SROs that the audit firms and lead auditors they appoint to carry out inspections must meet the requirements of Art. 24a AMLA. This means that the SRO is not only responsible for verifying compliance with the admission requirements at the time of admission, but must also ensure the **ongoing supervision** of the audit firms and lead auditors with regard to their continued compliance with these requirements. 15

IV. SROS OF LICENSED TRANSPORT COMPANIES (PARA. 2)

Based on Article 24 paragraph 2 AMLA, the recognition of SROs of **licensed transport companies** under the Passenger Transport Act of 20 March 2009 is subject to the condition that the SROs must be independent in terms of organization and personnel "from the management" of these companies. Two SROs were affected by this regulation: "SRO Post" and "SRO SBB". PostFinance AG, a wholly-owned subsidiary of Swiss Post Ltd, received a banking license in 2013 and has since been under the direct supervision of FINMA. The "SRO SBB" was replaced by the "SRO VÖV" (Association of Public Transport), and ceased its supervisory activities in 2018. The AMLA members were either 16

taken over by other SROs or placed themselves under the direct supervision of FINMA. Since none of the SROs concerned still exists, this provision is currently redundant.

BIBLIOGRAPHY

Basse-Simonsohn Detlev Michael, Geldwäschereibekämpfung und organisiertes Verbrechen, Die Sorgfaltspflichten der Finanzintermediäre und deren Konkretisierung durch Selbstregulierung, Bern 2002.

Häfelin Ulrich/Müller Georg/Uhlmann Felix, Allgemeines Verwaltungsrecht, 8. Aufl. Zürich/St. Gallen 2020.

Neese Martin, Kommentierung zu Art. 24 GwG, in: Peter Ch. Hsu/Daniel Flühmann (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Stadler Stephan, Die gelenkte Selbstregulierung im Bereich der Geldwäscherei, LeGes 2006/3, S. 49-58.

Thelesklaf Daniel, Kommentierung zu Art. 24 GwG, in: Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell Füssli Kommentar, Geldwäschereigesetz, 3. Aufl., Zürich 2019.

Zysset Pascal, Kommentierung zu Art. 24 GwG, in: Peter V. Kunz/Thomas Jutzi/Simon Schären (Hrsg.), Stämpflis Handkommentar (SHK) zum Geldwäschereigesetz (GwG), Bern/Zürich 2017.

Zysset Pascal, Selbstregulierung im Finanzmarktrecht, Grundlagen, verwaltungsrechtliche Qualifikationen und rechtsstaatlicher Rahmen, in: Dieter Zobl/Rolf H. Weber/Rolf Sethe, Schweizer Schriften zum Finanzmarktrecht, Band 124, Zürich 2017 (zit.: Zysset, Selbstregulierung).

MATERIALS

Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG) vom 17.6.1996, BBl 1996 III 1101, abrufbar unter https://www.fedlex.admin.ch/eli/fga/1996/3_1101_1057_993/de, besucht am 23.8.2024 (zit. Botschaft GwG 1996).

Botschaft des Bundesrates an die Bundesversammlung über die Revision des Bankengesetzes vom 13.5.1970, BBl 1970 1144, abrufbar unter https://

www.fedlex.admin.ch/eli/fga/1970/1_1144__/de, besucht am 23.8.2024 (zit. Botschaft BankG 1970).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 24a AMLA

A commentary by Caroline Kindler

SUGGESTED CITATION

Caroline Kindler, Commentary of art. 24a AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Kindler, art. 24a AMLA N. XXX

Art. 24a Licensing of audit firms and lead auditors

[1] The self-regulatory organisation shall grant the audit firms and lead auditors the necessary licence and supervise their activity.

[2] The audit firm shall be licensed if:

a. it is licensed as an auditor by the Federal Audit Oversight Authority in accordance with Article 6 of the Auditor Oversight Act of 16 December 2005;

b. it is adequately organised for this audit; and

c. it does not perform any other activity requiring authorisation under the financial market acts in accordance with Article 1 paragraph 1 of the FINMASA.

[3] The lead auditor shall be licensed to lead audits in accordance with paragraph 1 if he or she:

a. is licensed as an auditor by the Federal Audit Oversight Authority in accordance with Article 5 of the Auditor Oversight Act;

b. has the necessary specialist knowledge and the necessary practical experience for performing audits in accordance with paragraph 1.

[4] Article 17 of the Auditor Oversight Act applies by analogy to the self-regulatory organisation's withdrawal of the licence granted to audit firms and lead auditors in accordance with paragraph 1, as well as to its issuing of a reprimand.

CONTENT

I. Admission: concept and legal nature 454
II. Requirements 454
III. Requirements for the audit firm (para. 2) 455
A. Licensing as an auditor in accordance with Art. 6 AOA by the FAOA (lit. a) 455
B. Sufficient organization (lit. b) 455
C. No other activity requiring a license (lit. c) 456
IV. Requirements for lead auditors (para. 3) 456
A. Licensing as an auditor by the FAOA in accordance with Art. 5 AOA (lit. a) 456
B. Specialist knowledge and practical experience (lit. b) 456
V. Withdrawal of admission / Imposition of a reprimand by the SRO (Para. 4) 457
Bibliography 457

I. ADMISSION: CONCEPT AND LEGAL NATURE

1 Audit firms and lead auditors act as an **extended arm** of the self-regulatory organization (SRO) when conducting audits of financial intermediaries supervised by the SRO. Therefore, audit firms and lead auditors must meet the admission requirements when conducting audits on behalf of an SRO.

2 The SRO is **responsible for** granting licenses to audit firms and lead auditors.

3 There is disagreement in legal doctrine on the question of whether there is a **right** to licensing by the SRO if the licensing requirements are met: Zysset believes there is a "conditional right" to licensing, so that the situation is comparable to that of a police permit; according to Neese, this is Neese, due to the private-law nature of the legal relationship between the SRO and the audit firm and based on the principle of contractual freedom, this is not generally true; Zufferey, on the other hand, is of the opinion that, due to the performance of a public-law function, the admission decision should be regarded as a contestable ruling.

4 From a legal point of view, SROs are bound by **fundamental rights** based on the performance of state functions under Art. 35 para. 2 FC and must observe the principles of state action under Art. 5 para. 2 FC. According to the view represented here, the licensing procedure for audit firms and lead auditors is at least bound by the principle of legal equality (Art. 8 FC) and the prohibition of arbitrariness (Art. 9 FC): Thus, licensing decisions that treat audit firms or lead auditors differently despite the same conditions, or rejection decisions that are not based on any objective reasons, are not permissible; furthermore, the audit firm or lead auditor must be granted the right to a legal hearing (Art. 29 para. 2 FC), which in particular entails the right to a reasoned decision. The same applies to the withdrawal of admission or the issuing of a reprimand by the SRO in accordance with Art. 24a para. 4 AMLA in conjunction with Art 17 AOA.

II. REQUIREMENTS

5 The system of "**dual admission**" or "dual-track admission review" applies to the admission of audit firms and lead auditors: In order for both the audit firms and the lead auditors to be admitted, a "basic admission" by the Federal

Audit Oversight Authority (FAOA) is required. This basic admission is not re-examined by the SRO, but is merely a requirement. On this basis, the "special legal license" is granted by the SRO.

III. REQUIREMENTS FOR THE AUDIT FIRM (PARA. 2)

For the audit firm to be licensed, Art. 24a para. 2 AMLA requires that it is cu- 6
mulatively (1) licensed by the FAOA, (2) sufficiently organized and (3) does not carry out any other activity requiring a license under financial market laws. Art. 24a para. 5 AMLA would authorize the SRO to provide for further licensing criteria; it should be noted that so far no SRO has made use of this possibility.

A. Licensing as an auditor in accordance with Art. 6 AOA by the FAOA (lit. a)

Art. 24a para. 2 lit. a AMLA explicitly refers to Art. 6 AOA and thus to the fact 7
that the governing bodies (in their majority), employees (at least one fifth) and lead auditors (in total) must be licensed as **auditors in accordance with Art. 5 AOA**. To be licensed as an auditor, you must have a good reputation, have completed training in accordance with Art. 4 para. 2 AOA and have at least one year of professional experience (Art. 5 para. 1 AOA).

The licensing of the audit firm by the SRO is exclusively dependent on the 8
formal licensing of the audit firm as an **auditor in accordance with Art. 6 AOA**: The SRO is not responsible for the substantive examination of the licensing requirements in accordance with Art. 6 AOA.

B. Sufficient organization (lit. b)

Pursuant to Art. 24a para. 2 let. b AMLA, the audit firm must be **sufficiently** 9
organized for this audit. Pursuant to Art. 22a para. 1 AMLO, this is the case if the audit firm cumulatively (1) has at least two lead auditors within the meaning of Art. 24a para. 3 AMLA , (2) has at least two audit engagements in the area of the AMLA no later than three years after the license is granted, and (3) complies with the provisions on documentation and retention of documents in accordance with Article 730c CO.

C. No other activity requiring a license (lit. c)

10 Art. 24a para. 2 lit. c AMLA **prohibits** an audit firm active in the area of AMLA from engaging in any other activity requiring a license under financial market legislation. Art. 22a para. 2 AMLO extends this prohibition to the following persons: companies under common management with the audit firm (lit. a); natural persons who, directly or indirectly, hold at least 10% of the capital or votes in a company under lit. a or who are otherwise able to exert a decisive influence on its business activities (lit. b); and the lead auditors (lit. c).

IV. REQUIREMENTS FOR LEAD AUDITORS (PARA. 3)

11 For the licensing of the auditor in charge, Art. 24a para. 3 AMLA requires that he or she is cumulatively licensed by the FAOA (lit. a) and has the necessary specialist knowledge and the required practical experience for the audit (lit. b).

A. Licensing as an auditor by the FAOA in accordance with Art. 5 AOA (lit. a)

12 Art. 24a para. 3 lit. a AMLA explicitly refers to **Art. 5 AOA**, which requires, in addition to good repute, training in accordance with Art. 4 para. 2 AOA and professional experience of at least one year, as specified in para. 2.

13 As with the licensing of the audit firm, the licensing of the lead auditor by the SRO is also exclusively based on the formal **license to** practice as an auditor in accordance with Art. 5 AOA: The SRO is not responsible for the substantive review of the licensing requirements under Art. 5 AOA.

B. Specialist knowledge and practical experience (lit. b)

14 Art. 24a para. 3 lit. b AMLA requires the lead auditors to have the necessary **specialist knowledge** and the **required practical experience** for the audit. Art. 22b AMLO sets out the minimum requirements: (1) for admission: five years' professional experience in providing audit services in the field of the AMLO, 200 audit hours in the field of the AMLO, four hours of further training in the field of the AMLO AMLA within one year prior to submitting the license application (para. 1); (2) after the license has been granted: 100 audit

hours in the area of AMLA in the last four years, four hours of continuing education per year in the area of AMLA (para. 2).

Art. 22d AMLO specifies the requirements for **continuing education**: External and internal training events must cover the area of the AMLA and last at least one hour. At least three people must participate in internal training events. Self-study does not count as training. The actual duration of the training event is counted, unless a specialist lecture or course is given; in this case, double the duration of the lecture or course is counted. 15

V. WITHDRAWAL OF ADMISSION / IMPOSITION OF A REPRIMAND BY THE SRO (PARA. 4)

Art. 24a Para. 4 AMLA stipulates that Art. 17 AOA is applicable by analogy for the withdrawal of admission and the imposition of a reprimand by the SRO. As explained above, the **fundamental rights**, specifically the principle of equality before the law (Art. 8 FC), the prohibition of arbitrariness (Art. 9 FC) and the right to a fair hearing (Art. 29 para. 2 FC) must be observed not only in the context of the admission procedure but also when withdrawing admission or issuing a reprimand. 16

BIBLIOGRAPHY

Neese Martin, Kommentierung zu Art. 24a GwG, in: Peter Ch. Hsu/Daniel Flühmann (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Zufferey Jean-Baptiste, Kommentierung zu Art. 24a GwG, in: Cassani Ursula/Bovet Christian/Villard Katia (Hrsg.), Commentaire Romand, Loi sur le blanchiment d'argent, Basel 2022.

Zysset Pascal, Kommentierung zu Art. 24a GwG, in: Peter V. Kunz/Thomas Jutzi/Simon Schären (Hrsg.), Stämpflis Handkommentar (SHK) zum Geldwäschereigesetz (GwG), Bern/Zürich 2017.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 25 AMLA

A commentary by Caroline Kindler

SUGGESTED CITATION

Caroline Kindler, Commentary of art. 24 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Kindler, art. 24 AMLA N. XXX

Art. 25 Regulations

[1] Self-regulatory organisations must issue regulations.

[2] The regulations shall specify the duties of diligence of their affiliated financial intermediaries within the meaning of Chapter 2 and stipulate how these duties must be fulfilled.

[3] They shall further stipulate:

a. the requirements for the affiliation and exclusion of financial intermediaries;

b. how compliance with the duties in terms of Chapter 2 is monitored;

c. appropriate penalties.

CONTENT

I. Adoption of regulations by the self-regulatory organization (para. 1) 461
A. General 461
B. Limited autonomy of SROs in the design of regulations 461
II. Content of the regulations (para. 2 and 3) 462
A. Specification of the due diligence requirements under Chapter 2 (para. 2) 462
B. Requirements for the affiliation and exclusion of financial intermediaries (para. 3 let. a) 463
C. Monitoring compliance with the duties under Chapter 2 (para. 3 let. b) 465
D. Appropriate sanctions (para. 3 let. c) 466
Bibliography 468
Materials 469

I. ADOPTION OF REGULATIONS BY THE SELF-REGULATORY ORGANIZATION (PARA. 1)

A. General

Article 25 para. 1 stipulates that self-regulatory organizations (SRO) must adopt **regulations**. This provision has no independent significance, since the SRO regulations already constitute a requirement for the recognition of the SRO based on Art. 24 para. 1 let. a. 1

B. Limited autonomy of SROs in the design of regulations

According to the message, the Money Laundering Act is characterized by the idea of self-regulation. The legislator intended to create a framework law that regulates the duties imposed on financial intermediaries in a correspondingly restrained and less detailed manner, in order to leave the substantiating function to the self-regulatory organizations. However, the **autonomy** of the SROs, as formulated by the legislator, to freely determine the content of their regulations in compliance with the legal requirements, is limited: FINMA bases its approval of SRO regulations on the key provisions of AMLO-FINMA (Art. 1 para. 2 AMLO-FINMA). 2

Deviations from AMLO-FINMA are possible, but must be indicated in the SRO regulations (Art. 1 para. 3 AMLO-FINMA). In line with the legislator's aim of achieving the greatest possible uniformity in the application of the law, the Federal Supreme Court assumes that deviating SRO regulations should be limited to objectively justified, industry-specific peculiarities: This is to prevent individual deviating SRO regulations from jeopardizing the entire system of money laundering prevention through so-called “regulatory arbitrage” or a “race to the bottom”. Accordingly, FINMA should exercise restraint when dealing with SRO regulations that differ from AMLO-FINMA and are based on industry-specific features; however, tighter rules in the SRO regulations compared to the provisions of the AMLA and AMLO-FINMA should always be permissible. 3

As a result, the provisions of the SRO regulations that substantiate the due diligence requirements are largely **identical to** the provisions of AMLO-FINMA. 4

5 If FINMA intervenes in the content of the SRO regulations beyond the provisions of the AMLA, the question of compliance with the **principle of legality** arises: a regulation issued in the material sense in accordance with competence – i.e. a legislative or executive ordinance such as AMLO-FINMA – is sufficient when subordinate technical standards are involved; however, if fundamentally new obligations are to be created, a legal basis is required, i.e. an amendment to the AMLA. In this context, the line between permissible FINMA requirements and those that are no longer covered by the law is blurred. In the landmark decision BGE 143 II 162, the Federal Supreme Court largely supported FINMA when it implemented the FATF recommendations – without first amending the AMLA – on the basis of AMLO-FINMA and subsequently called on the SROs to amend their regulations accordingly. In fact, the Federal Supreme Court considered the FATF recommendations as "technical clarifications to ensure a nationally or internationally recognized 'minimum standard'", the implementation of which FINMA is allowed to enforce on the basis of AMLO-FINMA.

II. CONTENT OF THE REGULATIONS (PARA. 2 AND 3)

A. Specification of the due diligence requirements under Chapter 2 (para. 2)

6 Pursuant to Art. 25 para. 2 AMLA, the SRO regulations must specify the due diligence requirements for financial intermediaries under Chapter 2 (1) and (2) define how these obligations are to be fulfilled. Since the "**specification of**" the due diligence requirements naturally includes the "definition of how they are to be fulfilled", the second part of the sentence has no independent meaning.

7 It is questionable which provisions fall under the "due diligence requirements for financial intermediaries in accordance with the second chapter". The provisions of the second chapter that relate to dealers are clearly excluded, since dealers are not subject to SRO supervision and are therefore not the addressees
of the SRO regulations. Grammatical interpretation indicates that the **scope of application** of Article 25, para. 2 AMLA is limited to the first section of the second chapter, entitled "Due diligence requirements of financial intermediaries", which includes Articles 3 to 8 AMLA. The same conclusion is reached

by the systematic interpretation in connection with Art. 25 para. 3 let. b AMLA, which refers to the entire second chapter entitled "Duties". In terms of content, Articles 9 to 11a AMLA, due to their high level of detail, correspond less to the provisions of framework legislation and therefore require less concretization than Articles 3 to 8 AMLA. FINMA also appears to take this view, since the SRO regulations it has approved either adopt the wording of Arts. 9 to 11a AMLA unchanged or simply refer to the relevant legal provisions.

As explained above, the provisions of the SRO regulations that substantiate the due diligence requirements essentially correspond to the provisions of AMLO-FINMA. This applies all the more to organizations that, in addition to being recognized as a self-regulatory organization, are also licensed as a **supervisory organization** in accordance with Article 43a FINMASA: Their SRO regulations refer directly to the AMLO-FINMA. 8

B. Requirements for the affiliation and exclusion of financial intermediaries (para. 3 let. a)

According to Art. 25 para. 3 let. a AMLA, the SRO regulations must govern the requirements for the affiliation and exclusion of financial intermediaries. Although Art. 25 AMLA assumes "one set of regulations", it is possible to regulate the contents in accordance with Art. 25 paras. 2 and 3 AMLA in **several sets of regulations** or in the statutes of the SRO; in this case, all these regulations must be submitted to FINMA for approval in accordance with Art. 18 para. 1 let. c AMLA. 9

With regard to the conditions for **joining an** SRO, Art. 14, para. 2 and 3 AMLA must be observed: Pursuant to Art. 14, para. 2 AMLA, a financial intermediary is entitled to join an SRO if (a) it ensures compliance with the obligations under the AMLA by means of its internal regulations and operational organization, (b) it enjoys a good reputation and offers a guarantee of compliance with the obligations AMLA, (c) the persons who are entrusted with its administration and management also fulfill the conditions set out in lit. b, and (d) the qualified participants in it enjoy a good reputation and guarantee that their influence will not be detrimental to prudent and sound business activity. Pursuant to Art. 14 para. 3 AMLA, the SRO may also make affiliation dependent on activities in certain areas. The SRO regulations may not provide for any affiliation requirements that go beyond 10

the conditions expressly stated in Art. 14 para. 2 and 3 AMLA, as these are "maximum requirements".

11 The conditions for the **exclusion of** financial intermediaries arise from both supervisory and private law: an exclusion, i.e. the involuntary loss of membership, can be based either on violations of anti-money-laundering legislation (including criminal provisions) or on the violation of mere membership obligations, such as non-payment of membership fees. While exclusion under anti-money-laundering legislation is the *ultima ratio* sanction for violations of the law, for (most) SROs organized as an association under Art. 60 et seq. CC) – it is also the most important sanction that can be imposed on an SRO. The law on associations (Art. 72 CC) stipulates that a member must have committed a ground for exclusion. If there is no specific provision for the grounds for exclusion, an exclusion is only permissible for good cause (Art. 72 para. 3 CC).

12 If membership is based on a legal claim, such that there is an **entitlement to admission** – as is the case for financial intermediaries under Art. 2 para. 3 AMLA based on Art. 14 para. 2 AMLA – exclusion is only permissible if there are important reasons. Even though the legislator left the provision unchanged despite the introduction of the right of admission under Art. 14 AMLA, it cannot be automatically concluded that conditions for exclusion can be defined outside the scope of important reasons. Even before the introduction of the right of admission under Article 14, para. 2 AMLA, when the financial intermediary could still choose between SRO affiliation and direct supervision by FINMA, the prevailing doctrine affirmed that financial intermediaries were subject to compulsory admission, so that the SRO's right of exclusion was already restricted at that time and could only be exercised for important reasons. In its judgment BGE 123 III 193, the Federal Supreme Court also ruled that if "[...] an association presents itself to the public as well as to authorities, potential clients of its members, etc. as the authoritative organization of the profession or economic sector in question," there must be good cause for exclusion: Without such a reason, the (de facto) ban on activity associated with exclusion cannot be justified in view of the right of personality to economic development (Art. 28 CC). Christen/Kuert assume that, in accordance with this Federal Supreme Court practice, good cause for exclusion must exist only if the consequence is that the financial intermediary can no longer carry out financial intermediary activities in Switzerland. This applies

above all to financial intermediaries for whom only a single industry SRO is available, but less so for those who have the option of joining another SRO.

Although an SRO may not stipulate "failure to be excluded from an SRO" in its regulations as an (additional) condition for affiliation, since Art. 14, para. 2 and 3 AMLA are of an exhaustive nature. However, the exclusion or the facts that led to the exclusion may have a negative impact when examining the good reputation and the **guarantee of** the financial intermediary and/or its governing bodies in accordance with Art. 14 para. 2 lit. b and c AMLA. For this reason, the view expressed here is that caution is required when defining exclusion requirements outside the area of important reasons: Any exclusion requirements defined outside the area of important reasons must therefore be based on violations of anti-money laundering legislation (including criminal provisions) and meet the requirements for prudential supervisory sanctions under Art. 25 para. 3 let. c AMLA, i.e. they must be "appropriate" (Art. 25 para. 3 let. c AMLA) or "proportionate". 13

C. Monitoring compliance with the duties under Chapter 2 (para. 3 let. b)

According to Art. 25 para. 3 let. b AMLA, the regulations must also define "how compliance with the duties under Chapter 2 is **monitored**". The wording of this provision is thus broader than that of Art. 25 para. 2 AMLA, which mentions "the due diligence requirements in accordance with Chapter 2": It includes "the obligations under Chapter 2", thus not only Art. 3 to 8 AMLA, but also Art. 9 to 11a AMLA, excluding the provisions of Chapter 2 concerning dealers. SROs must therefore monitor compliance not only with the duties of due diligence under Arts. 3 to 8 AMLA, as specified in the SRO regulations, but also with Arts. 9 to 11a AMLA. With regard to the latter provisions, the SROs must only monitor compliance with the statutory provisions, as Art. 9 to 11a AMLA do not fall within the scope of Art. 25, para. 2 AMLA and therefore do not have to be specified by the SROs, nor are they allowed to do so. 14

The fact that an SRO must be in a position to monitor whether the affiliated financial intermediaries are complying with their duties in accordance with Chapter 2 is already a **condition for recognizing the SRO** (Art. 24, para. 1, let. b AMLA). From the point of view of the doctrine, this includes adequate organization, sufficient staff and sufficient financial resources. 15

16 Art. 25, para. 3, let. b AMLA also requires that the **manner in which** the control of compliance with the duties under Art. 3 to 11a AMLA is regulated in the SRO regulations ("how"). According to the legislator, this should be done "by means of suitable procedural standards". In all other respects, the legislator leaves the determination of the control modalities to the SROs. According to the doctrine, the regulations of an SRO must contain a control concept and answer a minimum set of questions, such as whether the AMLA audit is carried out by internal or external auditors, whether or not the AMLA audit is announced, and in what form the SRO reports.

17 Analysis of the SRO regulations shows that the answers given by the SROs to these questions vary. There are a number of **differences,** including the audit frequency and the sampling method, which are highlighted below as examples. Firstly, the ordinary audit is usually carried out annually. Depending on the SRO and risk category, however, the audit frequency can be increased to a maximum of two or three years on a risk-based approach. While certain SROs increase the audit frequency on their own initiative as part of the risk analysis, with other SROs this is only possible at the request of the financial intermediary. On the other hand, there are differences in the sampling method. Their selection and scope is determined by a risk-based approach, sometimes combined with tabular specifications that determine the sample size of the mandates in numerical terms, or the obligation to audit all business relationships with increased risks. It follows that FINMA, as the approval authority for SRO regulations, appears to support the autonomy of the SRO in designing its control modalities.

D. Appropriate sanctions (para. 3 let. c)

18 Based on Art. 25 para. 3 let. c AMLA, the regulations must define "appropriate sanctions". The systematic approach of Art. 25 AMLA determines which violations of obligations the regulations must provide for "appropriate sanctions": Since the regulations, based on Art. 25 para. 3 let. b AMLA, must govern the control of compliance with all the obligations of the second chapter, i.e. Art. 3 to 11a AMLA (excluding the duties applying only to dealers), it can be assumed that, as a consequence, Art. 25 para. 3 let. c AMLA requires sanctions for violations of all **duties of the second chapter**.

19 From the perspective of the doctrine, a sanction is "appropriate" if it is "**proportionate**", whereby the standard of the sanctions of FINMA according to

Art. 31 et seq. FINMASA can be applied by analogy. In addition to examining the objective breach of duty, i.e. the violation of a regulatory or legal duty by an action or omission, the proportionality test requires that the fault of the person concerned be taken into account. In this sense, the present provision not only requires that the principle of proportionality be observed in the specific case (at the "application of the law" level), but also at the "law-making" level, i.e. when the generally abstract provisions of the regulations are being defined. Although this understanding of proportionality can only be taken into account to a limited extent in the context of "law-making", it nevertheless requires a well-thought-out cascade of sanctions as a basis for an appropriate sanction in the context of "law enforcement". Against this background, regulations generally provide for the following types of sanction, in ascending order of severity: a warning, a fine and exclusion from the SRO.

20 According to the legislator, case law and doctrine, SRO sanctions are **of a private nature.** Accordingly, the fines are contractual penalties within the meaning of Art. 160, para. 1 CO.

21 It should be noted that in the assessment of the legal relationship between the SRO and its affiliated members, there appears to be a general tendency towards a **weighting** in the direction of public law, which has been reinforced not least by the introduction of the supervisory organizations under Art. 43a FINMASA. In its judgment 2C_887/2017 of 23 March 2021, the Federal Supreme Court confirmed the private-law character of the sanctioning mechanism of the SRO PolyReg; however, it emphasized that due to the development of the fight against money laundering in Switzerland in recent decades – from its initial form of purely private self-regulation to an essential public task – the Federal Supreme Court does not rule out the possibility that in the future the sanctions under money laundering law will be qualified as public law.

22 According to the view represented here, SROs are in any case bound by **fundamental rights** based on the assumption of state functions according to Art. 35 para. 2 FC and must observe the principles of state action according to Art. 5 para. 2 FC. The sanctioning procedure is therefore subject to the principle of equality before the law (Art. 8 FC) and the prohibition of arbitrariness (Art. 9 FC), both in terms of "law-making", i.e. with regard to the sanctioning provisions of the regulations, and in terms of "law-enforcement", i.e. with regard to the specific sanctioning decisions. In the framework of the sanctioning proce-

dure, the financial intermediary must also be granted the right to be heard (Art. 29, para. 2 FC), which specifically entails the right to a reasoned decision.

BIBLIOGRAPHY

Basse-Simonsohn Detlev Michael, Geldwäschereibekämpfung und organisiertes Verbrechen, Die Sorgfaltspflichten der Finanzintermediäre und deren Konkretisierung durch Selbstregulierung, Bern 2002.

de Capitani Werner, in: Schmid Niklaus (Hrsg.), Kommentar Einziehung, Organisiertes Verbrechen, Geldwäscherei, Band II, Zürich 2002.

Christen Marquard/Kuert Matthias, Kommentierung zu Art. 25 GwG, in: Peter Ch. Hsu/Daniel Flühmann (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Graber Christoph K./Oberholzer Dominik, Das neue GwG, 3. Aufl., Zürich 2009.

Kunz Michael, Aktuelle Entwicklungen bei der Bekämpfung der Geldwäscherei, Teil II: Änderungen 2020, in: Jusletter 9. März 2020.

Kuster Matthias, Zur Rechtsnatur der Sanktionsentscheide von Selbstregulierungsorganisationen und der Schweizer Börse, in: AJP 2005, S. 1502 ff.

Heierli Christian Marcus, Das Konzept der Selbstregulierung im GwG, in: GesKR 2010, S. 38 ff.

Hsu Peter/Bahar Rashid/Flühmann Daniel, Kommentierung zu Art. 33 FINMAG, in: Watter Rolf/Bahar Rashid (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

Neese Martin, Kommentierung zu Art. 24 GwG, in: Peter Ch. Hsu/Daniel Flühmann (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Ramelet Nicolas, Sorgfaltspflichten für «Händler» – Auslegeordnung einer Kompromisslösung, in: AJP 2015, S. 1160 ff.

Riemer Hans Michael, Kommentierung zu Art. 72 ZGB, in: Berner Kommentar, Kommentar zum schweizerischen Privatrecht, Zivilgesetzbuch, Die juristischen Personen, Die Vereine, Art. 60-79 ZGB Art. 712m Abs. 2 ZGB (Stockwerkeigentümergemeinschaft), 2. Aufl., Bern 2023.

Schott Ansgar/Kessler Martina A., Kommentierung zu Art. 8a GwG, in: Peter V. Kunz/Thomas Jutzi/Simon Schären (Hrsg.), Stämpflis Handkommentar (SHK) zum Geldwäschereigesetz (GwG), Bern/Zürich 2017.

Thelesklaf Daniel, Kommentierung zu Art. 25 GwG, in: Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell Füssli Kommentar, Geldwäschereigesetz, 3. Aufl., Zürich 2019.

Wyss David, FINMA-Bussenkompetenz – ein wirksames Mittel zur Abschreckung?, GesKR 2024, S. 129 ff.

Zysset Pascal, Kommentierung zu Art. 25 GwG, in: Peter V. Kunz/Thomas Jutzi/Simon Schären (Hrsg.), Stämpflis Handkommentar (SHK) zum Geldwäschereigesetz (GwG), Bern/Zürich 2017.

MATERIALS

Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG) vom 17.6.1996, BBl 1996 III 1101, abrufbar unter https://www.fedlex.admin.ch/eli/fga/1996/3_1101_1057_993/de, besucht am 23.8.2024.

Geschäftsbericht 2021 des Bundesgerichts vom 17.2.2022, abrufbar unter https://www.eidgenoessischegerichte.ch/de/files/geschaeftsberichte/GB_2021_d.pdf, besucht am 23.8.2024 (zit. Geschäftsbericht 2021 des Bundesgerichts).

Organisme de Surveillance pour Intermédiaires Financiers & Trustees (SO-FIT), Règlement relatif aux obligations des affiliés à l'organisme d'autorégulation du 1.10.2020, abrufbar unter https://so-fit.ch/wp-content/uploads/2021/02/Re%CC%80glement-daffiliation.OAR_.SO-FIT.2021.pdf, besucht am 23.8.2024 (zit. Reglement SO-FIT).

PolyReg Allg. Selbstregulierungs-Verein, Reglement vom 1.3.2023, abrufbar unter https://www.polyreg.ch/uploads/20230216.reglement.final.de.pdf, besucht am 23.8.2024 (zit. Reglement SRO PolyReg).

Schweizer Verband der Investmentgesellschaften (SVIG), Prüfungsreglement vom 1.4.2023, abrufbar unter https://www.svig.org/sites/default/files/downloads/sro-pruefungsreglement_v.01.01.2023.pdf, besucht am 23.8.2024 (zit. Prüfungsreglement SRO SVIG).

Schweizerische Aktiengesellschaft für Aufsicht (AOOS), Reglement der Selbstregulierungsorganisation nach Geldwäschereigesetz, abrufbar unter https://www.aoos.ch/dataset/file/3131-20230306-aoos-sro-reglement-pdf, besucht am 23.8.2024 (zit. Reglement AOOS).

Selbstregulierungsorganisation des Schweizerischen Anwaltsverbandes und des Schweizer Notarenverbandes (SRO SAV/SNV), Reglement vom 27.6.2023, abrufbar unter https://sro-sav-snv.ch/rechtliche-grundlagen/regelwerke, besucht am 23.8.2024 (zit. Reglement SRO SAV/SNV).

Selbstregulierungsorganisation des Schweizerischen Leasingverbandes SRO/SLV, Reglement Kontrollverfahren vom 23.8.2006 (Fassung vom 10.11.2023), abrufbar unter https://www.leasingverband.ch/de/downloadFileContent?id=17326710-4035-418D-961F-14ECFEC7C80F, besucht am 23.8.2024 (zit. Reglement Kontrollverfahren SRO/SLV).

Selbstregulierungsorganisation Schweizerischer Treuhandverband (SRO-Treuhand|Suisse), Prüfgrundsätze vom 1.1.2023, abrufbar unter https://sro-treuhandsuisse.ch/fileadmin/Pruefer/Pruefgrundsaetze/Pruefgrundsaetze_2023_def.pdf, besucht am 23.8.2024 (zit. Prüfgrundsätze SRO-Treuhand|Suisse).

Verein Selbstregulierungsorganisation des Schweizerischen Versicherungsverbandes (SRO-SVV), Kontroll-, Prüf- und Sanktionsreglement, abrufbar unter https://www.sro-svv.ch/images/pdf/de_regelwerk/KPS_SRO-SVV.pdf, besucht am 23.8.2024 (zit. KPS-Reglement SRO-SVV).

VQF Verein zur Qualitätssicherung von Finanzdienstleistungen (SRO VQF), Aufsichtskonzept der Selbstregulierungsorganisation nach Geldwäschereigesetz des VQF Verein zur Qualitätssicherung von Finanzdienstleistungen in Sachen Bekämpfung der Geldwäscherei und Terrorismusfinanzierung vom 21. September 2023, abrufbar unter https://www.vqf.ch/de/vqf-downloads, besucht am 23.8.2024 (zit. Aufsichtskonzept SRO VQF).

VQF Verein zur Qualitätssicherung von Finanzdienstleistungen (SRO VQF), Reglement der Selbstregulierungsorganisation nach Geldwäschereigesetz des VQF Verein zur Qualitätssicherung von Finanzdienstleistungen in Sachen Bekämpfung der Geldwäscherei und Terrorismusfinanzierung vom 30.1.2023, abrufbar unter https://www.vqf.ch/de/vqf-downloads, besucht am 23.8.2024 (zit. Reglement SRO VQF).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 26 AMLA

A commentary by Caroline Kindler

SUGGESTED CITATION

Caroline Kindler, Commentary of art. 26 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Kindler, art. 26 AMLA N. XXX

Art. 26 Lists

[1] The self-regulatory organisations must maintain lists of their affiliated financial intermediaries and of persons to whom they refuse affiliation.

[2] They must notify FINMA of these lists and of any amendments thereto.

CONTENT

I. List-keeping requirement (para. 1) 473
A. Purpose of the lists 473
B. Publication 473
C. Legal nature 474
II. Transmission requirement (para. 2) 474
A. Addressees 474
B. Frequency 474
1. Principle 474
2. Immediate reporting requirements in the event of changes 475
a. When new members are admitted 475
b. Upon withdrawal 475
c. In the event of exclusion 475
3. Immediate reporting requirements for rejected applicants 475
C. Form 476
Bibliography 476
Materials 476

I. LIST-KEEPING REQUIREMENT (PARA. 1)

Based on Article 26 para. 1 AMLA, self-regulatory organizations (SROs) must maintain lists of affiliated financial intermediaries and of those persons who have been refused membership. 1

A. Purpose of the lists

By requiring that complete and up-to-date lists be kept for the attention of FINMA, the legislator aims to ensure seamless **control over** the supervisory relationships. 2

These lists are of central importance to FINMA in the context of its statutory **supervisory mandate** under the Anti-Money Laundering Act (Art. 1 let. f FINMASA): by comparing these lists, FINMA can check whether a financial intermediary has fulfilled its duty of affiliation under Art. 14 para. 1 AMLA or whether there are indications of illegal activity under the Anti-Money Laundering Act. In the latter case, based on Article 20 para. 1 AMLA, FINMA has the supervisory instruments at its disposal in accordance with Articles 29–37 FINMASA; in addition, based on Article 20 para. 2 AMLA, it has the option of ordering the financial intermediary's liquidation. 3

Furthermore, FINMA relies on these lists to fulfil its duty under **Art. 18a para. 1 AMLA**. According to this provision, FINMA maintains a directory of financial intermediaries under Art. 2 para. 3 AMLA that are affiliated to a self-regulatory organization. Art. 18a para. 1 AMLA supplements Art. 23 para. 2 FINMASA, which stipulates that FINMA maintains a public register of all supervised institutions: Since financial intermediaries who are members of an SRO are not considered as supervised persons within the meaning of the FINMASA, Art. 18a para. 1 AMLA was introduced to ensure the completeness of the FINMA directory. 4

B. Publication

The SRO is not obliged to publish the lists. This obligation falls exclusively to FINMA, and only with regard to financial intermediaries affiliated with an SRO (Art. 23 para. 2 FINMASA in conjunction with Art. 18a para. 1 AMLA). However, nothing prevents an SRO from providing for the publication of the list of members in its statutes or regulations, or from allowing such publication 5

with the express consent of the member concerned. However, such a list of members may only include the supervised financial intermediaries. The publication of lists of rejected applicants would lack any legal basis, if only because the statutes only apply to members and have no legal effect on rejected applicants.

C. Legal nature

6 Despite their legal significance, the lists maintained by the SROs on the basis of this provision have a purely **declaratory effect**. The SRO's decisions on admission or exclusion are decisive, as these are constitutive. Membership of the SRO therefore begins or ends on the date of the SRO's legally binding decision. This means that, in the case of incomplete or inaccurate lists, duly affiliated financial intermediaries are not prevented from lawfully carrying out their activities. Conversely, an excluded financial intermediary cannot claim that it is still included on a list.

II. TRANSMISSION REQUIREMENT (PARA. 2)

7 In addition to the duty to keep lists in accordance with Art. 26, para. 1 AMLA, SROs are obliged under Art. 26, para. 2 AMLA to notify FINMA of these lists and of any changes to them.

A. Addressees

8 The law only provides for this provision to apply to **SROs**. If a financial intermediary that has been newly admitted by an SRO or an applicant that has been rejected informs FINMA of its status, this will have no effect, as FINMA is not permitted to take into account such reports from persons who are not subject to its supervision.

B. Frequency

1. Principle

9 The lists of affiliated financial intermediaries and rejected applicants are to be aggregated and sent to FINMA **on a quarterly basis**.

10 In addition, based on Art. 26 and Art. 27, Para. 2 AMLA and the FINMA Circular 2008/17 (formerly the Circular of the AMLA Control Authority 2006/1), the

SRO is entitled and obliged to report further information to FINMA **without delay** regarding the number of affiliated financial intermediaries (2.) or rejected applicants (3.). The exceptions are set out below.

2. Immediate reporting requirements in the event of changes

a. When new members are admitted

In addition to the ordinary quarterly report, the SRO is entitled to report the **admission of** a financial intermediary to FINMA at any time, provided this is in the interest of the financial intermediary. Furthermore, the SRO is obliged to report to FINMA immediately after affiliation if it knows or must assume on the basis of the circumstances that the affiliated financial intermediary has violated the obligations of Art. 11, para. 1, let. b AMLO. This is the case if the financial intermediary has failed to submit an application for affiliation to an SRO within two months of commencing his professional activity. 11

b. Upon withdrawal

In addition to the ordinary quarterly report, the SRO is obliged to report the **termination of membership** to FINMA immediately after the membership has ended, provided that the SRO knows or must assume that the terminating member will continue to pursue a professional activity. The letter of termination must be enclosed with the report. 12

c. In the event of exclusion

The SRO shall report **exclusion decisions** to FINMA without delay as soon as the first-instance decision has been issued, provided that any appeal has been withdrawn or after the first-instance decision has become legally binding or the arbitration court ruling in all other cases. The reasons for the decision must be enclosed with the report if available. 13

3. Immediate reporting requirements for rejected applicants

If the SRO **refuses to** admit an applicant, it shall report this to FINMA immediately after the first-instance decision has been issued, enclosing the reasons if these are available. If the SRO knows or must assume that a financial intermediary to which affiliation has been refused is or was operating in violation of Art. 11 para. 1 let. b AMLO, it shall report this to FINMA as part of the noti- 14

fication mentioned in the previous sentence, providing all relevant information known to the SRO.

C. Form

15 There are currently no specific rules for the electronic exchange between FINMA and the SRO. However, the **digital platforms of FINMA**, which have been continuously expanded in recent years, have considerably facilitated and promoted the electronic transmission of data.

BIBLIOGRAPHY

de Capitani Werner, in: Schmid Niklaus (Hrsg.), Kommentar Einziehung, Organisiertes Verbrechen, Geldwäscherei, Band II, Zürich 2002.

Jain Vivien/Frigo Patrick, Kommentierung zu Art. 18a GwG, in: Peter Ch. Hsu/Daniel Flühmann (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Neese Martin, Kommentierung zu Art. 26 GwG, in: Peter Ch. Hsu/Daniel Flühmann (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Ramelet Nicolas, Kommentierung zu Art. 26 GwG, in: Peter V. Kunz/Thomas Jutzi/Simon Schären (Hrsg.), Stämpflis Handkommentar (SHK) zum Geldwäschereigesetz (GwG), Bern/Zürich 2017.

Zufferey Jean-Baptiste, Kommentierung zu Art. 26 GwG, in: Cassani Ursula/Bovet Christian/Villard Katia (Hrsg.), Commentaire Romand, Loi sur le blanchiment d'argent, Basel 2022.

MATERIALS

Association romande des intermédiaires financiers (ARIF), Liste des membres, abrufbar unter https://arif.ch/membres/liste-des-membres-2/, besucht am 23.8.2024.

Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG) vom 17.6.1996, BBl 1996 III 1101, abrufbar unter https://www.fedlex.admin.ch/eli/fga/1996/3_1101_1057_993/de, besucht am 23.8.2024.

Eidgenössische Finanzmarktaufsicht (FINMA), Rundschreiben 2008/17 Informationsaustausch zwischen den SRO und der FINMA betreffend Anschlüsse, Ausschlüsse und Austritte von Finanzintermediären vom 20.11.2008, abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2008-17.pdf?sc_lang=de&hash=71FFD4758724C36DBC692710A9C8477B, besucht am 23.8.2024.

Eidgenössische Finanzverwaltung (EFV), Kontrollstelle GwG, Rundschreiben 2006/1 Informationsaustausch zwischen den SRO und der Kontrollstelle betreffend Anschlüsse, Ausschlüsse und Austritte von Finanzintermediären vom 10.4.2006, abrufbar unter https://www.finma.ch/finmaarchiv/gwg/d/dokumentationen/gesetze_und_regulierung/rundschreiben/index.php, besucht am 23.8.2024.

Schweizerische Aktiengesellschaft für Aufsicht (AOOS), Liste der angeschlossenen Finanzintermediäre, abrufbar unter https://www.aoos.ch/de/angeschlossene-sro, besucht am 23.8.2024.

Selbstregulierungsorganisation des Schweizerischen Leasingverbandes SRO/SLV, Liste der Mitglieder, abrufbar unter https://www.leasingverband.ch/de/schweizerischer-leasingverband-slv/ueber-uns/mitglieder/index.html, besucht am 23.8.2024.

Selbstregulierungsorganisation Schweizerischer Treuhandverband (SRO-Treuhand|Suisse), Mitgliederliste 2024, abrufbar unter https://sro-treuhandsuisse.ch/de/sro-treuhandsuisse/mitgliederliste-der-sro-treuhandsuisse, besucht am 23.8.2024.

Verein Selbstregulierungsorganisation des Schweizerischen Versicherungsverbandes (SRO-SVV), Mitgliederliste, abrufbar unter https://www.sro-svv.ch/de/ueber-uns/mitglieder, besucht am 23.8.2024.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 26a AMLA

A commentary by Caroline Kindler

SUGGESTED CITATION

Caroline Kindler, Commentary of art. 26a AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Kindler, art. 26a AMLA N. XXX

Art. 26a Swiss group companies

[1] FINMA may provide for financial intermediaries in accordance with Article 2 paragraph 3 that are Swiss group companies of a financial intermediary in accordance with Article 2 paragraph 2 letters a–d^{quater} that proof of compliance with the obligations specified in Chapter 2 may be provided in the audit report for the group.

[2] FINMA shall publish a list of group companies in accordance with paragraph 1.

CONTENT

I. Purpose and background 481
II. Requirements 481
A. Financial intermediaries in accordance with Art. 2 para. 3 AMLA 482
B. Financial intermediaries in accordance with Art. 2 para. 2 let. a–dquater AMLA 482
C. Domestic group company 483
1. Group company 483
2. "Domestic" group company 483
III. Legal consequence 484
A. "Optional provision" 484
B. Subject of the audit 485
C. Audit requirements 485
IV. List of FINMA 485
Bibliography 485
Materials 486

I. PURPOSE AND BACKGROUND

A financial intermediary under Art. 2 para. 3 AMLA is in principle subject to individual supervision. This focuses on the individual institution, which, however, can lead to a lack of **comprehensive understanding of money laundering risks within the entire corporate** group. To fill this gap, Art. 26a AMLA enables consolidated AMLA supervision. This is intended to supplement the supervision of individual institutions in view of the economic unity of the group. Consolidated supervision thus allows for a continuous double view – both at the level of the individual institution and at the group level. 1

FINMA's authority to subject corporate groups to consolidated AMLA supervision originally goes back to **Art. 4 aGwV-FINMA**. This regulation applied to both so-called "DUFI" (financial intermediaries directly subordinated to FINMA in accordance with Art. 2 para. 3 AMLA) and to holders of a "fintech license" (persons in accordance with Art. 1b BankG). When the FinIA came into force on January 1, 2020, Article 4 of the AMLA-FINMA was transferred to the legislative level in Article 26a AMLA. At the same time, the group of addressees was specified: in view of the abolition of the DSFI status as of January 1, 2020, this now includes all financial intermediaries according to Art. 2 para. 3 AMLA that are part of a financial group. However, persons according to Art. 1b BankG, i.e. holders of a fintech license, were not included in the group of addressees of Art. 26a AMLA. Thus, these persons do not have the option of consolidated AMLA supervision, since the provisions on consolidated supervision in the Banking Act do not apply to them. The reasons for their exclusion from the scope of the provisions are not apparent from the materials, since Art. 26a AMLA was not the subject of the dispatch on the FinSA/FinIA, but was only added during the parliamentary deliberations. In practice, however, this question is of little significance – at least for the time being – since none of the (five) holders of a fintech license is part of a group as of the cut-off date of July 1, 2024. 2

II. REQUIREMENTS

Article 26a AMLA applies to "financial intermediaries in accordance with Article 2 paragraph 3" that are considered "domestic group companies" of a "fi- 3

nancial intermediary in accordance with Article 2 paragraph 2 letters a–d^{quater}". These concepts are explained below.

A. Financial intermediaries in accordance with Art. 2 para. 3 AMLA

4 Financial intermediaries in accordance with Art. 2 para. 3 AMLA are persons who professionally accept or hold assets belonging to third parties or who assist in the investment or transfer of such assets. Examples of such financial intermediaries are listed in Art. 2 para. 3 let. a–c, f and g AMLA. The definition of such a financial intermediary is specified in the AMLO and in FINMA Circular 2011/1.

B. Financial intermediaries in accordance with Art. 2 para. 2 let. a–d^{quater} AMLA

5 The regulation of Article 26a AMLA refers to domestic group companies of financial intermediaries in accordance with Article 2, para. 2, let. a–d^{quater} AMLA. This refers to the following financial intermediaries in accordance with Article 2, para. 2 AMLA (**and exclusively**):

- banks in accordance with Art. 1a BankG and persons in accordance with Art. 1b BankG (lit. a);
- asset managers and trustees in accordance with Art. 2 para. 1 let. a and b FinIA (lit. a^{bis});
- fund management companies in accordance with Art. 2 para. 1 let. d FinIA (lit. b);
- licensees in accordance with Article 13 para. 2 let. b–d CISA and managers of collective assets in accordance with Article 2 para. 1 let. c FinIA (let. b^{bis});
- Insurance institutions in accordance with the ISA that operate direct life insurance or offer or distribute units in a collective investment scheme (c);
- Investment firms in accordance with Article 2 paragraph 1 letter e FinIA (d);
- Central counterparties and central securities depositories in accordance with the FinMIA (d^{bis});

- payment systems, provided they require a license from FINMA in accordance with Article 4 para. 2 FinMIA (lit. d^{ter});
- trading facilities for DLT securities in accordance with Article 73a FinMIA (DLT trading facilities; lit. d^{quater}).

C. Domestic group company

1. Group company

The terms "group of companies" and "group" are used synonymously. However, Swiss corporate group law does not have a uniform or generally valid concept of a group. The characteristics of a group of companies are defined individually in the various areas of law. Accordingly, the basic assumptions and legal criteria regarding the existence or non-existence of a group can differ considerably depending on the area of law. Nevertheless, all group concepts in Swiss law are based on three constitutive characteristics: Firstly, the individual group companies are legally independent entities, whereby their legal form can vary depending on the level in the hierarchy. Secondly, a group requires at least two companies – a parent company and at least one subsidiary. Thirdly, the link between the companies, the "glue", so to speak, is a unified management (so-called "group management"). In the context of the AMLA, the group is considered an **economic unit** if a company directly or indirectly holds more than half of the votes or capital of another company or controls it in some other way. The participations can be held both directly and indirectly, i.e. through other group companies. This means that both direct and indirect subsidiaries can be found across several hierarchical levels. 6

2. "Domestic" group company

As with Art. 2 para. 3 AMLA, the territorial scope of Art. 26a AMLA is limited to financial intermediaries that, in accordance with Art. 2 para. 1 let. a AMLO, operate **in or from Switzerland**. The financial intermediary under Art. 2 para. 3 AMLA or the domestic group company must therefore have its registered office in Switzerland and employ persons who permanently carry out financial intermediary business in Switzerland or from Switzerland. A subsidiary or branch of a foreign financial group, on the other hand, does not meet the requirements, since the controlling company must be a licensee un- 7

der Art. 2 para. 2 let. a–d^{quater} AMLA and must therefore also be considered a domestic group company.

III. LEGAL CONSEQUENCE

A. "Optional provision"

8 Article 26a AMLA is an "**optional provision**": if the conditions are met, i.e. if a financial intermediary under Article 2 para. 3 AMLA is a domestic group company of a financial intermediary in accordance with Article 2 para. 2 let. a–d^{quater} AMLA, FINMA "may" request a consolidated AMLA audit report. This means that FINMA can order such a report without the prior involvement or request of the financial intermediary. Conversely, it is possible for a domestic group company or a financial intermediary supervised by FINMA to request consolidated AMLA supervision from FINMA in accordance with Art. 2 para. 2 let. a–d^{quater} AMLA. Although FINMA states on its homepage that the content and scope of consolidated group supervision are determined by it on a case-by-case basis, It also states that it checks in particular whether the financial group:

- is appropriately organized;
- has an appropriate internal control system;
- appropriately records, limits and monitors the risks associated with its business activities;
- is managed by persons who guarantee proper business conduct;
- complies with the personnel separation between management, governance, supervision and control;
- complies with the capital and risk diversification requirements;
- has adequate liquidity;
- correctly applies the accounting rules;
- has a recognized, independent and knowledgeable audit firm.

It can therefore be assumed that an application by a group company for the ordering of a group audit report in the area of AMLA must include proof of the above points.

B. Subject of the audit

Art. 26a para. 1 AMLA requires that the group audit report verify compliance with the "obligations under Chapter 2". The wording of this provision is thus broader than that of Art. 25 para. 2 AMLA, for example, which only mentions the "due diligence obligations" under Chapter 2. Art. 26a AMLA, on the other hand, covers all "obligations under Chapter 2" and thus not only **Art. 3 to 8 AMLA** but also **Art. 9 to 11a AMLA**, excluding the provisions of Chapter 2 concerning dealers. The group audit report must therefore document compliance with both the due diligence requirements under Arts. 3 to 8 AMLA and the obligations under Arts. 9 to 11a AMLA. 9

C. Audit requirements

The audit process is regulated in **Art. 24 et seq. FINMASA** in conjunction with the Financial Market Auditing Ordinance (FINMA-PV). Among other things, the FINMA-PV specifies the licensing of audit firms and the auditing of supervised institutions in accordance with FINMASA. Further audit instructions are contained in FINMA Circular 2013/3, which also forms the basis for specific guidelines on regulatory audits on the FINMA website. It should be emphasized that, despite the consolidated group audit report, reporting on the individual institution and the group must, in principle, be done separately. 10

IV. LIST OF FINMA

Pursuant to Art. 26a para. 2 AMLA, FINMA publishes the list of group companies pursuant to Art. 26a para. 1 AMLA. As of the reporting date of July 1, 2024, such a list had **not yet** been published. It can therefore be concluded that no order within the meaning of Art. 26a AMLA had been issued by that date. 11

BIBLIOGRAPHY

Kunz Peter V., Wirtschaftsrecht, Grundlagen und Beobachtungen, Bern 2019.

Nobel Peter, Bank- und Finanzkonglomerate – eine aufsichtsrechtliche Auslegeordnung, Aktuelle Rechtsprobleme des Finanz- und Börsenplatzes Schweiz, Band 8/1999, Bern 2000, S. 171 ff.

MATERIALS

Amtliche Sammlung Nr. 155 vom 8.12.2020 zur Verordnung der Eidgenössischen Finanzmarktaufsicht über die Finanzinstitute (Finanzinstitutsverordnung-FINMA, FINIV-FINMA), abrufbar unter https://www.fedlex.admin.ch/eli/oc/2020/922/de, besucht am 23.8.2024 (zit.: AS 2020 5327).

Botschaft zum Finanzdienstleistungsgesetz (FIDLEG) und zum Finanzinstitutsgesetz (FINIG) vom 4.11.2015, BBl 2015 8901, abrufbar unter https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2015/2141/de/pdf-a/fedlex-data-admin-ch-eli-fga-2015-2141-de-pdf-a.pdf, besucht am 23.8.2024.

Eidgenössische Finanzmarktaufsicht (FINMA), Rundschreiben 2011/1 Tätigkeit als Finanzintermediär nach GwG, Ausführungen zur Geldwäschereiverordnung vom 4.11.2020, abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2011-01-01-01-2017.pdf?la=de, besucht am 23.8.2024.

Eidgenössische Finanzmarktaufsicht (FINMA), Rundschreiben 2013/3 Prüfwesen vom 7.12.2022, abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2013-03-20221207.pdf, besucht am 23.8.2024.

Eidgenössische Finanzmarktaufsicht (FINMA), Spezifische Anforderungen der FINMA an das Prüfwesen bei aufsichtsrechtlichen Prüfungen, abrufbar unter https://www.finma.ch/de/ueberwachung/branchenuebergreifende-themen/pruefwesen/, besucht am 23.8.2024.

Geschäft des Bundesrates Nr. 15.073 Finanzdienstleistungsgesetz (FIDLEG) und Finanzinstitutsgesetz (FINIG), Fahne Herbstsession 2017 Nationalrat, abrufbar unter https://www.parlament.ch/centers/eparl/curia/2015/20150073/N2%20D.pdf, besucht am 23.8.2024 (zit.: BR-Geschäft Nr. 15.073, Fahne Herbstsession 2017 NR).

Liste der von der FINMA bewilligten und beaufsichtigten Vermögensverwaltern sowie Trustees (inländische Gruppengesellschaften nach FINIG), abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/bewilligungstraeger/pdf/grfinig.pdf?la=de&hash=75FE-FE0A120F46AC945E8E4A20CF128C, besucht am 23.8.2024.

Liste der von der FINMA bewilligten Personen nach Art. 1b BankG (Fintech-Bewilligung), abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/bewilligungstraeger/pdf/fintech.pdf?sc_lang=de&hash=6C56E843908149147A3CC22EAB7DE1C6, besucht am 23.8.2024.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 27 AMLA

A commentary by Caroline Kindler

SUGGESTED CITATION

Caroline Kindler, Commentary of art. 27 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Kindler, art. 27 AMLA N. XXX

Art. 27 Exchange of information and duty to report

[1] The self-regulatory organisations and FINMA may mutually exchange any information or documents that they require in order to fulfil their duties.

[2] The self-regulatory organisations shall notify FINMA of:

a. terminations of memberships;

b. decisions on the refusal of affiliation;

c. decisions to exclude and the reasons therefor;

d. the opening of sanctions proceedings that may end in exclusion.

[3] They shall provide FINMA with a report at least once each year on their activities in terms of this Act together with a list of decisions on sanctions issued during the period covered by the report.

[4] They shall immediately submit a report to the Reporting Office if they have reasonable grounds to suspect that:

a. a criminal offence under Article 260ter or 305bis of the Swiss Criminal Code has been committed;

b. assets are the proceeds of a felony or an aggravated tax misdemeanour under Article 305bis number 1bis SCC;

c. assets are subject to the power of disposal of a criminal or terrorist organisation; or

d. assets serve the financing of terrorism (Art. 260^{quinquies} para. 1 SCC).

[5] The duty under paragraph 4 does not apply if a report has already been filed by a financial intermediary affiliated to a self-regulatory organisation.

CONTENT

I. Purpose and structure 492
II. General exchange of information between SRO and FINMA (para. 1) 492
III. Immediate duty of the SRO to inform FINMA (para. 2) 494
IV. SROs' periodic reporting obligation to FINMA (para. 3) 495
V. SRO reporting duty to MROS (para. 4 and 5) 496
1. Reporting duty (para. 4) 496
2. Subsidiarity (para. 5) 498
Bibliography 498
Materials 499

I. PURPOSE AND STRUCTURE

1 Art. 27 AMLA governs the **exchange of information** between official and non-official (supervisory) function holders within the framework of the Anti-Money Laundering Act. This provision is necessary to ensure an effective supervisory structure, since domestic administrative assistance under Art. 29 AMLA is only applicable to authorities. It should be noted that the supervisory organizations that operate an SRO in association also fall within the personal scope of application of Art. 27 AMLA.

2 Para. 1 defines the **basic principle** of the exchange of information between FINMA and the SRO and between the SROs themselves: "The self-regulatory organizations and FINMA may exchange all information and documents between themselves that they require to fulfill their task".

3 Para. 2 specifies Art. 26 para. 2 AMLA with regard to the **immediate reporting obligations of the SRO** to FINMA regarding changes in membership and also regulates other events that trigger an immediate reporting obligation to FINMA. These reporting requirements were specified in detail in FINMA Circular 2008/17 (formerly AMLA Control Authority Circular 2006/1).

4 para. 3 imposes a **periodic reporting requirement** on the SRO vis-à-vis FINMA, in that the SRO must report to FINMA at least once a year "on its activities under this Act" and "a list of the sanction decisions issued during the reporting period".

5 Para. 4 requires the SRO to report to the **Reporting Office for Money Laundering (MROS)** any facts that a financial intermediary under its supervision should have reported; para. 5 stipulates the subsidiarity of this reporting requirement, since it no longer applies if the financial intermediary has already made the report itself.

II. GENERAL EXCHANGE OF INFORMATION BETWEEN SRO AND FINMA (PARA. 1)

6 The original one-sided duty of disclosure of the SRO to the MLCA, as provided for in aArt. 19 and aArt. 27 AMLA, was replaced by the principle of information exchange with the revision that came into force on January 1, 2009. This exchange takes place both between FINMA and the SRO and between

the SROs themselves. The legislator recognized that a **mutual exchange of information** between all (supervisory) officials is more in line with practical requirements.

The legislator is thus creating the necessary **legal basis** for the exchange of information not accessible to the public between FINMA and the SRO, as well as between the SROs themselves. Art. 27 para. 1 AMLA thus not only supplements the domestic administrative assistance under Art. 29 AMLA for non-official (supervisory) functionaries, but also addresses the legal hurdles that stand in the way of the transmission or processing of information, such as those in criminal or data protection law. 7

FINMA and the SROs can act as both recipients and transmitters of "information" or "details and documents". The term "information" or "details and documents" is not defined in more detail in Art. 27 para. 1 AMLA. However, according to the view presented here, one should assume a **broad definition** that includes both oral and written information as well as the disclosure of documents, files and other records of any kind. 8

Restrictions therefore do not arise from the specific definition of these terms, but rather from the necessary connection with the fulfillment of the tasks (**principle of purpose limitation**): The exchange of information is only permissible if the information is relevant for the fulfillment of the tasks of FINMA and the SRO in the individual case. Due to the extensive tasks and competencies of both the SRO and FINMA, a very comprehensive transfer of information will probably be permissible. 9

In contrast to the unilateral information obligations of the SROs to FINMA as set out in paras. 2 and 3, Art. 27 para. 1 AMLA is formulated as an optional **provision**. This means that there is a right to exchange information, but no obligation or requirement for further coordination of supervisory activities. However, a general duty to provide information may arise in the sense that withholding essential information could contradict the objectives of financial market supervision in accordance with Art. 4 FINMASA. It should also be noted that the SROs are considered "supervised entities" within the meaning of Art. 3 let. a FINMASA and are therefore subject to the disclosure and reporting obligations to FINMA in accordance with Art. 29 FINMASA. However, these obligations apply only in relation to FINMA and not in relation to other SROs. 10

III. IMMEDIATE DUTY OF THE SRO TO INFORM FINMA (PARA. 2)

11 Art. 27 para. 2 AMLA lists the events that an SRO must report to FINMA without delay: terminations of membership (a), decisions to refuse affiliation (b), exclusion decisions and the reasons for them (c) and the opening of sanction proceedings that may end in exclusion (d). This list is presented as exhaustive. From the legislator's point of view, it is necessary that FINMA be informed immediately of the matters mentioned in Para. 2 in order to keep up to date on important decisions and proceedings of the SRO and to be able to intervene in good time if necessary.

12 Based on Article 26 AMLA, SROs are obliged to maintain lists of affiliated financial intermediaries and persons who have been refused membership and to notify FINMA of any changes. FINMA Circular 2008/17 (formerly AMLA Control Authority Circular 2006/1) specifies this provision and stipulates that these lists must be submitted to FINMA in aggregated form on a quarterly basis. In addition, individual changes in membership and rejected applicants must be reported immediately. Art. 27, para. 2 AMLA thus creates the **legal basis** for the SROs' immediate reporting obligations to FINMA in the event of changes in membership in the form of resignations and exclusions, as well as in the event of refusal of affiliation, and thus specifies the obligation to transmit information in accordance with Art. 26, para. 2 AMLA.

13 Accordingly, the **termination of** membership must be reported immediately after the membership has ended if the SRO knows or must assume that the terminating member continues to pursue a professional activity. The letter of termination must be enclosed with the report. The SRO shall report **exclusion decisions** to FINMA immediately as soon as the first-instance decision has been issued, provided that a possible appeal has been withdrawn, or after the first-instance decision has become legally binding or the arbitration court ruling in all other cases. The reasons for the decision must be enclosed with the report if available. If the SRO **refuses to** admit an applicant, it shall notify FINMA immediately after the first-instance decision has been issued, enclosing the reasons if available. If the SRO knows or must assume that a financial intermediary to which affiliation has been refused is or was operating in violation of Art. 11 para. 1 let. b AMLO, it shall report this to FINMA as part of the

notification mentioned in the previous sentence, providing all relevant information known to the SRO.

Changes to the inventory in the form of **new admissions** must also be reported to FINMA immediately in certain cases in accordance with FINMA Circular 2008/17. The SRO is obliged to inform FINMA immediately after a new financial intermediary has joined if it knows or must assume on the basis of the circumstances that the latter has violated the obligations under Art. 11, para. 1, let. b AMLO. Such a violation has occurred if the financial intermediary has failed to apply for admission to an SRO within two months of commencing its professional activity. Since this constellation does not fall within the scope of the immediate reporting obligations pursuant to Article 27, para. 2 AMLA, the legal basis for this arises from the general duty of the SRO to provide information and report to FINMA pursuant to Article 29 FINMASA. 14

The immediate reporting requirement in the event of a **withdrawn affiliation application** is also governed by FINMA Circular 2008/17. The legal basis for this is also to be found in Art. 29 FINMASA and not in Art. 27 para. 2 AMLA. In such cases, the reasons for withdrawal given to the SRO must be forwarded to FINMA. Should the SRO become aware or have reason to believe that a financial intermediary who has withdrawn their application for affiliation is violating or has violated Art. 11, Para. 1, lit. b AMLO, it must report this to FINMA, providing all relevant information known to it. 15

FINMA Circular 2008/17 does not contain any provisions on the SROs' duty to report immediately when **sanction proceedings** are initiated that could result in exclusion; however, this obligation is explicitly set out in Art. 27, para. 2, let. d AMLA. However, this provision is of limited practical significance, since the financial intermediary remains a member of the SRO and subject to its supervision until the legally binding sanction decision and a possible exclusion. 16

IV. SROS' PERIODIC REPORTING OBLIGATION TO FINMA (PARA. 3)

According to Art. 27 para. 3 AMLA, the SROs are obliged to transmit to FINMA at least once a year a **report on** their activity in the area of the Anti-Money Laundering Act, as well as a list of the sanction decisions issued during the reporting period. This reporting is one of the tools that FINMA uses to fulfil 17

its supervisory duties with respect to the SROs in accordance with Art. 18 para. 1 AMLA and to verify ongoing compliance with the SRO's recognition requirements in accordance with Art. 24 para. 1 AMLA.

18 The **structure and form** of the report are specified by FINMA. In recent years, FINMA's continuously expanded digital platforms have significantly facilitated and promoted the electronic transmission of data. Therefore, the template from the time of the Control Authority's supervision was replaced by a form on FINMA's electronic transmission platform.

19 In addition to this formalized reporting requirement, further supervisory measures by FINMA of the SROs have become established in **practical terms**: depending on FINMA's internal risk classification of the SRO, it is audited once a year, or every two or three years, as part of on-site inspections. In addition, regular supervisory discussions take place with the SRO. FINMA and the SRO also exchange information at the annual AMLA conference organized by FINMA and at the SRO forum.

V. SRO REPORTING DUTY TO MROS (PARA. 4 AND 5)

1. Reporting duty (para. 4)

20 SROs are also subject to a **reporting duty** to the Money Laundering Reporting Office Switzerland (MROS). Pursuant to Art. 27, para. 4 AMLA, it must report to MROS without delay if it has reasonable grounds to suspect that one of the following circumstances applies: a criminal offense under Art. 260ter no. 1 or 305bis SCC (lit. a), assets stem from a crime or a qualified tax offence under Art. 305bis no. 1bis SCC (lit. b), assets are subject to the power of disposal of a criminal or terrorist organization (lit. c) or assets are used to finance terrorism (Art. 260^{quinquies} para. 1 SCC) (lit. d).

21 The elements of the reporting requirement under Art. 27 para. 4 AMLA correspond essentially to the **wording of Art. 9 para. 1 AMLA**, although there are some differences, which are explained below. These differences do not, however, prevent the commentary on Art. 9 para. 1 AMLA from being used by analogy for interpretation. Unlike Art. 9, para. 1 AMLA, Art. 27, para. 4 AMLA only requires the SRO to report cases if there is reasonable suspicion. However, the obligation is not explicit if the SRO knows or has reliable information that an offence has been committed. However, it seems questionable whether

this was actually intended, or whether it is merely a legislative oversight, since it is hard to imagine that the legislature consciously wanted to deviate from the regulatory concept of the reporting requirement under Art. 9 AMLA. Furthermore, the suspicion relevant for the reporting obligation according to Art. 27 para. 4 lit. b–d AMLA refers to the assets themselves and not, as in Art. 9 para. 1 AMLA, to "the assets involved in the business relationship". If one wants to see this as intentional and does not also consider it to be legislative negligence, it could be explained by the fact that, in contrast to the financial intermediary, the supervisory authorities are not obliged to clarify the situation in accordance with Article 6 AMLA and therefore have less specific knowledge. Finally, unlike a violation of the reporting requirement under Article 9 AMLA, a violation of Article 27, para. 4 AMLA is not sanctioned under Article 37 AMLA.

22 The counterpart to Art. 27 para. 4 AMLA is Art. 16 AMLA for supervisory organizations, with the difference, however, that SROs are not subject to the duty to report violations in terms of **Art. 305ter para. 1 SCC** by their affiliated financial intermediaries: According to Art. 305ter para. 1 SCC, a financial intermediary is liable to prosecution if he fails to take the necessary due diligence to determine the identity of the beneficial owner. The legislator justified this difference by stating that, unlike the supervisory authorities established under special legislation and FINMA, SROs are subject to private law. However, since an SRO must respond appropriately to such violations as part of its supervisory activities, the facts of the case may nevertheless be reported to MROS. This is done indirectly, with the SRO reporting the sanction proceedings under Art. 27 para. 2 let. d AMLA to FINMA, which in turn files a report with MROS based on Art. 16 AMLA.

23 According to Art. 11 para. 2 AMLA, the **exclusion of criminal and liability proceedings** under Art. 11 para. 1 AMLA also expressly applies to SROs that report in accordance with Art. 27 para. 4 AMLA. Art. 11 para. 1 AMLA states that the reporting person, provided they act in good faith, "shall not be liable to any proceedings for breach of official, professional or business confidentiality nor to any liability in damages". This provision ensures that an SRO that fulfills its reporting obligation in connection with suspicious assets in accordance with Art. 27 para. 4 AMLA does not have to fear any civil or criminal consequences. Art. 11 AMLA thus resolves the conflict between contradictory rights and obligations. The underlying general legal principle is based on the

obvious fact that the law cannot prescribe or permit and at the same time punish one and the same behavior of a person. In criminal law, this principle is expressly enshrined in Art. 14 SCC. The same considerations also apply to the exclusion of liability under civil law: civil liability for reporting is therefore excluded, although this exclusion already applies at the level of the facts and not only when examining fault. Thus, for example, the assumption of illegality within the meaning of Art. 41 CO does not apply.

2. Subsidiarity (para. 5)

24 The reporting duty of the SRO under Art. 27, para. 4 AMLA is **subsidiary**, i.e. it only applies if the financial intermediary itself has not reported anything to the MROS (Art. 27, para. 5). Conversely, this means that the SRO is released from the reporting requirement under Art. 27, para. 4 AMLA if the affiliated financial intermediary has already submitted a corresponding report. On the other hand, the SRO's reporting obligation takes precedence if the report relates directly to the financial intermediary, based on the assumption that a financial intermediary is not likely to report suspicious assets within his own organization.

BIBLIOGRAPHY

Benninger Nora/Wyss David, 65. Zusammenarbeit mit anderen inländischen Behörden, S. 300 ff., in: Zulauf Urs/Wyss David (Hrsg.), Finanzmarktenforcement, 3. Aufl., Bern 2002.

Beuret Arnaud, Kommentierung zu Art. 16 GwG, in: Peter V. Kunz/Thomas Jutzi/Simon Schären (Hrsg.), Stämpflis Handkommentar (SHK) zum Geldwäschereigesetz (GwG), Bern/Zürich 2017.

de Capitani Werner, in: Schmid Niklaus (Hrsg.), Kommentar Einziehung, Organisiertes Verbrechen, Geldwäscherei, Band II, Zürich 2002.

Häfelin Ulrich/Müller Georg/Uhlmann Felix, Allgemeines Verwaltungsrecht, 8. Aufl., Zürich/St. Gallen 2020.

Ivell Katrin, Kommentierung zu Art. 16 GwG, in: Peter Ch. Hsu/Daniel Flühmann (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Kuster Matthias, Zur Abgrenzung des Melderechts nach Art. 305ter Abs. 2 StGB von der Meldepflicht nach Art. 9 GwG, in: Jusletter vom 26. Juni 2017.

Neese Martin, Kommentierung zu Art. 27 GwG, in: Peter Ch. Hsu/Daniel Flühmann (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Niggli Marcel Alexander/Göhlich Carola, Kommentierung zu Art. 14 StGB, in: Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Strafgesetzbuch, Jugendstrafrecht, 4. Aufl., Basel 2019.

Porpiglia Gianni/Kunz Oliver M., Kommentierung zu Art. 11 GwG, in: Peter Ch. Hsu/Daniel Flühmann (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Ramelet Nicolas, Kommentierung zu Art. 27 GwG, in: Peter V. Kunz/Thomas Jutzi/Simon Schären (Hrsg.), Stämpflis Handkommentar (SHK) zum Geldwäschereigesetz (GwG), Bern/Zürich 2017.

Schwob Renate/Wohlers Wolfgang, Kommentierung zu Art. 39 FINMAG, in: Watter Rolf/Bahar Rashid (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz / Finanzmarktinfrastrukturgesetz (FINMAG/FinfraG), 3. Aufl., Basel 2019.

Stadler Stephan, Die gelenkte Selbstregulierung im Bereich der Geldwäscherei, LeGes 2006/3, S. 49-58.

Vollenweider Marino/Parigi Gianluca, Kommentierung zu Art. 88 FIDLEG, in: Sethe Rolf/Bösch René/Favre Olivier/Kramer Stefan/Schott Ansgar (Hrsg.), Kommentar zum Finanzdienstleistungsgesetz FIDLEG, Zürich/Basel/Genf 2021.

Zufferey Jean-Baptiste, Kommentierung zu Art. 27 GwG, in: Cassani Ursula/Bovet Christian/Villard Katia (Hrsg.), Commentaire Romand, Loi sur le blanchiment d'argent, Basel 2022.

MATERIALS

Amtliche Sammlung des Bundesrechts, Nr. 11, 24.3.1998, Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG), S. 892 ff., abrufbar unter https://www.amtsdruckschriften.bar.admin.ch/viewOrigDoc/30002712.pdf?id=30002712, besucht am 23.8.2024.

Botschaft zum Bundesgesetz über die Eidgenössische Finanzmarktaufsicht (Finanzmarktaufsichtsgesetz; FINMAG) vom 1.2.2006, BBl 2006 2829, abruf-

bar unter https://www.fedlex.admin.ch/eli/fga/2006/303/de, besucht am 23.8.2024.

Eidgenössische Finanzmarktaufsicht (FINMA), Rundschreiben 2008/17 Informationsaustausch zwischen den SRO und der FINMA betreffend Anschlüsse, Ausschlüsse und Austritte von Finanzintermediären vom 20.11.2008, abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2008-17.pdf?sc_lang=de&hash=71FFD4758724C36DBC692710A9C8477B, besucht am 23.8.2024.

Eidgenössische Finanzverwaltung (EFV), Kontrollstelle GwG, Rundschreiben 2006/1 Informationsaustausch zwischen den SRO und der Kontrollstelle betreffend Anschlüsse, Ausschlüsse und Austritte von Finanzintermediären vom 10.4.2006, abrufbar unter https://www.finma.ch/finmaarchiv/gwg/d/dokumentationen/gesetze_und_regulierung/rundschreiben/index.php, besucht am 23.8.2024.

Forum Schweizer Selbstregulierungsorganisationen (Forum-SRO), Statuten vom 30.9.2009, abrufbar unter https://www.forum-sro.ch/_files/ugd/f269ef_75384def8a2144b9814c2d42076907d9.pdf, besucht am 23.8.2024.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 28 AMLA

A commentary by Caroline Kindler

SUGGESTED CITATION

Caroline Kindler, Commentary of art. 28 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Kindler, art. 28 AMLA N. XXX

Art. 28 Withdrawal of recognition

[1] FINMA shall not withdraw recognition from a self-regulatory organisation under Article 37 of the FINMASA without prior warning.

[2] If a self-regulatory organisation has its recognition withdrawn, its affiliated financial intermediaries must submit a request for affiliation with another self-regulatory organisation within two months.

[3] and [4] ...

CONTENT

I. Withdrawal of recognition (Para. 1) 503
A. Legal basis 503
B. Requirements under Art. 37 FINMASA: grounds for withdrawal 503
1. Failure to meet the operating conditions 503
2. Serious violation of supervisory provisions 504
C. Subsidiarity 505
D. Legal consequences of the withdrawal for the SRO 506
II. Consequences for affiliated financial intermediaries (para. 2) 507
Bibliography 507
Materialis 508

I. WITHDRAWAL OF RECOGNITION (PARA. 1)

A. Legal basis

Until the entry into force of the FINMASA on January 1, 2009, the conditions for withdrawing the recognition of a self-regulatory organization (SRO) were governed exclusively by Article 28 paragraph 1 AMLA. With the introduction of the FINMASA as an umbrella law for the various areas supervised by FINMA, the supervisory instruments that had previously been regulated by special laws, in particular the withdrawal of licenses, recognitions or admissions, were standardized and harmonized in Art. 37 FINMASA. Since then, Art. 28 AMLA no longer contains the requirements for the withdrawal of an SRO's recognition, but instead refers to Art. 37 FINMASA in para. 1, while para. 2 exclusively regulates the consequences of a withdrawal of recognition for the supervised financial intermediary. The only requirement from the original version of Art. 28 para. 1 AMLA that was retained is the requirement to issue a prior warning of withdrawal. 1

B. Requirements under Art. 37 FINMASA: grounds for withdrawal

FINMA orders the withdrawal of recognition in accordance with Art. 37 para. 1 FINMASA if the SRO either (1) "no longer fulfills the requirements for the activity" or (2) "seriously violates supervisory provisions". The reasons for the withdrawal of recognition are **alternatively**, i.e. it is sufficient if the SRO either no longer fulfills the recognition requirements or has seriously violated supervisory provisions. 2

1. Failure to meet the operating conditions

The operating conditions are the **recognition conditions** for an SRO in accordance with Art. 24 AMLA: (1) The SRO must have regulations in accordance with Art. 25 AMLA; (2) it must prove that it is able to monitor whether the affiliated financial intermediaries are complying with their obligations under Art. 3–11a AMLA; (3) the SRO itself and the persons and audit firms entrusted with the control must guarantee irreproachable business and auditing 3

activities; and (4) the audit firms and lead auditors entrusted by the SRO with the control must meet the requirements of Article 24a AMLA.

4 These requirements for recognition must not only be met at the time of recognition, but must be **permanently complied with**. If, for example, an SRO refuses to adapt its regulations, which were originally approved as part of the recognition process, to the amended requirements of FINMA (AMLO-FINMA), the conditions for recognition are no longer met. If certain conditions were not met at the time of granting the recognition and the administrative act of recognition was thus flawed from the outset, this defect is not remedied retrospectively by the granting of recognition. In such a case, the original recognition can be withdrawn at any time.

5 Furthermore, the recognition requirements must be met **cumulatively**, so that the elimination of even one requirement would generally be sufficient to call the recognition into question. According to the doctrine, however, it must be an essential requirement; the elimination of a subordinate requirement can be corrected in another way under supervisory law.

2. Serious violation of supervisory provisions

6 As an alternative to the loss of the license conditions, a serious violation of supervisory provisions can also justify the withdrawal of the license. In this context, a **broad definition** of the supervisory provisions is to be assumed, which, in addition to the FINMASA and the associated ordinances, also includes the AMLA and the ordinances and circulars issued by FINMA.

7 The "**seriousness of**" a violation of supervisory provisions is an indeterminate legal concept, and FINMA has a certain technical leeway in its interpretation. The principle of proportionality requires that the more serious the measure ordered, the higher the requirements for classifying a violation as "serious". Since the withdrawal of recognition under Article 37 FINMASA is the *ultima ratio* under supervisory law, the decision depends to a large extent on the severity of the violation and the significance of the violated provision: a minor violation of an essential provision justifies the withdrawal no more than a serious violation of a subordinate duty does. The severity of the violation must always be assessed on a case-by-case basis, taking into account the specific circumstances.

C. Subsidiarity

Art. 28 para. 1 AMLA stipulates that the withdrawal of recognition under Art. 37 FINMASA "shall not be made without prior warning". This mandatory prior warning of the withdrawal of recognition goes beyond the wording of Art. 37 FINMASA. It remains questionable whether this additional requirement and thus Art. 28 para. 1 AMLA as a whole has any independent significance, since, as explained below, the **subsidiarity of the withdrawal of recognition** already follows from Art. 31 FINMASA and from the basic principles of administrative law, which must be observed when withdrawing recognition. These basic principles include, in particular, the principle of proportionality enshrined in constitutional law (Art. 5 para. 2 FC), which ensures that state intervention is only permissible if it is appropriate, necessary and proportionate in the strict sense. 8

The legislator regards the withdrawal of recognition under Art. 37 FINMASA as the *ultima ratio* of the supervisory system. According to the **principle of proportionality**, this may only be ordered if no suitable, milder measure is available. The proportionality test therefore requires that the withdrawal of recognition is only justified if it appears to be suitable, necessary and proportionate in view of the objective pursued. This means that a less severe measure that is equally suitable for safeguarding the public interest must be given priority. Since the withdrawal of recognition is the most serious measure in the supervisory system, FINMA must first take the necessary supervisory measures in accordance with Article 31 FINMASA to restore compliance and rectify the irregularities. The prior threat of withdrawal should be combined with a demand to rectify the unlawful situation, whereby the threat also implies a reasonable period of time to restore compliance with the law in accordance with Art. 31 FINMASA. One possible measure, for example, could be to demand the removal of the responsible bodies of a legal entity whose organs have violated legal requirements or supervisory provisions. 9

The withdrawal of recognition is to be understood under administrative law as the **revocation of** an originally granted (police) license in the sense of **a ruling under Art. 5 APA**. This revocation in turn constitutes a new ruling that is subject to the requirements of a proper administrative procedure. The procedure for the withdrawal of recognition is based on the provisions of the APA. In addition to the formal procedural principles, as regulated in Art. 7 ff. APA, the fundamental principles of administrative law must be observed, including 10

the principle of proportionality, the prohibition of arbitrariness and the right to be heard.

11 When a ruling is revoked, a **weighing of interests** must be carried out if there is no clear legal regulation or if there is room for interpretation. In this context, the interest in the correct application of objective law must be weighed against the interest in legal certainty and the protection of legitimate expectations. In cases such as the withdrawal of an SRO's recognition, the public interest in the protection of the financial market, for example ensuring market integrity, is on the one hand. On the other hand, there are the private interests of the SRO, whose activities would be completely terminated without recognition. While the proportionality test examines the suitability and necessity of the measure, the weighing of interests ensures that the public interest outweighs the private interest and that less severe measures would be insufficient. Each decision must therefore be based on a careful consideration of the specific circumstances.

D. Legal consequences of the withdrawal for the SRO

12 With the withdrawal of recognition, the SRO loses the right to continue its activity under Article 24 AMLA in accordance with Article 37 para. 2 FINMASA For the other consequences of the withdrawal, Article 37 para. 2 FINMASA refers to the corresponding financial market laws that apply in the specific case. It should be noted that Art. 28 AMLA does not provide for any additional legal consequences in the event of withdrawal of recognition, unlike other financial market laws, which generally require the authorized company to be dissolved. Even if the purpose of the association is exclusively to act as an SRO, the impossibility of fulfilling this purpose does not constitute a compelling reason for dissolution. The members of the SRO therefore remain bound by their membership for as long as the association continues to exist. However, they are free to leave the association or to decide to dissolve the association at an extraordinary general meeting, if one is convened. The situation is different for SROs that are not a separate legal entity but are part of an industry association. In such cases, the industry association continues to exist but no longer operates any SROs.

II. CONSEQUENCES FOR AFFILIATED FINANCIAL INTERMEDIARIES (PARA. 2)

Art. 28 para. 2 AMLA requires that all financial intermediaries must submit an application **for admission to another SRO** within two months if their previous SRO has had its recognition withdrawn. 13

With the entry into force of the FinIA on January 1, 2020, the option to choose between FINMA direct supervision and affiliation to an SRO was eliminated. In this context, the legislator has merely provided that financial intermediaries whose SRO has had its recognition withdrawn must join another SRO. However, practical issues arising from the termination of an SRO's activities – in particular, how to deal with the supervisory gap between the date of the withdrawal of recognition and the date of the financial intermediaries' affiliation to a new SRO – remain unregulated by law. 14

BIBLIOGRAPHY

Arpagaus Reto, Kommentierung zu Art. 23^{quinquies} BankG, in: Zobl Dieter/Schwob Renate/Winzeler Christoph/Kaufmann Christine/Weber Rolf H./Kramer Stefan (Hrsg.), Bodmer Daniel/Kleiner Beat/Lutz Benno, Kommentar zum Bundesgesetz über die Banken und Sparkassen, Zürich 2015 (zit.: B/K/L-Arpagaus)

de Capitani Werner, in: Schmid Niklaus (Hrsg.), Kommentar Einziehung, Organisiertes Verbrechen, Geldwäscherei, Band II, Zürich 2002.

Häfelin Ulrich/Müller Georg/Uhlmann Felix, Allgemeines Verwaltungsrecht, 8. Aufl., Zürich/St. Gallen 2020.

Neese Martin, Kommentierung zu Art. 28 GwG, in: Peter Ch. Hsu/Daniel Flühmann (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Poledna Tomas, Staatliche Bewilligungen und Konzessionen, Bern 1994.

Poledna Tomas/Jermini Davide, in: Watter Rolf/Vogt Nedim Peter/Bauer Thomas/Winzeler Christoph (Hrsg.), Basler Kommentar, Bankengesetz, 2. Aufl., Basel 2013.

Ramelet Nicolas, Kommentierung zu Art. 28 GwG, in: Peter V. Kunz/Thomas Jutzi/Simon Schären (Hrsg.), Stämpflis Handkommentar (SHK) zum Geldwäschereigesetz (GwG), Bern/Zürich 2017.

Roth Pellanda Katja/Kopp Lara, Kommentierung zu Art. 37 FINMAG, in: Watter Rolf/Bahar Rashid (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

Thelesklaf Daniel, Kommentierung zu Art. 25 GwG, in: Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell Füssli Kommentar, Geldwäschereigesetz, 3. Aufl., Zürich 2019.

Zulauf Urs/Wyss David/Tanner Kathrin/Kähr Michel/Fritsche Claudia M./Eymann Patric/Ammann Fritz, Finanzmarktenforcement, 3. Aufl., Bern 2022 (zit.: Zulauf et al.).

MATERIALIS

Botschaft des Bundesrates an die Bundesversammlung über die Revision des Bankengesetzes vom 13.5.1970, BBl 1970 1144, abrufbar unter https://www.fedlex.admin.ch/eli/fga/1970/1_1144__/de, besucht am 23.8.2024.

Botschaft zum Bundesgesetz über die Eidgenössische Finanzmarktaufsicht (Finanzmarktaufsichtsgesetz; FINMAG) vom 1.2.2006, BBl 2006 2829, abrufbar unter https://www.fedlex.admin.ch/eli/fga/2006/303/de, besucht am 23.8.2024.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 29 AMLA

A commentary by Tina Triller

SUGGESTED CITATION

Tina Triller, Commentary of art. 29 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Triller, art. 29 AMLA N. XXX

Chapter 4 Administrative Assistance

Section 1 Cooperation among Domestic Authorities

Art. 29 Exchange of information among authorities

[1] FINMA, the FGB, the intercantonal authority, the Central Office and the Reporting Office may provide each other with any information they require for the application of this Act.

[2] The federal, cantonal and communal authorities shall if requested by the Reporting Office or the central offices of the Federal Criminal Police pass on to the Reporting Office or the said central offices all the data required for the analyses in relation to combating money laundering, its predicate offences, organised crime or the financing of terrorism. The data include in particular financial information and other

sensitive personal data obtained in criminal, administrative criminal and administrative proceedings, including those from pending proceedings.

[2bis] The Reporting Office may provide, on a case-by-case basis, the authorities referred to in paragraph 2 with information in individual cases provided the authorities use the information exclusively for combating money laundering, its predicate offences, organised crime or the financing of terrorism. Article 30 paragraphs 2–5 applies by analogy.

[2ter] The Reporting Office may only pass on information from foreign reporting offices with their express consent to the authorities referred to in paragraphs 1 and 2 for the purposes specified in paragraph 2[bis].

[3] The Reporting Office shall inform FINMA, the FGB, the intercantonal authority and the Central Office of the decisions of the cantonal prosecution authorities.

CONTENT

I. Introduction 512
II. Requirements for national administrative assistance pursuant to Art. 29 para. 1 AMLA 513
A. Definition of authorities according to Art. 29 para. 1 AMLA 513
B. Optional provision 513
C. The purpose limitation as a barrier to the exchange of information 514
D. Content of the information exchange 514
E. Form and nature of the information 515
III. Requirements for national administrative assistance under Art. 29 para. 2 AMLA 515
A. Covered authorities 516
B. Obligation to surrender upon request 516
C. Content of the information exchange 516
IV. Requirements for national administrative assistance in accordance with Art. 29 para. 2bis AMLA 516
A. Definition of authority in accordance with Art. 29 para. 2 AMLA 516
B. Optional provision 518
C. Purpose limitation as a barrier to information exchange 518
D. Restrictions under Article 30, paras. 2–5 AMLA 519
1. Content of the exchange of information under Art. 30 para. 2 AMLA 519
2. Form in accordance with Art. 30 para. 3 AMLA 521
3. Requirements for the disclosure of information to third-party authorities in accordance with Art. 30 paras. 4 and 5 AMLA 521
V. Information from foreign reporting offices in accordance with Art. 29 para. 2ter AMLA 522
VI. Information for the supervisory authorities under Art. 29 para. 3 AMLA 523
Bibliography 524
Materials 524

I. INTRODUCTION

1 The exchange of information between national authorities and the Money Laundering Reporting Office Switzerland MROS is regulated in the first section of the fourth chapter of the Anti-Money Laundering Act. MROS is at the center of these administrative assistance regulations.

2 The legal mandate of MROS can be divided into three main areas of responsibility: Intelligence (analysis of reports of suspicions and forwarding to law enforcement authorities), prevention (strategic analysis, risk detection, methods and trends, awareness-raising) and cooperation (administrative assistance).

3 Cooperation, i.e. the exchange of financial information, is of the utmost importance and a cornerstone of international efforts to combat money laundering, terrorist financing and the associated predicate offences. MROS acts as the **linchpin of this system**. In cases where only fragmented information is available, MROS can play a substantial role in piecing together the full picture and forward the (consolidated) information to the authorities.

4 The aim of national administrative assistance must be to ensure an **efficient flow of information**, to coordinate investigations, to increase transparency and to support criminal prosecution. It is a central element in protecting the integrity of the financial center and the financial system and effectively combating illegal activities. Money laundering and terrorist financing can only be counteracted if information can be transmitted quickly and completely. To carry out this task efficiently, MROS requires appropriate administrative assistance provisions that keep the hurdles for exchanging information as low as possible. The administrative burden of transmitting information, which ultimately has a significant impact on human resources, must also be kept to a minimum, as far as national and international requirements allow.

5 The exchange of information between the prosecution authorities and MROS under the administrative assistance provisions (Art. 29 para. 2bis AMLA) must be **distinguished from** the reporting to the prosecution authorities under Art. 23 para. 4 AMLA. If MROS concludes on the basis of its analysis that there is a suspicion of money laundering, its predicate offenses, organized crime, terrorist financing or a lack of due diligence in financial transactions, it is obliged under Article 23 para. 4 AMLA to report the matter to the competent law enforcement authority. Unlike a report, however, the exchange of in-

formation under Art. 29 para. 2bis AMLA is subject to the restrictions on use under Art. 29 para. 2bis AMLA in conjunction with Art. 30 paras. 2–5 AMLA, which define the content and form of the information transmitted, but also provide for restrictions on the use and disclosure of this information (see OK-Triller, Art. 29 AMLA, N. 34 below). The distinction between a report pursuant to Art. 23 para. 4 AMLA and an exchange of information through administrative assistance is therefore of central importance when it comes to the question of the usability of the information received by the prosecuting authorities.

II. REQUIREMENTS FOR NATIONAL ADMINISTRATIVE ASSISTANCE PURSUANT TO ART. 29 PARA. 1 AMLA

Art. 29 para. 1 AMLA governs national administrative assistance between MROS and **supervisory authorities**. The authorities mentioned in the law may provide each other with any information they require for the application of the AMLA. 6

A. Definition of authorities according to Art. 29 para. 1 AMLA

The following are covered by the wording of the law according to Art. 29 para. 1 AMLA: the Swiss Financial Market Supervisory Authority FINMA, the Federal Gaming Board FGB, the intercantonal authority (Intercantonal Supervisory and Enforcement Authority according to Art. 105 of the Gambling Act), the Central Office (for Precious Metals Control) and MROS, whereby this list is **exhaustive**. 7

Art. 29b AMLA provides a separate legal basis for the exchange of information with self-regulatory and supervisory organizations. The content of the regulation is practically identical to that of Art. 29, para. 1 AMLA. 8

B. Optional provision

Article 29, para. 1 AMLA is an "optional provision" (**Kann-Bestimmung**). The decision to provide administrative assistance is therefore at the discretion of the supervisory authorities and MROS. 9

10 In MROS practice, administrative assistance is the **general rule**. MROS only refuses administrative assistance in exceptional cases, when justified, or when the conditions of Article 29, para. 1 AMLA are not met.

C. The purpose limitation as a barrier to the exchange of information

11 The exchange of information between MROS and the supervisory authorities is limited to the "**application of the Anti-Money Laundering Act**". This purpose limitation stipulates which information the authorities can exchange with each other.

12 The article of purpose of the AMLA states that the law regulates the fight against money laundering, the fight against terrorist financing and the ensuring of due diligence in financial transactions. The latter also includes the due diligence obligations of financial intermediaries, the obligations in the event of suspected money laundering and the obligation to disclose information. Thus, information that may indicate a violation of money laundering provisions **under supervisory law** (violation of due diligence obligations, violation of the reporting requirement, etc.) may be exchanged with the authorities in accordance with Art. 29 para. 1 AMLA. On the other hand, Art. 29 para. 1 AMLA does not provide a legal basis for the transmission of information that, for example, relates exclusively to another special or (financial market) law and thus has no connection with the application of the Anti-Money Laundering Act.

D. Content of the information exchange

13 The supervisory authorities and MROS may provide each other with "**all information**" for the purpose of applying the AMLA. This includes all information in the internal goAML information system and any other information held by MROS. This information may include personal data, sensitive personal data and financial information. For example, this includes information on: date of receipt of the report, content of the suspicious activity report (transactions), contracting partner, beneficial owner, date of transmission to the law enforcement agency.

14 In the case of a request for administrative assistance, the information must be limited to the **subject of the request** (need-to-know principle / proportionality). No further information may be provided. However, MROS may provide

additional information on its own initiative in response to a request if the conditions are met.

E. Form and nature of the information

The authorities mentioned in Art. 29, para. 1 AMLA may provide each other with any "information" they need to apply the law. However, it is not clear from the wording of the law whether the information includes the exchange of documents or only summary compilations. 15

The transmission of "documents" was deleted from the legal text of Art. 29 para. 1 AMLA with the revision of the Anti-Money Laundering Act as of January 1, 2023. This means that no (original) documents may be exchanged. The reason given for this was that MROS, as an administrative authority, produces "financial intelligence" and is therefore not allowed to exchange any documents that could be used in administrative or criminal proceedings. 16

This argument is open to criticism from today's perspective. The fact that the authorities mentioned in Article 29, para. 1 AMLA can provide each other with any information they need to apply the AMLA is undisputed. Similarly, there is no restriction on national information not being included in procedural files. The fact that no (original) documents are exchanged means that the information must be transmitted in a **report form**. This causes a considerable administrative and time overhead for all authorities involved. 17

The exchange of information can be done orally, electronically or on paper. Consequently, the decision on the **method of** providing information is left to MROS and the individual supervisory authorities, although a written exchange is preferred (for reasons of traceability and with a view to maintaining official secrecy). 18

III. REQUIREMENTS FOR NATIONAL ADMINISTRATIVE ASSISTANCE UNDER ART. 29 PARA. 2 AMLA

Art. 29 para. 2 AMLA governs the transmission of information from third-party authorities to the reporting office. The reporting office may, upon request, obtain from federal, cantonal and municipal authorities all the data it requires for the analysis to combat money laundering, its predicate offenses, organized crime or terrorist financing. 19

A. Covered authorities

20 Art. 29 para. 2 AMLA applies to all federal, cantonal and municipal authorities that hold relevant information that may be relevant for the analysis of the reporting office or the federal criminal police headquarters. According to the message, this also includes the tax authorities, customs authorities, land registry offices and residents' registration offices.

B. Obligation to surrender upon request

21 If the conditions of Article 29, para. 2 AMLA are met, the authorities shall transmit the information to MROS and the Federal Criminal Police at their request, provided that the special laws applicable to the authorities in question do not provide for other restrictions that prevent disclosure.

C. Content of the information exchange

22 MROS may request from the authorities basically **all information** required for its operational analysis activities (combating money laundering, its predicate offences, organized crime and terrorist financing). This includes in particular financial information as well as other personal data worthy of protection that is gathered in criminal, administrative penal and administrative proceedings, including such data from pending proceedings. Art. 7 MLO further specifies the information content.

IV. REQUIREMENTS FOR NATIONAL ADMINISTRATIVE ASSISTANCE IN ACCORDANCE WITH ART. 29 PARA. 2BIS AMLA

23 Art. 29 para. 2bis AMLA regulates the transmission of information from MROS to third-party authorities in return for para. 2. The legal norm is difficult to apply, in particular due to its **norm complexity**.

A. Definition of authority in accordance with Art. 29 para. 2 AMLA

24 Art. 29 para. 2bis AMLA refers to the definition of "**authorities**" to which MROS can provide administrative assistance in para. 2 of the aforementioned provision. This includes federal, cantonal and municipal authorities. However,

the scope of application is limited to the use of information in accordance with Art. 29 para. 2bis AMLA for those authorities that are active in the fight against money laundering, its predicate offences, organized crime or terrorist financing.

In principle, the **law enforcement authorities** are also covered by the scope of application. This applies in particular to spontaneous information or requests for administrative assistance without a prior formal report under Article 23, para. 4 AMLA by the MROS. If a report has been filed, it must be determined whether new findings can be transmitted in the sense of supplementing the report. If this is not the case, then only the mutual assistance route is possible. The same conditions apply to the exchange of information as with the other authorities. This means that the prosecuting authorities only receive the information in report form and this is subject to the restrictions on use (Art. 29 para. 2bis AMLA in conjunction with Art. 30 para. 2– 5 AMLA). 25

To determine which authorities are active in combating money laundering, it is first necessary to define what is covered by the term money laundering. The AMLA does not provide a definition in this regard. 26

Art. 305bis no. 1 SCC describes an act that typically makes it more difficult to determine the origin, locate or confiscate assets. This covers a wide range of actions, from mere concealment to failure to report to MROS. This makes it possible to exchange information with the authorities that combat such behavior and thus help to prevent the assets obtained by criminal means from remaining unseized. Money laundering is a secondary offense and requires a **predicate offense**, i.e. an upstream offense. The predicate offences are crimes under Art. 10 para. 2 SCC or a qualified tax offence. As such, those criminal offences under the Special Part of the SCC and the ancillary penal legislation for which the abstract penalty range is more than three years' imprisonment are considered. If an authority is responsible for prosecuting crimes, MROS can in principle provide administrative assistance. 27

Furthermore, the AMLA does not define the terms “organized crime” and “terrorism financing”. **Organized crime** is not explicitly included in the scope of the AMLA. However, Art. 29, para. 2 AMLA expressly states that information may also be exchanged with authorities that use the information to combat organized crime. By analogy, reference can be made to the corresponding criminal offence of criminal and terrorist organization under Art. 260ter SCC. 28

29 Anyone who finances a violent crime intended to intimidate the population or to coerce a state or an international organization to perform or refrain from performing an act, or who collects or provides assets to that end, is liable to prosecution for **financing terrorism** (Art. 260^{quinquies} para. 1 SCC). However, terrorist financing does not require a predicate offense. Furthermore, there is no uniform definition of "terrorism".

B. Optional provision

30 As with Art. 29 para. 1 AMLA, Art. 29 para. 2bis AMLA is an "optional provision", which is supplemented by the expression "in individual cases". This stipulates that **no automatic data exchange** may take place between MROS and the other public authorities. MROS must always weigh the circumstances and decide in the light of the specific situation whether it is legally permissible, appropriate and proportionate to share information with other authorities. In particular, MROS may decide at the analysis stage not to provide information until it is clear whether or not it will be forwarded to the law enforcement agency. This avoids any **anticipation of** and, in particular, any circumvention of Art. 30, para. 5 AMLA.

C. Purpose limitation as a barrier to information exchange

31 MROS may provide information to the aforementioned authorities provided that they use the information exclusively to combat money laundering, its predicate offences, organized crime and terrorist financing. Consequently, MROS may only provide administrative assistance if the requesting authority states, or if it is clear from the authority's legally defined area of responsibility, that it will use the information for the aforementioned purposes. MROS provides the authorities with information in accordance with Article 29, para. 2 AMLA only on condition that the information is "used" in the aforementioned area of application. This restriction reflects the **principle of purpose limitation or specialty**.

32 Based on this, the intended use must be checked for each request for administrative assistance or for each spontaneous information. When exchanging information upon request, the **reasoning** of the requesting authority is particularly crucial. It is the responsibility of the requesting authority to explain the intended use of the information. Usually, it is necessary to assess whether the authority in question is active in AMLA-specific areas in the first step of the

admissibility of the information exchange. In particular, the descriptions of the responsibilities in the legal bases of the respective authority or the penal provisions of the relevant norms can be used for the assessment. In accordance with the purpose of the exchange of information, namely to promote downstream proceedings, the principle of purpose limitation and the principle of speciality must be interpreted broadly within the given framework.

In summary, MROS must adhere to the principle of purpose limitation and the principle of speciality when exchanging information, but **no absolute identity of purpose** can be demanded within the framework of administrative assistance. This allows MROS a certain amount of discretion, which it should make use of. Administrative assistance is to be provided to those authorities that are active in the fight against money laundering, its predicate offenses, organized crime and terrorist financing and that also use the information for these purposes. 33

D. Restrictions under Article 30, paras. 2–5 AMLA

National administrative assistance can only take place in accordance with the reference in Art. 29 para. 2bis AMLA if Art. 30, paras. 2–5 AMLA is complied with mutatis mutandis. This ensures that domestic authorities are **treated equally** with foreign authorities in terms of information exchange with MROS when compared to the information received by foreign authorities via the FIU channel. 34

Art. 30 para. 2 AMLA defines the information content and para. 3 the form of the information exchange. Art. 30 paras. 4 and 5 AMLA govern the conditions under which foreign FIUs may forward information received from MROS to third-party authorities. In the analogous application of this provision to national administrative assistance, this means that the restrictions that MROS must observe and ensure are those that apply both to the disclosure of information from foreign FIUs to national authorities (counterpart to Art. 29 para. 2ter AMLA) and to the intended disclosure of information by the recipient to a national third-party authority (tripartite relationship). 35

1. Content of the exchange of information under Art. 30 para. 2 AMLA

In addition to financial information, the exchange of information may also include other personal data that is particularly worthy of protection. According- 36

ly, the Reporting Office may in particular receive information concerning the name of the financial intermediary or dealer (provided that the anonymity of the [natural] person involved is thereby preserved) who has filed a report or fulfilled a duty to provide information under the AMLA (lit. a); on the account holder, account numbers and account balances (lit. b); on the beneficial owner (lit. c); and on transactions (lit. d).

37 The wording of Art. 29, para. 2, subpara· AMLA does not contain a reference to Art. 30, para. 1 AMLA, which establishes the **availability principle**. This means that data available directly or indirectly to MROS may be exchanged with foreign FIUs. In this case, the exchange of information also extends to data that MROS can obtain from public or private data controllers based on the legal provisions. Based on a request for administrative assistance from a foreign FIU, an in-depth analysis is carried out, which also includes, among other things, database queries in the police system.

38 In the absence of a corresponding reference, only the information that is **immediately** available at MROS is to be provided in the case of national administrative assistance. The information contained in the "goAML" information system is considered to be immediately available. Therefore, if an authority requests administrative assistance, only "goAML" is consulted. The information contained in this system comes in particular from suspicious activity reports, requests for administrative and mutual assistance (including international administrative assistance) or from communications from criminal authorities under Art. 29a AMLA. If the search does not produce any relevant hits in response to the specifically justified request for administrative assistance, a negative response is sent. However, no actual analysis, as in the case of cooperation with foreign reporting offices, is carried out.

39 Furthermore, a request for information under Article 11a AMLA based on information from a national request for administrative assistance is not permitted. Such a request is only possible if a SAR has already been received and the request is based on this report or if it is clear from the analysis of information from a foreign FIU that a financial intermediary under the Act is or has been involved in a transaction or business relationship related to this information.

2. Form in accordance with Art. 30 para. 3 AMLA

The analogous application of Art. 30 para. 3 AMLA to domestic administrative assistance determines the form of the information exchange. MROS provides information to the national authorities in accordance with Art. 29 para. 2bis AMLA in "**report form**", as is already the case with foreign reporting offices. This applies to both administrative assistance upon request and spontaneous information. The transmission of documents to the requesting authority is not permitted. 40

3. Requirements for the disclosure of information to third-party authorities in accordance with Art. 30 paras. 4 and 5 AMLA

The reference in Article 29 paragraph 2bis AMLA to the application of Article 30 paragraphs 4 and 5 AMLA implies that the forwarding of information by domestic authorities to other administrative units (third-party authority) requires the prior express consent of MROS (para. 4). If criminal proceedings are already pending in the matter, MROS must also obtain the approval of the competent prosecuting authority before it can consent to the forwarding of the information (para. 5). It should be noted that the analogous application of Art. 30 para. 4 and para. 5 AMLA with regard to national administrative assistance primarily concerns those constellations in which the recipient of information from MROS intends to make this **information available to a third-party authority**. The main purpose of this consent to dissemination to a third-party authority is to ensure control over the forwarding (including compliance with the purpose limitation) (see Art. 30 para. 4 AMLA) and not to jeopardize any criminal investigations (see Art. 30 para. 5 AMLA). 41

If, on the other hand, MROS passes on information that is available to it and does not come from a foreign FIU, it **does not** have to obtain **the prior consent** of the domestic authority to disseminate the information. An exception to this is when the authority from which the information originates also imposes restrictions on use. 42

The application of Art. 30, para. 4 AMLA by analogy stipulates that MROS may only consent to the forwarding of information to a third authority if the latter uses the information exclusively (1.) for analysis purposes in the context of combating money laundering and its predicate offences, organized crime or terrorist financing, or (2.) for the initiation of criminal proceedings for money 43

laundering and its predicate offenses, organized crime or terrorist financing, or to substantiate a request for mutual legal assistance in the context of such criminal proceedings (lit. a); it does not use the information as evidence (lit. c) and maintains official or professional secrecy (lit. d). Verification of dual criminality as defined in b) is not required for national administrative assistance, since the application of the law is limited to the same jurisdiction.

44 It should be noted that the transmission of information from a national authority to a third-party authority is subject to **more restrictive conditions** than the direct administrative assistance provided by MROS to an authority in accordance with Art. 29 para. 2bis AMLA. This applies in particular to the use of information as evidence.

45 A further requirement of Art. 29 para. 2bis in conjunction with Art. 30 para. 5 AMLA is the prior approval of the competent public prosecutor if the request for forwarding to a third-party authority concerns a matter that is the subject of criminal proceedings. If the database search shows that proceedings are pending, the competent public prosecutor must be contacted. If the public prosecutor in charge of the proceedings refuses to authorize the forwarding of information, the requirement for dissemination is not met, and the information must not be forwarded to the (third-party) authority. This procedure prevents any possible interference with the investigation.

46 In summary, MROS is authorized to provide administrative assistance to national authorities in accordance with Article 29, paragraph 2 AMLA, provided that the information is sent to an authority that is active in combating money laundering, its predicate offences, terrorist financing or organized crime and that the authority uses the information for these purposes (Article 29, paragraph 2bis AMLA). If the recipient of the information intends to forward it to a third-party authority, MROS must give its consent to the dissemination in compliance with the relevant requirements (Art. 29 para. 2bis AMLA in conjunction with Art. 30 para. 4 and 5 AMLA and Art. 29 para. 2ter AMLA).

V. INFORMATION FROM FOREIGN REPORTING OFFICES IN ACCORDANCE WITH ART. 29 PARA. 2TER AMLA

47 While MROS can forward information from national sources (e.g. information from suspicious activity reports) without the consent of the respective sources, information from foreign reporting offices is subject to more restric-

tive provisions. Art. 29 para. 2ter AMLA stipulates that MROS may only forward information from foreign reporting offices to the supervisory authorities pursuant to Art. 29 para. 1 AMLA and to the authorities pursuant to Art. 29 para. 2 AMLA with the **explicit consent of** the reporting office.

Furthermore, the disclosure of information from foreign reporting offices is only permitted for the purposes stated in Art. 29 para. 2bis AMLA. This addition is to be extended in line with international obligations, so that the entire **restrictions** of Art. 29 para. 2bis AMLA are to be observed. This in turn refers to the application of Art. 30 para. 2–5 AMLA. Unlike national information that MROS obtains domestically, Art. 29 para. 2ter AMLA is subject to the same restrictions as those applying to administrative assistance to other authorities under Art. 29 para. 2bis AMLA. In the case of foreign information, it does not matter to which type of authority it is forwarded. 48

In addition, the foreign FIU's **usage restrictions** (disclaimer) must always be observed in these cases. The corresponding restrictions regarding the use of the information must also be passed on in national administrative assistance under Art. 29 AMLA. 49

VI. INFORMATION FOR THE SUPERVISORY AUTHORITIES UNDER ART. 29 PARA. 3 AMLA

The basic idea of Art. 29, para. 3 AMLA is that the findings of MROS's analysis of judgments are fed back to the financial intermediaries via the supervisory authorities. This is to ensure that the financial intermediaries are made aware of the requirements of the prosecuting authorities. In this way, Art. 29 para. 3 AMLA serves as a link to Art. 29a paras. 1 and 2 AMLA, which ensure the **feedback mechanism** of the cantonal prosecuting authorities. 50

This legal construct of information transfer from the reporting office via the supervisory authorities to the financial sector proved to be inefficient; rather, in everyday practice, **direct** communication between the reporting office and the financial intermediaries regarding findings on combating money laundering, their predicate offences, organized crime and terrorist financing has become established. MROS regularly exchanges information with the financial sector and financial intermediaries, thereby also fulfilling its awareness-raising mandate (Art. 1 para. 1 let. c AMLA). 51

BIBLIOGRAPHY

Ackermann Jürg-Beat (ed.), Wirtschaftsstrafrecht der Schweiz, 2nd ed., Bern 2021.

Beuret Arnaud, commentary on Art. 29 AMLA, in: Kunz Peter V./Jutzi Thomas/Schären Simon (eds.), SHK – Stämpflis Handkommentar, Anti-Money Laundering Act (AMLA), Bern et al. 2017.

Derungs Corsin/Dobrauz Günther (eds.), Financial Market Law Tables – Anti-Money Laundering Act (AMLA), Zurich 2020.

Fiolka Gerhard, Commentary on Art. 260^{quinquies} SCC, in Niggli Marcel Alexander/Wiprächtiger Hans, Criminal Law, Basler Kommentar, 4th ed., Basel 2019.

Isenring Bernhard, Commentary on Art. 305bis SCC, in: Andreas Donatsch (ed.), OFK - Orell Füssli Commentary, SCC/JStG, 21st ed., Zurich 2022.

Kilgus Sabine/Losinger Paolo, Commentary on the preamble to Art. 1 AMLA, in: Hsu Peter Ch./Flühmann Daniel, Basler Kommentar, Anti-Money Laundering Act, Zurich 2021.

Kiener Regina/Rütsche Bernhard/Kuhn Mathias, Public Procedural Law, 3rd ed., Zurich 2021.

Nägeli Vera, Commentary on Art. 29 AMLA, in: Hsu Peter Ch./Flühmann Daniel, Basler Kommentar, Anti-Money Laundering Act, Zurich 2021.

Nägeli Vera, Commentary on Art. 29a AMLA, in: Hsu Peter Ch./Flühmann Daniel, Basler Kommentar, Geldwäschereigesetz, Zurich 2021.

MATERIALS

Message on the Amendment of the Anti-Money Laundering Act of June 27, 2012, BBl 2012, available at https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2012/1031/de/pdf-a/fedlex-data-admin-ch-eli-fga-2012-1031-de-pdf-a.pdf, visited on July 1, 2024 (cited. Message AMLA 2013).

Message zur Änderung des Geldwäschereigesetzes vom 26.6.2019, BBl 2019, available at https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/

fga/2019/1932/de/pdf-a/fedlex-data-admin-ch-eli-fga-2019-1932-de-pdf-a.pdf, visited on July 1, 2024 (cited as AMLA 2019 message).

Message zur Umsetzung der 2012 revidierten Empfehlungen der Groupe d'action financière (GAFI) of December 13, 2013, BBl 2013, available at https://www.fedlex.admin.ch/filestore/fedlex.data.admin. ch/eli/fga/2014/100/de/pdf-a/fedlex-data-admin-ch-eli-fga-2014-100-de-pdf-a.pdf, accessed on July 1, 2024 (cited as Message AMLA 2012).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 29a AMLA

A commentary by Marcel Scholl / Marion Wyss

SUGGESTED CITATION

Marcel Scholl/Marion Wyss, Commentary of art. 29a AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Scholl/Wyss, art. 29a AMLA N. XXX.

Art. 29*a* Prosecution authorities

[1] The prosecution authorities shall notify the Reporting Office without delay of any pending proceedings connected with Articles 260ter, 260^{quinquies} paragraph 1, 305bis and 305ter paragraph 1 SCC. They shall provide the Reporting Office without delay with judgements and decisions on the closure of proceedings, including the grounds therefor.

[2] They shall also notify the Reporting Office without delay of rulings that they have issued on the basis of a report from the Reporting Office.

[2bis] They shall use the information passed on by the Reporting Office in accordance with the conditions laid down by the Reporting Office in each individual case in accordance with Article 29 paragraph 2ter.

[3] They may provide FINMA, the FGB, the intercantonal authority and the Central Office with all the information and documents they request

in the course of performing their task, provided that this is not prejudicial to the criminal proceedings.

[4] FINMA, the FGB, the intercantonal authority and the Central Office shall coordinate any interventions in relation to a financial intermediary with the competent prosecution authorities. They shall consult the competent prosecution authorities before passing on any information or documents received.

CONTENT

I. History 530
II. Concept of criminal authorities 534
III. Obligations of the criminal authorities towards the reporting office 536
A. Information obligations (paragraphs 1 and 2) 536
B. Compliance with restrictions on use (paragraph 2bis) 541
IV. Cooperation between criminal authorities and supervisory authorities 549
A. Criminal authorities: disclosure of information and documents to supervisory authorities (para. 3) 549
B. Supervisory authorities: coordination of proceedings with law enforcement authorities (para. 4) 551
Bibliography 552
Materials 552

I. HISTORY

1 Back in the 1990s, the FATF recommended in its **Recommendation No. 32** that member states continuously review the effectiveness of their anti-money laundering measures. To this end, statistical data should be collected not only on suspicious activity reports received and forwarded, but also on criminal proceedings and convictions relating to money laundering, seized and confiscated assets, and international mutual legal assistance in the area of money laundering. Against this background, the original version of the Anti-Money Laundering Act, which came into force in Switzerland in 1998, already required cantonal criminal authorities in **Art. 29 para. 2 aGwG** to report all pending proceedings in connection with a criminal organization (Art. 260ter SCC), money laundering (Art. 305bis SCC) and lack of due diligence in financial transactions (Art. 305ter SCC). Beyond the requirements of FATF Recommendation No. 32, the Swiss legislature also intended that this information would help the reporting office to continuously improve its own analysis and forwarding practices and to train financial intermediaries.

2 In practice, it became apparent after only a few years that the reporting office was not receiving sufficient information to fulfill its tasks. This was due, on the one hand, to gaps in the existing provisions of Art. 29 para. 2 aGwG and, on the other hand, to the inadequate implementation of the reporting obligations contained therein by the cantonal law enforcement authorities. The **shortcomings in the collection of statistical data** were also criticized by the FATF in its 2005 country review report. As part of the 2007 revision of the Anti-Money Laundering Act, the Federal Council proposed, among other things, **amendments to the regulations on the exchange of information** between the criminal authorities and the other Swiss authorities involved in the implementation of the Anti-Money Laundering Act. Parliament made only cosmetic changes, and the new regulations came into force on February 1, 2009. These contained the following key changes:

- Replacement of the previous Art. 29 para. 2 AMLA with the new Art. 29a AMLA,
- Extension of reporting obligations to all criminal authorities, now also including federal authorities and all courts,
- Obligation to deliver decisions, including their reasoning,

- Explicit regulation of reporting obligations in proceedings initiated by reports to the Money Laundering Reporting Office,
- Creation of a legal basis for the disclosure of information by the criminal authorities to the supervisory authorities responsible for implementing the AMLA,
- Obligation of the supervisory authorities to coordinate their proceedings with the criminal prosecution authorities.

With the Money Gaming Act, which came into force on January 1, 2019, organizers of large-scale games were defined as financial intermediaries within the meaning of the AMLA (Art. 2 para. 2 lit. f AMLA), in addition to casinos. Since **the supervision of large-scale games** falls within the competence of the cantons (Art. 106 para. 3 of the FC), the cantons were required by federal law in the Money Gaming Act to entrust an intercantonal authority with the supervision of large-scale games. This authority complements the Federal Gaming Board and, like the latter, has the task of monitoring compliance with anti-money laundering obligations (Art. 107 para. 1 lit. a no. 2 BGS) In order to enable this intercantonal authority, the Intercantonal Money Gaming Supervisory Authority (Gespa), to fulfill its tasks in the area of money laundering, Art. 29a AMLA was amended to allow the criminal authorities to disclose information and documents not only to the ESBK but also to the intercantonal authority. 3

The Federal Decree on the Approval and Implementation of the Council of Europe Convention on Terrorism of September 25, 2020, contained the following **two cosmetic amendments to Art. 29a para. 1 AMLA,** which came into force on July 1, 2021: 4

- Replacement of the word "promptly" with the word "immediately";
- Deletion of "paragraph 1" after "Article 260ter."

The **reason for replacing "promptly" with 'immediately'** is not mentioned in the materials. Naegeli suspects that this was done to correct the stylistically unattractive double use of "promptly" in the same paragraph. 5

The **reason for deleting "no. 1"** is more difficult to understand: in the version applicable until 2021, the offense of participation in a criminal organization was included in no. 1 of Art. 260ter SCC. In the version that came into force on July 1, 2021, the offense is included in paragraph 1. It would therefore 6

have been obvious to replace "paragraph 1" with "paragraph 1" in Art. 29a AMLA, especially since the references to Art. 260^{quinquies} and 305ter in Art. 29a AMLA also contain the clarification "paragraph 1." The deletion of "paragraph 1" only becomes understandable when the history of the revised Art. 260ter SCC is taken into account: this article contained the criminal offense in two paragraphs in both the consultation draft and the draft federal decree on the approval and implementation of the Council of Europe's Convention on Terrorism (paragraph 1 concerning criminal organizations and paragraph 2 concerning terrorism). The proposal to delete "paragraph 1" in Art. 29a AMLA was therefore correct. It would have been possible to replace "paragraph 1" with "paragraphs 1 and 2." However, during parliamentary deliberations, paragraphs 1 and 2 of Art. 260ter SCC proposed by the Federal Council were combined into a newly worded paragraph 1. Consequently, the reference to Art. 260ter "paragraph 1" in Art. 29a AMLA should have been replaced by "paragraph 1." This may simply have been overlooked.

7 **As a result, Art. 29a AMLA in its current version is inconsistently worded** in that there are references to paragraph 1 with regard to Art. 260^{quinquies} and Art. 305ter SCC, but not with regard to Art. 260ter SCC, even though this article also only contains the criminal offenses in paragraph 1. However, it is not clear what purpose the clarifications regarding "paragraph 1" in Art. 29a AMLA serve. If these were omitted, nothing would change in terms of content: the criminal authorities would have to report exactly the same criminal proceedings. It would therefore be appropriate to delete all references to "paragraph 1" in Art. 29a in a future revision of the AMLA. This would streamline the article and make its wording more consistent.

8 In 2016, the FATF evaluated Switzerland's legal and institutional framework for combating money laundering and terrorist financing. The Federal Council took up the recommendations of the **FATF country report 2016** and initiated a revision process of the AMLA in 2017, which led to the following two amendments to Art. 29a AMLA:

- Introduction of para. 2bis in Art. 29a AMLA with the following text: "They *[the criminal authorities]* shall use the information forwarded by the reporting office in accordance with the conditions laid down by the latter in each individual case in accordance with Article 29 paragraph 2ter."

- Paragraph 3: Replacement of ”intercantonal supervisory and enforcement authority under Article 105 BGS“ with ”intercantonal authority“ and insertion of ”and the Central Office" .

Para. 2bis created the legal basis for the reporting office to comply with FATF Recommendation No. 40, which requires that information received from foreign authorities may only be passed on to other domestic authorities in compliance with the conditions associated with its disclosure. This amendment to Art. 29a AMLA, which came into force on January 1, 2023, implemented a long-standing request by the reporting office. However, this regulation raised numerous questions in criminal proceedings that remained unresolved. 9

In addition, this revision newly designated trade auditors and group companies pursuant to Art. 42bis of the Precious Metals Control Act (EMKG) as financial intermediaries (Art. 2 para. 2 lit. g AMLA) and thus subject to the AMLA. At the suggestion of the Swiss Association of Precious Metal Manufacturers and Dealers (ASFCMP), the **Central Office for Precious Metals Control**, which is already responsible for enforcing the Precious Metals Control Act, was also tasked with supervising and monitoring the obligations arising from the AMLA (Art. 36, 42bis and 42ter EMKG). Consequently, the Central Office was placed on an equal footing with the other supervisory authorities involved in the enforcement of the AMLA, including in Art. 29a para. 3 AMLA. 10

The **replacement of “intercantonal supervisory and enforcement authority under Article 105 FCA” with “intercantonal authority”** was not explained in the message in the explanatory notes to Art. 29a AMLA. The aim was probably to streamline the text of the law: In Art. 12 AMLA, a new lit. b^{bis} was introduced in paragraph 1. This refers to the intercantonal supervisory and enforcement authority and notes in brackets that this authority is referred to in the rest of the text of the law as “intercantonal authority.” 11

On August 30, 2023, the Federal Council opened the consultation process on the **Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners**. This involves amendments to the AMLA. In particular, “advisors” are to be subject to the AMLA. “Advisors” are essentially persons who perform certain activities in connection with the establishment and structuring of legal entities, i.e., who are particularly active in legal advice and fiduciary services. As a consequence, supervisory authorities could intervene with advisors in the future, which is why Art. 29a AMLA is to be amend- 12

ed to stipulate that supervisory authorities must also coordinate any interventions with "an advisor" with the law enforcement authorities. In its message published on May 22, 2024, the Federal Council largely stuck to its proposals, including the amendment to Art. 29a AMLA. The Federal Assembly debated the actual Transparency Act and the amendments to the Anti-Money Laundering Act contained in the bill separately. Although the Federal Council's proposals regarding the subordination of "advisors" were controversially discussed, this had no influence on the amendment to Art. 29a para. 4 AMLA proposed by the Federal Council. It was adopted without amendments by the Council of States on June 17, 2025, and by the National Council on September 11, 2025.

II. CONCEPT OF CRIMINAL AUTHORITIES

13 Art. 29a AMLA imposes various rights and obligations on "criminal authorities." The AMLA does not contain a definition of this term. The framework for the term "criminal authorities" in Art. 29a AMLA is derived from the scope of application of the AMLA: In principle, Art. 29a AMLA only covers criminal authorities that are active in the fight against money laundering, organized crime, and terrorist financing. Administrative criminal authorities such as the Criminal Affairs and Investigations Division of the Federal Tax Administration do not fall under the term "criminal authorities" within the meaning of Art. 29a AMLA. The legislative history and materials also show that Art. 29a AMLA refers not only to cantonal criminal authorities, but also to those **of the federal government**. Furthermore, the term "criminal authorities" includes the **courts** of all instances. This is evident from the materials and the systematics of the AMLA, which only uses the term "criminal authorities" in Art. 29a, but otherwise consistently refers to "law enforcement authorities." In this respect, the use of the term in the AMLA is consistent with the definitions contained in Articles 12–14 of the Swiss Criminal Procedure Code.

14 It is not entirely clear whether the **police** also belong to the "criminal authorities" within the meaning of Art. 29a AMLA. Applying the definition of terms in the Criminal Procedure Code, this would be the case: according to Art. 12 CrimPC, the police, together with the public prosecutor's office and the misdemeanor authorities, form the "law enforcement authorities," which, together with the courts, form the "criminal authorities." It should be noted, however, that the Swiss Criminal Procedure Code (CrimPC) did not come into force

until 2011. The AMLA, which came into force in 1998, could therefore not be based on the definition in the CrimPC at the time of its enactment. In practice, the authorities involved (the reporting office, federal and cantonal public prosecutors, police) traditionally understood the term "law enforcement authorities" to mean the public prosecutor's office and not the police. In particular, the reporting office has so far filed reports with the federal and cantonal public prosecutors' offices within the meaning of Art. 23 AMLA, and the police have not reported any pending criminal proceedings to the reporting office on the basis of Art. 29a para. 1 AMLA. On the other hand, the 2012 message on the amendment to the Anti-Money Laundering Act indicates that the term "law enforcement authorities" used in Art. 23 para. 4 AMLA includes not only the public prosecutor's office but also the police. Apart from a reference to Art. 12 of the CrimPC, this interpretation of the term "law enforcement authorities" is not further justified in the dispatch. The requirement for coherent legislation is that a term should have the same meaning at least within the same law. The term "law enforcement authorities" is used in numerous places in the AMLA: for example, the reporting of suspicious transactions by the reporting office to the "law enforcement authorities" in accordance with Art. 23 para. 4 AMLA triggers a freezing of assets by financial intermediaries. According to the AMLA, this must be maintained until a decision is received from the "law enforcement authorities" (Art. 10 para. 1 and 2 AMLA). However, according to the CrimPC, only the public prosecutor's office is responsible for the seizure of assets and the issuance of account freezes (Art. 198 para. 1 in conjunction with Art. 263 CrimPC), not the police. It is inconsistent that the term "law enforcement authority" in Art. 10 AMLA cannot include the police, but in Art. 23 para. 4 AMLA the same term is supposed to include the police.

It should therefore be noted that the terms "criminal authority" and "law enforcement authority" are not used consistently and uniformly in the AMLA. The terms must therefore be interpreted teleologically (purpose-oriented). With regard to Art. 29a AMLA, this means that the terms "law enforcement authorities" and "criminal authorities" also include the police, because it would be incompatible with the purpose of Art. 29a para. 2bis AMLA, for example, if only the public prosecutor's office and the criminal courts had to comply with the restrictions on use imposed by the reporting office, but not the police. In addition, the information provided by the police is just as important to the AMLA supervisory authorities as the information provided by the public prosecutors, which is why Art. 29a para. 3 AMLA must also include 15

the police when viewed from a teleological perspective. Consequently, the police also fall under the category of "criminal authorities" within the meaning of Art. 29a para. 1 AMLA and are therefore generally obliged to report to the reporting office any proceedings pending before them in the areas of money laundering, organized crime, and terrorist financing. However, as long as the reporting office refrains from requesting such reports from the police, this obligation remains a dead letter.

16 The consistent use of the terms "criminal authorities" and "law enforcement authorities" in the AMLA therefore remains **a matter for future revision of the law**. In the interests of consistency in the legal system, the definition of terms in the Swiss Criminal Procedure Code should be adopted and applied uniformly and clearly to the AMLA.

III. OBLIGATIONS OF THE CRIMINAL AUTHORITIES TOWARDS THE REPORTING OFFICE

A. Information obligations (paragraphs 1 and 2)

17 The reporting office is tasked, among other things, with conducting operational and strategic analyses and producing an annual report on money laundering, its predicate offenses, organized crime, and terrorist financing (Art. 1 MGwV). To this end, the reporting office requires information on criminal proceedings conducted in Switzerland in these areas of crime. The reporting office is aware of some of these proceedings, namely those initiated on the basis of reports made by the reporting office to the criminal prosecution authorities pursuant to Art. 23 para. 4 AMLA. However, the criminal authorities also conduct criminal proceedings relating to money laundering, lack of due diligence in financial transactions, organized crime, and terrorist financing that are *not* based on reports from the reporting office. In order to fulfill its tasks, the reporting office must be informed about these proceedings. However, this is only a first step: a mere overview of the criminal proceedings conducted in Switzerland in the aforementioned areas of crime is not sufficient for their analysis. For this **purpose**, the reporting office requires in-depth information from the criminal case files. In principle, it would be useful to have access to the entire files of the relevant criminal proceedings. However, it would not be feasible for the reporting office to process the complete case files. For reasons of efficiency, it makes sense to limit the reporting to deci-

sions that conclude criminal proceedings (judgments, summary penalty orders, orders to discontinue proceedings). In addition to the criminal consequences, these decisions usually contain a description of the facts of the case, including the respective predicate offenses of money laundering, and a statement of reasons.

In order to enable the reporting office to fulfill its mandate, it therefore makes sense to legally oblige the criminal authorities to do the following: 18

- Report all pending proceedings relating to money laundering, organized crime, terrorist financing, and lack of due diligence in financial transactions of which the reporting office is not yet aware.
- To deliver the complete final decisions (judgments in the reasoned version, summary penalties, orders to discontinue proceedings) in all proceedings concerning money laundering, organized crime, terrorist financing, and lack of due diligence in financial transactions.

The **reporting** of all relevant criminal proceedings by the criminal authorities is stipulated in Art. 29a para. 1 AMLA. The presiding judge (cf. Art. 61 CrimPC) is obliged to report criminal proceedings relating to the aforementioned areas of crime to the reporting office as soon as such proceedings become pending. Criminal proceedings are pending even before they are formally opened within the meaning of Art. 309 of the CrimPC. 19

Art. 29a AMLA contains the following provisions regarding the service of criminal proceedings files: 20

- Paragraph 1: Service of *judgments and orders to discontinue proceedings*, including reasons, concerning proceedings that are not based on reports from the reporting office.
- Paragraph 2: Reporting of all *orders* issued on the basis of a report by the reporting office.

This provision is **flawed in several respects:**

1) In view of the purpose of the provision (preparation of analyses by the reporting office), it makes no sense to have different provisions for criminal proceedings that have been initiated with or without a report by the reporting office. There is no justification for the different provisions in the materials and none is apparent.

2) para. 1 limits delivery to "judgments and orders to discontinue proceedings." This wording is very narrow and does not even cover all final decisions (penalty orders and orders not to prosecute are missing). In practice, many more criminal proceedings are concluded with penalty orders than with judgments. No justification for this restriction can be found in the materials, nor is it apparent.

3) In contrast to para. 1, para. 2 defines the scope of the documents to be served in an extremely broad manner: the wording covers the service not only of final decisions, but of all decisions and thus also of all interim decisions relating to the conduct of the proceedings. These include investigation orders to the police, search warrants, arrest warrants and detention orders issued by the coercive measures court, disclosure orders of all kinds (including bank disclosures), orders for covert coercive measures such as telephone surveillance, and many more. The literal implementation of the text of the law would lead to a high workload for the criminal authorities and an extraordinarily high workload for the reporting office in analyzing the incoming orders.

4) Para. 2 refers to orders that were issued "on the basis of" a report by the reporting office. If a particular suspicion is already known to a law enforcement agency before the reporting office files a report, in practice this is added to the criminal proceedings already pending. If para. 2 is interpreted literally, orders issued later in these criminal proceedings are not made "on the basis" of the report by the reporting office, but on the basis of the criminal proceedings already pending. Some criminal authorities conclude from this that in such cases no reports need to be made to the reporting office.

21 The shortcomings of a literal interpretation can be partially offset by a teleological interpretation. As already explained, the purpose of the provisions contained in Art. 29a para. 1 and 2 AMLA is to enable the reporting office to compile analyses and statistics on money laundering, its predicate offenses, organized crime, and terrorist financing, and to publish the results in an annual report. In addition, this should enable better training and awareness-raising among financial intermediaries and self-regulatory organizations.

22 Taking into account a teleological interpretation yields the following results for **paragraph 1**:

- "Judgments": **Penalty orders** become judgments without a valid objection (Art. 354 para. 3 CrimPC). Penalty orders are therefore understood as

"proposed judgments" and the public prosecutor's office exercises a judicial function when issuing a penalty order. The term "judgment" therefore also includes summary orders within the meaning of Art. 353 CrimPC when interpreted correctly.

- "Discontinuation orders": The requirements for issuing a **non-prosecution order** and a dismissal order are the same, except for the question of whether the criminal investigation to be concluded was opened within the meaning of Art. 308 CrimPC. With regard to the regulation of non-prosecution orders, the law essentially refers to the provisions on the discontinuation of proceedings (Art. 310 para. 2 CrimPC). The term "discontinuation orders" therefore also includes, when interpreted correctly, non-prosecution orders within the meaning of Art. 310 of the CrimPC.

With regard to **paragraph 2**, the reporting office already interprets the word "decisions" restrictively and requires the criminal authorities to provide not only the opening decisions but also, in addition to judgments, summary orders, discontinuation and non-prosecution decisions, also suspension and resumption decisions. This restriction makes sense from a teleological point of view, as the delivery of criminal proceedings files should empower the reporting office to fulfill its tasks and not block them. From a systematic and teleological point of view, paragraphs 1 and 2 should also be brought into line with each other as far as possible. The word "decision" in paragraph 2 should therefore be interpreted restrictively to mean that the criminal authorities are only required to deliver **final decisions** (including suspension orders) to the reporting office. 23

According to Art. 381a of the CrimPC, federal authorities are entitled to take legal action if federal law stipulates that they must be notified of a decision. Decisions on the disposition of criminal proceedings concerning money laundering, organized crime, terrorist financing, and lack of due diligence in financial transactions must therefore be communicated to the reporting office **before they become legally binding**. 24

It was pointed out above that a literal interpretation of the term "on the basis of" allows the conclusion that no "decisions" need to be served on the reporting office if a report from the reporting office has been attached to criminal proceedings that are already pending. However, FATF Recommendation 2023, No. 33, calls on member states to maintain comprehensive statistics on 25

all areas that are essential to the effectiveness and efficiency of the anti-money laundering regime, including explicitly statistics on suspicious activity reports received and forwarded. The reporting office must therefore know whether its reports had any consequences and, if so, what those consequences were. A **teleological interpretation of the term "on the basis of"** therefore means that the decision to close the case, which finally decided on a suspicion reported by the reporting office to the public prosecutor's office, must be communicated to the reporting office, regardless of whether this suspicion was already known to the law enforcement authorities before the report was made. The following consideration leads to the same conclusion: the parties to criminal proceedings have the right to appeal regardless of how the criminal authorities initially became aware of the suspicions (Art. 107/382 CrimPC). The same must apply to the reporting office's right to appeal as enshrined in Art. 381a CrimPC: the reporting office must be notified of the disposition of its report so that it can exercise its right of appeal, regardless of whether the reported suspicion was already known to the prosecution authorities beforehand. However, if the law enforcement authorities are investigating various suspicions in the same criminal proceedings (e.g., for traffic offenses and money laundering), the reporting office does not have to be notified of decisions concerning suspects who do not fall within its jurisdiction. If the same decision on the case covers several grounds for suspicion, including one that falls within the reporting office's jurisdiction, the complete (uncensored) decision on the case must be sent to the reporting office, as the reporting office is bound by official secrecy and may only publish anonymized analyses and statistics on incidents within its jurisdiction.

26 Even if the legal basis for the delivery of decisions to the reporting office in Art. 29a para. 1 and 2 AMLA is not optimally formulated, the real challenge for the reporting office in fulfilling its mandate to prepare operational and strategic analyses and an annual report on money laundering, its predicate offenses, organized crime, and terrorist financing lies not in the flawed wording of the legal basis, but in its implementation: Unfortunately, the provisions contained in Art. 29a AMLA have **only been partially implemented** by the criminal authorities to date. The reporting office therefore contacts the criminal authorities at regular intervals and requests them to submit any outstanding notifications of decisions on the completion of proceedings. This does lead to an improvement in the data situation. However, the implementation of an IT-

based solution and the automation of the delivery of final decisions remain indispensable for the comprehensive enforcement of reporting obligations.

B. Compliance with restrictions on use (paragraph 2bis)

The background to this regulation, which came into force on January 1, 2023, is as follows: According to the FATF recommendations, each country must have a Financial Intelligence Unit (FIU) that acts as a nationwide central office for receiving, analyzing, and forwarding suspicious activity reports. These FIUs should be able to exchange information quickly and easily with each other. In addition, the FIUs should become members of the Egmont Group and comply with its rules on the exchange of information with foreign FIUs. In particular, exchanged information should only be used for the purpose for which it was requested, unless the FIU that provided the information consents to its use for other purposes. According to the principles of the Egmont Group, the FIU that receives information must **treat it as confidential** and may only use it within the scope of the consent given by the FIU that provided the information. Appropriate legal provisions must be in place. 27

Such legal bases did not exist in Switzerland when the revised FATF recommendations came into force in 2012. Accordingly, the relevant legal basis was added to the existing Art. 29 AMLA: since then, para. 2bis has contained the legal basis for the transmission of information by the reporting office to other authorities, in particular to public prosecutors and the police, both on request and spontaneously (i.e., on the reporting office's own initiative and without a request from the receiving authority). Para. 2ter restricted this possibility of administrative assistance by the reporting office to domestic authorities to the extent that the reporting office may only pass on information received from foreign FIUs with their express consent. In doing so, the legislator implemented a core principle of the Egmont Group. 28

In practice, however, it became apparent that **these legal bases were not sufficient** to ensure Switzerland's compliance with the Egmont principles: Although the reporting office routinely imposed the condition that information from foreign FIUs be treated confidentially by the recipient authority (usually the public prosecutor's office), not be included in the case files, and, in particular, not be disclosed to the parties to criminal proceedings, these 29

conditions **conflicted** with the provisions of the Swiss Criminal Procedure Code concerning the keeping of files and access to files by the parties:

- **File management:** According to the Swiss Criminal Procedure Code, all information and evidence relating to criminal proceedings must be included in the files (Art. 100 CrimPC). In principle, the prosecution authorities may not withhold any material they have collected or received that is relevant to the case.
- **Right to inspect files:** According to the Criminal Procedure Code, the parties must be granted access to the complete files (Art. 101 and 107 para. 1 lit. a CrimPC). Although the right to inspect files may be restricted in certain respects, this does not apply to legal counsel (Art. 108 CrimPC).

30 Various cantonal public prosecutors therefore took the view that the reports in which the reporting office forwarded information from a foreign FIU to a public prosecutor's office for use in criminal proceedings should be included in the criminal files. Compliance with the confidentiality requirement was not possible, or only within the narrow limits of the Swiss Criminal Procedure Code. This meant that although the reporting office complied with the disclosure requirements of foreign FIUs and forwarded the information received to the law enforcement authorities only under appropriate conditions, it could not guarantee that the law enforcement authorities would actually comply with these confidentiality requirements. By taking this approach, Switzerland risked violating its international obligations and causing foreign FIUs to stop transmitting information to Switzerland or to the reporting office.

31 The **purpose of paragraph 2bis** is now to resolve this conflict between the Egmont Principles and the Swiss Criminal Procedure Code by legally obliging the criminal authorities to comply with the reporting office's requirements regarding the further use of transmitted information. According to the materials, the legislature wanted this provision to enable the public prosecutor's office to obtain information in accordance with the conditions set by the reporting office **without having to include it in the case files**. However, the wording chosen is difficult to understand, even for specialists. In addition, important questions arise in the implementation process for both the reporting office and the public prosecutor's office, which remain unresolved. The legal solution must be considered a failure.

According to the **wording** of Art. 29 para. 2bis AMLA, when using the information forwarded by the reporting office, the criminal authorities must comply with the conditions specified by the reporting office in each individual case "in accordance with Article 29 para. 2ter." A grammatical interpretation of this passage suggests that Art. 29 para. 2ter AMLA lists the various possible conditions that the reporting office may impose. However, this is not the case. Instead, Art. 29 para. 2ter AMLA refers to Art. 29 para. 2bis AMLA with regard to the "purposes of disclosure." However, Art. 29 para. 2bis AMLA also does not contain any substantive provisions, but refers to Art. 30 paras. 2–5 AMLA. Art. 30 paras. 2, 3, and 5 are not relevant. Only Art. 30 para. 4 AMLA contains provisions concerning the conditions that the reporting office may impose when disclosing information. Although Art. 30 para. 4 AMLA concerns foreign FIUs, this paragraph could be applied "mutatis mutandis" to the Swiss criminal authorities. **Based on the wording of the law**, the reporting office can therefore only impose the conditions contained in Art. 30 para. 4 AMLA on the criminal authorities when forwarding information from foreign FIUs. With this interpretation of Art. 29a para. 2bis AMLA, the phrase "in accordance with Article 29 para. 2ter" would ultimately have only declaratory value, because the forwarding of information from foreign FIUs to all authorities in Switzerland, including the criminal authorities, is in any case regulated by Art. 29 para. 2ter AMLA. If anything, instead of the cumbersome triple reference in Art. 29a para. 2bis AMLA, a direct reference to Art. 30 para. 4 AMLA could have been made. 32

However, the **materials** reveal a **completely different meaning** of the phrase "in accordance with Article 29 paragraph 2ter." According to the message, the purpose of Art. 29a para. 2bis AMLA is to enable public prosecutors to obtain information in accordance with the conditions laid down by the reporting office without having to include it in the case file. The phrase "in accordance with Article 29 paragraph 2ter" is intended solely to clarify that the reporting office may only make the disclosure of information from foreign FIUs to the criminal authorities subject to this condition (namely, non-inclusion in the case files). There is no indication in the materials that the reporting office should be restricted in the formulation of conditions for the disclosure of information from foreign FIUs to Swiss criminal authorities. However, the intention of the legislature as set out in the dispatch could have been clearly formulated in the law in a simple manner by omitting the phrase "in accor- 33

dance with Article 29 paragraph 2bis" in Art. 29a para. 2bis AMLA and instead inserting the phrase "foreign reporting offices" after "information."

34 In the absence of court rulings, it remains unclear whether the reporting office is bound by the restrictions of Art. 30 para. 4 AMLA when formulating the conditions of use for the transmission of information from foreign FIUs to the criminal authorities, or whether it is free to choose the conditions of use. This distinction is particularly **relevant with regard to the inclusion of reports containing information from foreign FIUs in the files of criminal proceedings**, because Art. 30 para. 4 AMLA does not contain any legal basis for such a restriction.

35 The reporting office has been implementing Art. 29a para. 2bis AMLA in practice since January 1, 2023, by adopting the conditions imposed by the foreign reporting office when passing on foreign information to a Swiss criminal authority. Even though the restrictions on use applied by the reporting office are therefore generally tailored to each individual case, the reporting office usually uses the following standard notice:

"Use of the (international) information received in accordance with Art. 29 para. 2ter AMLA:

The above information is sensitive and subject to official secrecy. It is disclosed subject to compliance with the following conditions of use:

(1) The information may only be used for intelligence purposes.

(2) The receiving authority shall use the information exclusively for analysis purposes in the context of combating money laundering and its predicate offenses, organized crime, and terrorist financing.

(3) The information may not be used as evidence in administrative or judicial proceedings.

(4) The information may not be disclosed to third-party authorities under any circumstances without the prior, express, and written consent of MROS.

MROS reserves the right to request information about the use made of the information.

This standard notice does not include the requirement for the criminal authorities not to include the report or the information in the criminal proceed-

ings file. Given that, according to the message, this was the purpose of introducing Art. 29a para. 2bis AMLA into the law, this is very surprising.

The question arises as to how the public prosecutor's office deals with these requirements. First of all, it should be noted that the report transmitted by the reporting office to the public prosecutor's office with the information from the foreign FIUs must be included in the criminal proceedings files by the criminal authorities, because the warning notice from the reporting office does not contain any instructions to the contrary. It is also clear and unproblematic that the information may only be used in relation to money laundering and its predicate offenses, organized crime, and terrorist financing. Such reservations of specialty are also common in judicial assistance and can be implemented by the public prosecutor's office without further ado. In addition, the above-mentioned conditions of use raise the following questions for the criminal authorities in their implementation: 36

- **Use for information and analysis purposes only:** It is unclear what is meant by the public prosecutor's office only being allowed to use the information for information ("intelligence") and analysis purposes. The task of the public prosecutor's office is to investigate criminal offenses (Art. 6, 299, 308 CrimPC). To this end, it collects evidence (Art. 139 CrimPC), which can only be used in court if it has been collected in a legally correct manner and is therefore admissible (Art. 141 CrimPC). The public prosecutor's office does not collect information for intelligence and analysis purposes outside of criminal proceedings. The public prosecutor's office may therefore only include a report from the reporting office containing information from foreign FIUs in the files of a (pending or newly initiated) proceeding and analyze it like all other evidence to determine whether it contains information relevant to the assessment of a criminal offense. It remains unclear in what respect the public prosecutor's office should use the reports from the reporting office differently from other evidence.
- **No use as evidence:** This restriction on use has a clear legal basis in Art. 30 para. 4 lit. c AMLA. In terms of content, it undoubtedly means that foreign information may not be used to justify the final court decision. This restriction on use can be implemented by the criminal authorities without further ado. If a criminal authority wishes to use information received from the reporting office of a foreign FIU as evidence for a final criminal decision, it must follow the path of judicial assistance. However, it is unclear

whether this restriction on use means that the criminal authorities can use the foreign information to justify investigative measures, e.g., an international request for legal assistance, the disclosure of bank records, or the ordering of pre-trial detention. At the latest in the appeal proceedings (or the proceedings before the coercive measures court in the case of ordering pre-trial detention), the public prosecutor's office will have to submit the report received from the reporting office with the information from a foreign FIU to the court as evidence. The wording of the above restriction on use prohibits this. However, this would mean that the reports received from the reporting office could no longer be used by the public prosecutor's office at all and would therefore be worthless. The wording chosen by the reporting office should therefore be interpreted restrictively to mean that **only the use of the reports as admissible evidence in the final decision is prohibited**. Ultimately, the report from the reporting office containing information from foreign authorities has the same value as other police information, e.g., information transmitted by foreign police authorities to Swiss police authorities via Interpol. This view is supported by Art. 30 para. 4 lit. a no. 2 AMLA: Here, the use of foreign information (by analogy) for the initiation of criminal proceedings or to substantiate a request for legal assistance is explicitly provided for. If information can be used to initiate criminal proceedings, it must also be possible to use it for further investigative measures. The opposite would not make sense, as it would mean that the public prosecutor's office could initiate criminal proceedings on the basis of foreign information, but would not be allowed to continue with subsequent investigative measures. **In summary, it can be concluded that, despite the restrictions on use, the public prosecutor's office may use information received from foreign FIUs via the reporting office to justify further investigative measures.** However, its use as evidence in reaching and justifying the final decision is excluded.

- **No disclosure to third-party authorities:** Until the end of 2024, the reporting office used a standard text that prohibited disclosure not only to third-party authorities, but also to "third parties" in general. This raised the question of whether this also meant the parties and participants in the criminal proceedings. Such a restriction on use would have been contrary to fundamental party rights, in particular those of the accused, and would have been difficult to uphold. Since the beginning of 2025, the reporting office's standard text has only prohibited disclosure to third-party authori-

ties. The wording of this restriction on use prohibits the public prosecutor's office from disclosing foreign information to the criminal court or the police from disclosing it to the public prosecutor's office. This would restrict the use of foreign information to such an extent that it could hardly be used at all. The wording of the restriction on use must therefore be interpreted restrictively: disclosure between criminal authorities is permitted. However, disclosure to other authorities, such as the tax authority or a debt collection office, is prohibited.

37 It has already been pointed out that, in its previous practice, the reporting office does *not* instruct the criminal authorities not to include reports containing foreign information in criminal files. Since, according to the dispatch, this was the central purpose of the introduction of Art. 29a para. 2bis AMLA, the following comments are nevertheless appropriate: Although the new Art. 29a para. 2bis AMLA, as lex specialis and lex posterior, should in principle take precedence over the rules of the Criminal Procedure Code, even after the revision, the AMLA does not contain any explicit legal basis for restricting the criminal authorities' obligation to keep files and, associated with this, for restricting the right to inspect files. It is questionable whether the implicit provision contained in Art. 29a para. 2bis AMLA is sufficient for a derogation from the CrimPC, especially since the right to inspect files is a fundamental right of the accused guaranteed by the Federal Constitution. If, despite these doubts, it is assumed that there is a sufficient legal basis for the reporting office to instruct the criminal authorities not to include reports containing information from foreign FIUs in the criminal case files, the question arises for the criminal authorities as to how they should **specifically implement** this instruction in practice. There are basically two options: On the one hand, the report received from the reporting office could be included in the criminal case files, but without granting the parties to the criminal proceedings access to it, which could be based on Art. 108 para. 1 lit. b CrimPC. However, this solution has several weaknesses: First, a corresponding instruction from the reporting office not to include the report in the case files would not be implemented literally, but only in spirit. Second, it is unclear how such "secret files" would have to be marked so that all authorities, including any courts dealing with the case files, would not inadvertently disclose the report to the parties. Finally, the right to a fair hearing and access to files can only be temporarily restricted on the basis of Art. 108 of the CrimPC (see Art. 108 para. 3 and 4 of the CrimPC). However, at the time the information is used for further investigative

measures (with restriction of the right to a fair hearing), it is uncertain whether the foreign FIU will ever agree to the use of the information as evidence. It is unclear how to proceed if the foreign FIU does not give its consent. The better option would be for the criminal authorities not to include the report from the reporting office containing information from foreign FIUs in the files of the pending criminal proceedings, but to file it under a separate file number. In this way, the relevant requirement of the reporting office would be implemented verbatim and it would be clear that the parties to the previously pending criminal proceedings would not have access to the separately filed information. If the criminal authority comes to the conclusion that the report from the reporting office contains information that is relevant to the pending criminal proceedings (either incriminating or exonerating, cf. Art. 6 para. 2 CrimPC), the criminal authority would have to request the reporting office to grant permission to include the report in the files of the pending criminal proceedings.

38 The provision introduced into the law by Art. 29a para. 2bis AMLA has the advantage that the reporting office is authorized to comply with any requirements imposed by foreign FIUs by imposing binding restrictions on use on the criminal authorities. This improves the reporting office's opportunities for international cooperation and enables it to remain **in the Egmont Group**. For the criminal authorities, the problem arises that evidence that has not been collected in a legally correct manner may not be admissible in court (Art. 141 CrimPC). In the present context, this means that evidence used by the criminal authorities contrary to the restrictions on use imposed by the reporting office may not be admissible, as may any subsequent evidence (Art. 141 para. 4 CrimPC). The interpretation of Art. 29a para. 2bis AMLA as a validity provision within the meaning of Art. 141 CrimPC is contradicted by the fact that Art. 29a para. 2bis AMLA does not aim to protect the accused from punishment. Nevertheless, the restrictions on use, some of which are currently unclear, **pose procedural risks** for the criminal authorities. The reporting office faces the challenge of translating the requirements formulated by the Egmont Group for the handling of exchanged information into meaningful instructions for the criminal authorities acting in accordance with Swiss procedural law. A particular challenge is that the strictly confidential exchange of information required by the FATF and the Egmont Group conflicts with the principle of party disclosure in criminal proceedings in Switzerland. Art. 29a para. 2bis AMLA has not resolved this problem.

IV. COOPERATION BETWEEN CRIMINAL AUTHORITIES AND SUPERVISORY AUTHORITIES

A. Criminal authorities: disclosure of information and documents to supervisory authorities (para. 3)

While paragraphs 1 to 2bis codify the obligations of the criminal authorities towards the reporting office and the legally established feedback mechanism primarily serves the strategic functions of the reporting office, since February 1, 2009, para. 3 has regulated the **right to information** of all special supervisory authorities, namely FINMA, the ESBK, the intercantonal supervisory and enforcement authority under Article 105 BGS, and the Central Office for Precious Metals Control vis-à-vis the criminal authorities, and is intended to support the former in their supervisory activities. 39

The right to information closed a **legal loophole** at the federal level in 2009 and provided an adequate legal basis for effective cooperation between criminal and supervisory authorities. Based on the Swiss Criminal Procedure Code, which came into force on January 1, 2011, Article 101 para. 2 now also grants supervisory authorities the right to inspect files, but expressly only for pending proceedings. 40

However, in order to assess the guarantees required by law and compliance with the obligations under the Anti-Money Laundering Act, the supervisory authorities need to know not only whether a criminal investigation is currently underway against a company subject to supervision or its managers, but also whether and how previous criminal investigations have been concluded. Only by **inspecting** the files of **ongoing** ***and*** **completed criminal proceedings** do the supervisory authorities have all the information they need to grant, refuse, or withdraw licenses or to order supervisory measures. Their right to information should enable them to proactively perform their tasks of protecting the reputation and integrity of the financial center, as well as protecting creditors and the functioning of the market. 41

The supervisory authorities' right to information is therefore comprehensive in terms of content: the criminal authorities may provide them with all information and documents they request in the course of performing their duties. The scope of exchange between the criminal and supervisory authorities is thus broader than that between the reporting office and the supervisory au- 42

thorities based on Art. 29 para. 1 AMLA, which is limited to the application and enforcement of the Anti-Money Laundering Act.

43 While the right to information in favor of the supervisory authorities is comprehensive in terms of content, the present provision preserves the criminal authorities' scope for action with regard to the **timing** of the disclosure of the requested information and documents: The criminal authorities are authorized and required to provide the requested information, provided that this does not prejudice the criminal proceedings and that the interest of criminal prosecution does not (or no longer) preclude the disclosure of the information.

44 In addition to Art. 29a para. 4 AMLA, the revised Art. 38 FINMASA, which came into force on January 1, 2016, has been applicable to exchanges between law enforcement authorities and FINMA as a further legal and administrative assistance provision, although the relationship between these standards is not regulated by law and is therefore unclear. While Art. 38 FINMASA regulates the **mutual exchange** between FINMA and the criminal prosecution authorities within the framework of administrative and legal assistance, Art. 29a para. 3 AMLA only covers the unilateral exchange between these authorities, insofar as the criminal prosecution authority discloses and transmits information and documents from its proceedings. The relationship between criminal and supervisory proceedings in the exchange of information, which is the subject of heated debate due to the administrative cooperation obligations of supervised entities, is therefore irrelevant in the scope of application of Art. 29a AMLA and will not be discussed further here.

45 However, the legal provisions also differ in that Art. 29a AMLA stipulates that the criminal authorities shall transmit the information and documents **requested by the supervisory authorities**. Art. 38 FINMASA also contains a general authorization for criminal authorities to communicate with FINMA: information, which includes not only details but also documents, should be able to be transmitted by the criminal authorities to FINMA quickly and informally, not only at FINMA's request, but **also on their own initiative**.

46 Art. 38 FINMASA is also relevant to the exchange of information between the criminal prosecution authorities and the Central Office for Precious Metals Control due to the reference in Art. 42ter para. 3 EMKG.

For the ESBK, there is an explicit legal provision on mutual administrative and legal assistance with the criminal prosecution authorities in Art. 102 para. 2 BGS of September 29, 2017, and for the intercantonal authority in Art. 111 para. 2 of the same decree. As the intercantonal authority has no law enforcement powers, Art. 111 para. 2 BGS does not contain any provisions on mutual coordination of proceedings. 47

B. Supervisory authorities: coordination of proceedings with law enforcement authorities (para. 4)

The interests of law enforcement enjoy special protection during **ongoing criminal proceedings**. In contrast to the preceding para. 4, which therefore only refers to the coordination of proceedings between the supervisory authorities and the law enforcement authorities and does not include the adjudicating courts. In criminal and supervisory proceedings running in parallel, the exchange of information is intended to avoid duplication and enable effective cooperation between law enforcement and supervisory authorities. At the same time, it must be ensured that information and documents from the preliminary criminal proceedings are not made available to parties to the proceedings or third parties at an inopportune moment as a result of intervention by the supervisory authorities. Action by the supervisory authorities could warn those affected prematurely and jeopardize or prevent the subsequent access of the law enforcement authorities to evidence required for the criminal proceedings. If the interests of creditors, investors, or insured persons are at acute risk and action by the supervisory authority to avert danger cannot be postponed, information and coordination appear to be particularly important. This is all the more important given that supervised entities regularly contest law enforcement agencies' access to information and documents held by FINMA, citing their administrative obligations to cooperate. 48

Supervisory authorities are therefore generally required to **coordinate** their **interventions** with the financial intermediary concerned with the law enforcement agencies. Before forwarding the information and documents received from the law enforcement authorities, the supervisory authorities are additionally and expressly obliged to consult with the law enforcement authorities, although it remains unclear in what form this consultation should take place and whether the consent of the law enforcement authorities is required. According to the explanations in the dispatch, however, it is the inten- 49

tion of the legislator that the supervisory authority should consult with the law enforcement authorities on the use of the information and documents as soon as they are received, so that any interference with the ongoing criminal proceedings can be ruled out.

50 Following the entry into force of the revised Art. 38 FINMASA, FINMA signed memoranda of understanding on cooperation with the Office of the Attorney General of Switzerland and various cantonal public prosecutors' offices, which contain agreements on the form and content of mutual administrative and legal assistance requests.

BIBLIOGRAPHY

Naegeli Vera, Kommentierung zu Art. 29 GwG, in: Hsu Peter/Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Naegeli Vera, Kommentierung zu Art. 29a GwG, in: Hsu Peter/Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Beuret Arnaud, Kommentierung zu Art. 29a GwG in: Kunz Peter/Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar, Geldwäschereigesetz, Bern 2017.

Schwob Renate/Wolfgang Wohlers, Kommentierung zu Art. 38 FINMAG, in Watter Rolf/Bahar Rashid (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. Aufl., Basel 2019.

MATERIALS

Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG) vom 17.6.1996, BBl 1996 1101 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1996/3_1101_1057_993/de, besucht am 10.8.2024 (zit. Botschaft GwG 1996).

Botschaft zum Bundesgesetz über die Eidgenössische Finanzmarktaufsicht (Finanzmarktaufsichtsgesetz, FINMAG) vom 1.2.2006, BBl 2006 2829 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2006/303/de, besucht am 29.3.2025 (zit. Botschaft FINMAG 2006).

Botschaft zur Umsetzung der revidierten Empfehlungen der Group d'action financière (GAFI) vom 15.6.2007, BBl 2007 6269 ff, abrufbar unter https://

www.fedlex.admin.ch/eli/fga/2007/938/de, besucht am 10.8.2024 (zit. Botschaft GAFI 2007).

Botschaft zur Änderung des Geldwäschereigesetzes vom 27.06.2012, BBl 2012 6941 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2012/1031/de, besucht am 24.3.2025 (zit. Botschaft GwG 2012).

Botschaft zur Umsetzung der 2012 revidierten Empfehlungen der Group d'action financière (GAFI) vom 13.12.2013, BBl 2014 605 ff, abrufbar unter https://www.fedlex.admin.ch/eli/fga/2014/100/de, besucht am 29.3.2025 (zit. Botschaft GAFI 2014).

Botschaft zum Finanzmarktinfrastrukturgesetz (FinfraG) vom 3.12.2014, BBl 2014 7483 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2014/1633/de, besucht am 29.3.2025 (zit. Botschaft FinfraG 2014).

Botschaft zum Geldspielgesetz vom 21.10.2015, BBl 2015 8387 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2015/2141/de, besucht am 10.8.2024 (zit. Botschaft BGS 2015).

Botschaft zur Genehmigung und Umsetzung des Übereinkommens des Europarates zur Verhütung des Terrorismus mit dem zugehörigen Zusatzprotokoll und Verstärkung des strafrechtlichen Instrumentariums gegen Terrorismus und organisierte Kriminalität vom 14.9.2018, BBl 2018 6427 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2018/2301/de, besucht am 11.8.2024.

Erläuternder Bericht zur Vernehmlassungsvorlage bezüglich der Änderung des Bundesgesetzes über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung vom 1.6.2018, abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/52554.pdf, besucht am 11.8.2024.

Botschaft zur Änderung des Geldwäschereigesetzes vom 26.6.2019, BBl 2019 5451 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2019/1932/de, besucht am 11.8.2024 (zit. Botschaft GwG 2019).

Erläuternder Bericht zur Vernehmlassungsvorlage bezüglich des Bundesgesetzes über die Transparenz juristischer Personen und die Identifikation der wirtschaftlich berechtigten Personen vom 30.8.2023, abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/82297.pdf, besucht am 12.8.2024.

Botschaft zum Bundesgesetz über die Transparenz juristischer Personen und die Identifikation der wirtschaftlich berechtigten Personen vom 22.5.2024, BBl 2024 1607 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2024/1607/de, besucht am 24.3.2025 (zit. Botschaft TJPG 2024).

Bundesamt für Polizei, Die Praxis der Meldestelle; eine Zusammenfassung der Praxis seit 2004, Bern, März 2016.

Egmont Group of Financial Intelligence Units: Principles for Information exchange between financial intelligence units vom 28.10.2013, abrufbar unter https://egmontgroup.org/wp-content/uploads/2021/09/Egmont-Group-of-Financial-Intelligence-Units-Principles-for-Information-Exchange-Between-Financial-Intelligence-Units.pdf, besucht am 12.8.2024.

Eidgenössische Finanzmarktaufsicht FINMA, Leitlinien zur Rechtshilfe gegenüber inländischen Strafbehörden vom 20.11.2015, abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente//dokumentencenter/myfinma/3durchsetzung/leitlinien-zur-rechtshilfe-gegenüber-inländischen-strafbehörden.pdf?sc_lang=de&hash=3474150F154945950326994961137 56Ff, besucht am 30.3.2025.

Eidgenössische Finanzkontrolle (EFK); Bericht über die Prüfung der Aufgabenerfüllung der Meldestelle für Geldwäscherei vom 20.12.2021, abrufbar unter https://www.efk.admin.ch/wp-content/uploads/publikationen/berichte/sicherheit_und_umwelt/justiz_und_polizei/20146/20146be-endgueltige-fassung-v04.pdf, besucht am 30.3.2025.

Financial Action Task Force (FATF), International Standards on Combating Money laundering and the Financing of Terrorism & Proliferation (FATF-Recommendations) 2012, updated February 2025, abrufbar unter https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf, besucht am 30.3.2025.

Financial Action Task Force (FATF)/Groupe d'actioin financière (GAFI), 3ème Rapport d'Évaluation mutuelle de la Lutte Anti-Blanchiment de capitaux et contre le Financement du terrorisme, Suisse, Novembre 2005, Zusammenfassung abrufbar unter https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/mer%20switzerland%20resume.pdf.coredownload.pdf, besucht am 30.3.2025.

FATF (2016), Anti-money laundering and counter-terrorist financing measures – Switzerland, Fourth Round Mutual Evaluation Report, FATF Paris, abrufbar

unter https://www.fatf-gafi.org/content/dam/fatf-gafi/images/mer/mer-switzerland-2016.pdf, besucht am 12.8.2024.

Meldestelle für Geldwäscherei, Jahresberichte 1999 bis 2024, abrufbar unter https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/publikationen.html, besucht am 8.10.2025.

Vorentwurf und erläuternder Bericht bezüglich der Genehmigung und Umsetzung des Übereinkommens des Europarates zur Verhütung des Terrorismus mit dem zugehörigen Zusatzprotokoll und Verstärkung des strafrechtlichen Instrumentariums gegen Terrorismus und organisierte Kriminalität vom Juni 2017, abrufbar unter https://www.bj.admin.ch/bj/de/home/sicherheit/gesetzgebung/archiv/terror-europarat.html, besucht am 11.8.2024.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 29b AMLA

A commentary by Tina Triller

SUGGESTED CITATION

Tina Triller, Commentary of art. 29b AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Triller, art. 29b AMLA N. XXX

Section 1*a* Cooperation with Supervisory Organisations and Self-Regulatory Organisations

Art. 29*b*

[1] The Reporting Office may exchange with the supervisory organisations and self-regulatory organisations all information that is necessary for the application of this Act.

[2] It may only pass on information from prosecution authorities with their express consent to supervisory organisations and self-regulatory organisations.

[3] It may only pass on information from foreign reporting offices with their express consent and exclusively for the purposes specified in

Article 29 paragraph 2bis to supervisory organisations and self-regulatory organisations.

CONTENT

I. Introduction 560
II. Exchange of information with self-regulatory organizations (SROs) and supervisory organizations (AOs) (Art. 29b para. 1 AMLA) 560
A. Institutions eligible for administrative assistance 560
B. Optional provision 561
C. Exchange of "information" 561
D. Purpose limitation as a barrier to the exchange of information 561
III. Approval of the prosecuting authorities (Art. 29b para. 2 AMLA) 562
IV. Restrictions on use when forwarding foreign information (Art. 29b, para. 3 AMLA) 562
Bibliography 562
Materials 562

I. INTRODUCTION

1 With the creation of Art. 29b AMLA, the logical expansion of the national exchange of information to include self-regulatory and supervisory organizations (so-called para-statal supervisory authorities), which can exchange all information required for the enforcement of the AMLA with the reporting office. This legal amendment, which came into force on January 1, 2023, strengthens national cooperation and ensures compliance with the recommendations of the Financial Action Task Force (FATF). The content of Article 29b AMLA is practically identical to the provision on the exchange of information with supervisory authorities under Article 29, para. 1 AMLA, which is why the following explanations often refer to OK-Triller, Art. 29 AMLA, N. 9 ff.

II. EXCHANGE OF INFORMATION WITH SELF-REGULATORY ORGANIZATIONS (SROS) AND SUPERVISORY ORGANIZATIONS (AOS) (ART. 29B PARA. 1 AMLA)

2 Art. 29b AMLA provides the legal basis for the exchange of information between the Reporting Office and the self-regulatory organizations (SROs) and supervisory organizations (AO). In terms of content, this exchange of information is substantially aligned with Art. 29 para. 1 AMLA, since the SROs and AOs, as para-statal supervisory authorities, must also have access to the information available at MROS. Administrative assistance is reciprocal.

A. Institutions eligible for administrative assistance

3 Art. 29b para. 1 AMLA covers "**recognized**" SROs. According to Art. 24 AMLA, these are SROs that are recognized and supervised by the Swiss Financial Market Supervisory Authority FINMA and also have statutory authority to regulate and supervise their affiliated financial intermediaries. All financial intermediaries within the meaning of Article 2 paragraph 3 AMLA (Article 14 paragraph 1 AMLA) must be affiliated to an SRO.

4 MROS can also exchange information with AO. As a para-statal supervisory authority, an AO must be licensed by FINMA in order to carry out its financial market supervisory activities and implement its legal mandate. All indepen-

dent asset managers and trustees subject to the law must join an AO (Art. 5 in conjunction with Art. 61 FinIA).

B. Optional provision

In line with Article 29, paragraph 1 AMLA, the regulation of the exchange of information with self-regulatory and supervisory organizations is an "**optional provision**". The decision on whether to provide administrative assistance lies with MROS, the SROs or the AOs. 5

Administrative assistance can be provided in response to a specific request or spontaneously. 6

C. Exchange of "information"

In line with Article 29, para. 1 AMLA, the reporting office and the parastatal supervisory authorities can only exchange information, but not documents. This means that the information transmitted must be in **report form** and without delivery of (original) documents. 7

For further information on the practical aspects and the associated problems involved in the transmission of "information", please refer to OK-Triller, Art. 29 AMLA, N. 13 ff. 8

D. Purpose limitation as a barrier to the exchange of information

The exchange of information between MROS and the self-regulatory and supervisory organizations is limited to the **application of the Anti-Money Laundering Act**. This earmarking determines what information the authorities can exchange with each other. 9

In line with Article 29, para. 1 AMLA, the purpose of the AMLA includes all information relating to the fight against money laundering, the fight against terrorist financing and ensuring due diligence in financial transactions. The latter also includes the due diligence obligations of financial intermediaries or the obligations in the event of suspected money laundering (see also OK-Triller, Art. 29 AMLA, N. 12 et seq.). 10

III. APPROVAL OF THE PROSECUTING AUTHORITIES (ART. 29B PARA. 2 AMLA)

11 Unlike the administrative assistance between MROS and the supervisory authorities under Article 29, para. 1 AMLA, MROS may only pass on information from law enforcement authorities to the SROs and AOs with their express **consent.**

12 The report on the results of the consultation on the amendment of the Federal Act on Combating Money Laundering and Terrorist Financing stated that this provision is intended to take account of any conflicts of interest and to align the regulations with those concerning foreign reporting offices. The ultimate goal is to ensure that parastatal supervisory authorities are treated the same as foreign reporting offices (Art. 30 para. 5 AMLA).

IV. RESTRICTIONS ON USE WHEN FORWARDING FOREIGN INFORMATION (ART. 29B, PARA. 3 AMLA)

13 In line with the provisions of Art. 29 para. 2ter AMLA, information from foreign reporting offices may only be passed on to SROs and AOs with the express **permission of** the reporting office in question. In addition, Art. 29b para. 3 AMLA explicitly refers to the provisions of Art. 29 para. 2ter AMLA and thus to the analogous application of Art. 30 para. 2–5 AMLA.

14 For a detailed discussion of the associated interpretation issues, please refer to the OK-Triller, Art. 29 AMLA, N. 47 ff..

BIBLIOGRAPHY

Nägeli Vera, Kommentierung zu Art. 29 GwG, in: Hsu Peter Ch./Flühmann Daniel, Basler Kommentar, Geldwäschereigesetz, Zürich 2021.

MATERIALS

Botschaft zur Änderung des Geldwäschereigesetzes vom 26.6.2019, BBl 2019, abrufbar unter https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2019/1932/de/pdf-a/fedlex-data-admin-ch-eli-fga-2019-1932-de-pdf-a.pdf, besucht am 27.8.2024 (zit. Botschaft GwG 2019).

Vernehmlassung zur Änderung des Bundesgesetzes über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereigesetz), Ergebnisbericht vom 26.6.2019, abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/57537.pdf, besucht am 27.8.2024 (zit. Ergebnisbericht 2019).

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 30 AMLA

A commentary by Nathalie Kläy / Simon Zaugg

SUGGESTED CITATION

Nathalie Kläy/Simon Zaugg, Commentary of art. 30 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Kläy/Zaugg, art. 30 AMLA N. XXX.

Section 2 Cooperation with Foreign Authorities

Art. 30 Cooperation with foreign reporting offices

[1] The Reporting Office may pass on the personal data and other information that are in its possession or that it may obtain under this Act to a foreign reporting office provided that office:

a. guarantees that it will use the information solely for the purpose of analysis in the context of combating money laundering and its predicate offences, organised crime or terrorist financing;

b. guarantees that it will reciprocate on receipt of a similar request from Switzerland;

c. guarantees that official and professional secrecy will be preserved;

d. guarantees that it will not pass on the information received to third parties without the express consent of the Reporting Office; and

e. will comply with the conditions and restrictions imposed by the Reporting Office.

2 It may pass on the following information in particular:

a. the name of the financial intermediary or the dealer, provided the anonymity is preserved of the person making the report or who has complied with a duty to provide information under this Act;

b. account holders, account numbers and account balances;

c. beneficial owners;

d. etails of transactions.

3 Information is passed on in the form of a report.

4 The Reporting Office may consent to information being passed on by the foreign reporting office to a third authority provided the latter guarantees that:

a. it will use the information solely:

for the purpose of analysis in the context of combating money laundering and its predicate offences, organised crime or terrorist financing, or
to institute criminal proceedings relating to money laundering and its predicate offences, organised crime or terrorist financing or to obtain evidence in response to a request for mutual assistance relating to such criminal proceedings;

b. they will not use the information to prosecute offences that are not offences predicate to money laundering under Swiss law;

c. they will not use the information in evidence; and

d. they will preserve official or professional secrecy.

5 If the request to pass on the information to a foreign third authority concerns a matter that is the subject of criminal proceedings in

Switzerland, the Reporting Office shall first obtain the consent of the public prosecutor's office responsible for the proceedings.

[6] The Reporting Office is entitled to make more detailed arrangements on the modalities of cooperation with foreign reporting offices.

CONTENT

I. General 570
A. Background 570
B. Exchange of information between FIUs 571
1. International dimension of reports 571
2. Purpose 572
3. Extended powers of MROS 573
4. Egmont Group 573
II. Disclosure of information to foreign reporting offices (para. 1) 574
A. Requirements for the exchange of information with foreign FIUs 574
B. Types of information 574
1. Financial information 574
2. Personal data and police information 575
C. Use for analytical purposes in the fight against money laundering (lit. a) 575
1. Exchange of information for analysis purposes 576
2. Money laundering reference 576
D. Reciprocity principle (b) 577
E. Official or professional secrecy (lit. c) 578
F. Prohibition on disclosure without explicit consent (lit. d) 578
G. MROS's option to impose further conditions and restrictions on use (lit. e) 579
III. Examples of information to be transmitted (para. 2) 579
A. Exchange of financial information 579
B. Name of the reporting person (lit. a) 580
1. Maintaining anonymity 580
2. Duty to provide information 581
C. Further examples of financial information (lit. b–d) 582
IV. Reporting form (para. 3) 582
V. Forwarding to a foreign third authority (para. 4) 583
A. General 583
B. Possible uses of the information by a foreign third authority (lit. a) 584
1. Forwarding for analysis 584
2. Forwarding for law enforcement purposes 584
C. Dual criminality (lit. b) 585
1. MROS practice 585
2. Difference to Art. 30 para. 1 let. a AMLA 585
D. Prohibition on using the information as evidence (c) 585
E. Official or professional secrecy (let. d) 586
VI. Requirement for authorization in the event of Swiss criminal proceedings (para. 5) 586
A. General 586
B. Priority of Swiss criminal proceedings 586

C. Sources of information 587
D. MROS practice 587
VII. Memorandum of Understanding (para. 6) 588
A. MROS's authority to conclude 588
B. Reasons for an MoU 588
C. MROS practice 589
Bibliography 589
Materials 590

I. GENERAL

1 Article 30 AMLA governs the **collaboration between** the Money Laundering Reporting Office Switzerland (MROS) and foreign reporting Offices (often also referred to as Financial Intelligence Units or "FIUs").

2 In this context, the article can be divided into three thematic parts. The first thematic part, which consists of paras. 1–3 of Art. 30 AMLA, deals with the **transmission of** information from the reporting office to a foreign partner authority. It defines the requirements that the foreign reporting office must fulfill in order for MROS to be able to provide personal data and other information. In addition, the type of information transmitted and the form of transmission are specified.

3 Paras. 4 and 5 constitute the second thematic part of Art. 30 AMLA. This regulates the **forwarding of** information supplied by MROS by the foreign reporting office to a third-party authority. On the one hand, the conditions to be fulfilled by the third-party authority in the event of such forwarding are defined. On the other hand, the procedure to be followed by MROS is determined in the event that the request for forwarding of the information by the foreign reporting office to a third-party authority concerns a matter that is the subject of criminal proceedings in Switzerland.

4 The third and final part of Article 30 AMLA concerns para. 6. This gives MROS the authority to regulate the **arrangements for cooperation** with foreign reporting offices itself.

A. Background

5 When dealing with Article 30 AMLA, it is important to note that it did not come into force until November 1, 2013. This means that for the first 16 years of its existence, MROS was not authorized to exchange financial information, such as account holder, account number or transaction details, with foreign partner authorities due to banking secrecy and official secrecy. This was despite the fact that MROS is the Swiss *Financial* Intelligence Unit. Consequently, the entry into force of Article 30 AMLA, in addition to the **new powers** it granted to the Swiss reporting office, is noteworthy in that this new article removed the primacy of bank-client confidentiality and official secrecy when exchanging information between MROS and foreign reporting offices.

Before November 1, 2013, the Swiss reporting office's international exchange of information was based on Art. 32 para. 2 AMLA and essentially consisted of personal data and information on criminal proceedings pending in Switzerland, with reference being made to other channels, such as the police or mutual legal assistance channels. Art. 32 para. 2 AMLA, which had become redundant due to the new Art. 30 AMLA, was deleted without replacement.

The entry into force of Art. 30 AMLA was preceded by strong **international pressure**. In February 2012, the Financial Action Task Force (FATF, also known by its French name Groupe d'Action Financière, GAFI for short) revised its recommendations to the effect that reporting offices must be allowed to exchange all information, including financial information. According to the revised wording and the interpretative notes, this now explicitly included the financial information contained in the reports of financial intermediaries. This revision by the FATF regarding the exchange of financial information conflicted with Swiss banking secrecy and official secrecy. As a result, the option of passing on financial information was only introduced at MROS very late in international comparison. It was the last reporting office in the Egmont Group to receive this extension of competence – otherwise it would have been threatened with exclusion from the Egmont Group. However, Switzerland had an independent interest in being able to exchange financial information across borders. Foreign reporting offices could refuse to provide MROS with financial information as long as they did not provide such information themselves. This was detrimental to the efficient and successful fight against money laundering and its predicate offenses, organized crime and terrorist financing. 6

Article 30 AMLA not only gave MROS the ability to exchange **financial information** with foreign partner authorities, but also the authority to regulate cooperation with foreign FIUs itself (para. 6). In practice, this is a memorandum of understanding (MoU). Prior to November 1, 2013, the approval of MoUs with other reporting offices was reserved for the Federal Council. 7

B. Exchange of information between FIUs

1. International dimension of reports

The exchange of information between reporting offices is of central importance for the efficient combating of money laundering and its predicate offences, organised crime and terrorist financing at the national and interna- 8

tional level. This importance is evident from the fact that the majority of reports submitted to MROS have an **international dimension**. In accordance with Article 23 AMLA, MROS analyzes the suspicious activity reports submitted by Swiss financial intermediaries and decides whether to file a report with a Swiss law enforcement agency. The difficulty for MROS often lies in identifying the predicate offense that could have preceded the suspected money laundering. If the report shows a connection to a foreign country, MROS can resort to the fast and uncomplicated way of exchanging information internationally between reporting offices. This allows MROS to obtain potentially relevant information from abroad and to incorporate it into the report to a Swiss law enforcement agency. The exchange of information is either initiated by a request from MROS or can be made spontaneously by partner FIUs abroad, which independently forward potentially relevant information with a Swiss connection to MROS (spontaneous information).

2. Purpose

9 The information originating from a foreign FIU and forwarded by MROS to a Swiss law enforcement agency considerably simplifies any **international letters rogatory** by the Swiss law enforcement agencies. In this way, MROS can obtain key information (in practice, this is mostly financial information) through the exchange of information in a fast and efficient way, compared to the often lengthy and formal process of requesting mutual legal assistance. Supporting international mutual legal assistance is one of the main objectives of FIU exchanges.

10 In this context, the Swiss reporting office may decide to send the information contained in the report to a foreign reporting office instead of to a Swiss law enforcement agency. This makes particular sense if proceedings are already pending abroad in relation to the facts of the case or if it must be assumed that the Swiss law enforcement agency will not take action. In this situation – as well as when MROS responds to inquiries from foreign partner authorities – the often underestimated **added value** of information from reports submitted by Swiss financial intermediaries that is not forwarded to a Swiss law enforcement agency becomes apparent. The added value of MROS thus consists not only of its often-cited "filter function" between financial intermediaries and law enforcement authorities, but also of the targeted exchange of relevant financial information with foreign partner authorities. In this context, the in-

formation transmitted by the Swiss reporting office to foreign FIUs is of central importance, not only for the analysis carried out independently by the foreign reporting office or for the initiation of criminal proceedings, but above all for enabling or completing requests for mutual legal assistance from abroad to a Swiss authority.

3. Extended powers of MROS

The entry into force of Article 11a, para. 2bis AMLA on July 1, 2021 must be mentioned as a major **milestone** in MROS's cooperation with foreign reporting offices. Since that date, the Swiss reporting office has been able to request further information from financial intermediaries subject to the AMLA on the basis of information received from abroad (in particular spontaneous information and inquiries). This authority has expanded the powers of MROS to facilitate targeted and effective cooperation with foreign partner authorities. Before Article 11a Para. 2bis AMLA came into force, MROS was only allowed to request information from financial intermediaries subject to the AMLA when this information was related to a SAR that had already been received. 11

4. Egmont Group

The Egmont Group was founded in 1995 to ensure that the exchange of information between reporting offices is **secure and rule-based** despite the more informal nature of mutual assistance requests. MROS has been a member since it was founded in 1998. As of August 2024, a total of 177 FIUs were members of the Egmont Group – and the trend is rising. These 177 members cover all regions of the world, although there are still some gaps on the map, particularly in Asia and Africa. FIUs that are members of the Egmont Group can exchange information via the Egmont Secure Web, an electronic communication system. It should be noted that neither Art. 30 AMLA nor any other article of the law limits MROS to exchanging information only with members of the Egmont Group. Rather, the message regarding the amendment of the Anti-Money Laundering Act of June 27, 2012, clarifies that Article 30 AMLA applies to the exchange of information with the reporting offices of the Egmont Group as well as with the FIUs of all other countries. In practice, however, MROS only exchanges information with members of the Egmont Group. The main reasons for this are, on the one hand, the “seal of quality” that Egmont Group membership lends to foreign reporting offices and, on the other hand, the communication channel provided by Egmont Secure Web. 12

Depending on the circumstances and the characteristics of the foreign reporting office (e.g. independence from other authorities, internal organization or compliance with data protection), a response to a request from a FIU that is not a member of the Egmont Group will be considered if this serves the interests of MROS.

13 The **Principles for** Exchange of Information between Financial Intelligence Units, which are binding on the members of the Egmont Group, ensure that FIUs exchange information on combating money laundering, associated predicate offences, organized crime and terrorist financing in a fast, constructive and effective manner. In the worst case, failure to comply with the binding principles can lead to the exclusion of a reporting office from the Egmont Group.

II. DISCLOSURE OF INFORMATION TO FOREIGN REPORTING OFFICES (PARA. 1)

A. Requirements for the exchange of information with foreign FIUs

14 The first paragraph of Article 30 AMLA, together with paragraphs 2 and 3, governs the transmission of information from MROS to a foreign FIU. Para. 1 lists five **preconditions** that must be cumulatively fulfilled before the Swiss reporting office can pass on information to the partner authority abroad.

B. Types of information

15 In principle, MROS can exchange information with a partner FIU on **any subject** (i.e. financial information, personal data, police information) that it already has either through the receipt of reports of suspicions pursuant to Art. 9 AMLA (reporting requirement) or Art. 305ter para. 2 SCC (right to report) or that it can obtain by means of Art. 11a para. 1–2bis AMLA and Art. 29 para. 2 AMLA.

1. Financial information

16 In practice, the focus is clearly on the exchange of **financial information**. This generates the greatest added value in MROS's cooperation with foreign FIUs, since this information is usually only available at the national level at

MROS or can only be obtained from it. In this context, Art. 11a para. 2bis AMLA, which was mentioned in Chapter I.B.3., undoubtedly makes the greatest contribution to this added value in the exchange of financial information with partner FIUs. Before this MROS competence came into force on July 1, 2021, the international exchange of information via the FIU channel, which is based on reciprocity, was impaired. Since the entry into force of Art. 11a para. 2bis AMLA, the exchange with partner FIUs has improved considerably, which is also of great importance for Switzerland in the fight against money laundering at the national level (it should be noted here that the majority of suspicious activity reports from Swiss financial intermediaries have an international connection).

2. Personal data and police information

The exchange of personal data or police information primarily involves the exchange between **police authorities**, even though the Swiss FIU also transmits such information, which it obtains through access to various judicial and police databases. This occurs primarily in cases in which no prior exchange between police authorities has taken place, in which the requesting FIU specifically asks for it or in combination with financial information. In principle, the focus when analyzing FIU requests is on answering them – so mainly the information that covers the questions asked is transmitted to the corresponding partner FIU. 17

C. Use for analytical purposes in the fight against money laundering (lit. a)

Para. a is the first of five cumulative conditions that must be met in order for MROS to share information with partner FIUs. This first condition can be subdivided into two separate, yet interdependent, conditions: firstly, the information may only be used by the foreign FIU for **analytical purposes** (in the international exchange of information between FIUs, this is referred to as "for intelligence purposes only"), and secondly, this information may only be used in **the context of combating money laundering** and its predicate offenses, organized crime or terrorist financing. 18

1. Exchange of information for analysis purposes

19 In the case of cooperation between FIUs, information is generally only exchanged for **analysis purposes**. This means that the information may be used for analysis, investigations and/or to obtain investigative leads, but not as evidence or to support evidence. For the latter, the mutual assistance route must always be taken. Mutual assistance must never be circumvented through the exchange between reporting offices (the reason for this is to safeguard the rights of persons who are the subject of a request for mutual assistance), and for reasons of efficiency, double channelling (simultaneous exchange of the same information via the FIU and mutual assistance channels) must always be avoided.

2. Money laundering reference

20 The second condition in a) is more complex. In principle, it means that the FIU request must contain information that explicitly or implicitly describes **money laundering activities** or indicates a predicate offence to money laundering, organized crime or terrorist financing. It should be emphasized that the explicit condition that the predicate offence must be "under Swiss law" is not a requirement stipulated by the legislator when information is exchanged between FIUs. In Art. 30 para. 4 let. b AMLA – only when it comes to the disclosure of MROS information by the partner FIU to foreign third-party authorities – this becomes a requirement. In practice, however, the partial condition "in the context of combating money laundering and its predicate offenses, organized crime or terrorist financing" is interpreted according to Swiss law. In Switzerland, according to Art. 305bis para. 1 SCC, predicate offenses for money laundering are all acts in relation to assets that originate from a crime according to Art. 10 para. 2 SCC or from a qualified tax offense according to Art. 305bis para. 1bis SCC. However, the partner FIU does not have to explicitly state the predicate offense in its FIU request – it is sufficient if possible money laundering activities can be inferred from the facts of the case as stated in the information letter. The partner FIUs, with their core competence of forwarding substantiated suspicious cases to law enforcement authorities, are often at an early stage of analysis and do not yet have any definite evidence to definitively determine the predicate offense. In principle, the indicators of money laundering contained in the appendix to AMLO-FINMA are used by analogy. If no explicit predicate offense is mentioned in an FIU

request, MROS can exchange information with a partner FIU for analysis purposes (if necessary, also to determine the predicate offense). However, if the partner FIU explicitly mentions a predicate offense that is not a predicate offense for money laundering under Swiss law, and if no other connection to a crime can be established (for example, through the existence of a report from a Swiss financial intermediary), MROS does not pass on any information in this regard to the requesting partner FIU.

Each jurisdiction has its own laws and thus also different predicate offenses for money laundering. However, a **similar concept** of money laundering and its predicate offenses also prevails at the international level. The FATF lists a number of offenses in the appendix of its recommendation document, which sets minimum requirements for predicate offenses to money laundering ("Designated categories of offenses"). In practice, MROS conducts in-depth clarifications for two offenses before it delivers information to a foreign reporting office or grants permission to pass it on to foreign third-party authorities: tax offenses and sanction evasion. In the event of such suspicions, the Swiss reporting office clarifies in advance whether or not the case analyzed abroad actually falls under a money laundering offense in Switzerland. 21

D. Reciprocity principle (b)

The FIU exchange is always a give and take. A reporting office is expected to exchange with its foreign partners the information that it can obtain under the law applicable in its country. This is anchored in law in the **principle of reciprocity** of lit. b. As a general principle of international law and a basic principle of both the FATF (Recommendation 40) and the Egmont Group (Principles for Information Exchange between Financial Intelligence Units), a state is allowed to make its behavior towards another state dependent on the behavior of that state in a similar situation. Consequently, an FIU could refuse to cooperate, for example due to a lack of reciprocity or repeated inadequate cooperation. In such cases, MROS can only base its decision on its expectations and previous experiences with the partner FIU. In practice, this is not always easy due to the different types of FIUs (police, judicial, administrative) and the associated differences in their competencies (e.g. some FIUs can freeze assets while others cannot). Ultimately, however, the common goal of all FIUs is to combat money laundering and its predicate offenses, organized crime and terrorist financing. This also means that FIUs provide certain infor- 22

mation even if they know that their partner FIU cannot do so due to a lack of authority in this area. However, point b) creates the possibility for MROS to adapt its behavior towards a foreign FIU or not to have to exchange certain information if it finds that the partner FIU intentionally and systematically fails to provide information that it could obtain under its legal framework. In order for the Egmont Group FIUs to have an overview of the type of FIU and the existing competencies of their partner FIUs, the so-called "Egmont Biennial Census" exists, which is completed and updated by all FIUs every two years.

E. Official or professional secrecy (lit. c)

23 This provision also represents a fundamental principle of the FATF and the Egmont Group (Principles for Information Exchange between Financial Intelligence Units). It stipulates that all FIU employees must have legally committed themselves to maintaining **official and professional secrecy** and must have been sufficiently instructed about the associated obligations.

F. Prohibition on disclosure without explicit consent (lit. d)

24 Point d) stipulates that a FIU may not disclose information received to third parties without the **explicit consent of** MROS. The basis for this provision is also found in the Principles for Information Exchange between Financial Intelligence Units of the Egmont Group. The conditions for forwarding information transmitted by MROS to a partner FIU to foreign third-party authorities are governed by Article 30, paras. 4 and 5 AMLA. The reason lit. d is so important is that the FIU information exchange is only ever used for analysis purposes and is intended to prevent this information from being passed on to authorities that could misuse it as evidence. This ensures that the source of the information, i.e. the transmitting FIU, has control over the forwarding and use of the information after it has been transmitted to a partner reporting office. In practice, however, this requires a certain degree of trust, which is generally present between the members of the Egmont Group (and must be present for an efficient FIU information exchange). The Egmont Group also ensures that this provision is adhered to and takes repressive measures in the event of a violation (by initiating a non-compliance procedure in accordance with the Egmont Group Support and Compliance Process). Furthermore, the foreign FIU would have to bear the consequences of a breach of trust and

would no longer receive any information from MROS for the time being – a consequence that should not be underestimated, given the importance of the Swiss financial center. A resumption of the exchange of information between the Swiss reporting office and the affected FIU would only be possible if a satisfactory explanation for the failure to comply with this provision was provided and appropriate measures were taken to prevent such a breach in the future.

G. MROS's option to impose further conditions and restrictions on use (lit. e)

Para. e clarifies that the provisions in let. a–d are not exhaustive conditions, but that the Swiss reporting office can impose further **conditions and restrictions on use** on a partner FIU, both in individual cases and as standard. However, this is only possible if MROS ensures compliance with all legal requirements (international standards, principles of administrative assistance, Egmont Principles, etc.). Thanks to this provision, no legal changes are needed should the Swiss reporting office's disclaimer need to be modified. 25

Para. e thus also provides the legal basis for the MROS **disclaimer**. This is added to every information letter from the Swiss FIU and varies depending on whether or not permission is granted to forward information to foreign third-party authorities of a partner FIU. The MROS disclaimer is in itself a summary of the requirements of Art. 30 para. 1 and para. 4 AMLA and also states that MROS must always be protected as a source of information. 26

III. EXAMPLES OF INFORMATION TO BE TRANSMITTED (PARA. 2)

A. Exchange of financial information

Para. 2 lists non-exhaustive examples ("in particular") of the various types of information that MROS can transmit to foreign partner authorities. At the same time, it forms the legal basis for the exchange of financial information with foreign FIUs, making para. 2 the **central component** of Art. 30 AMLA, which came into force on November 1, 2013. This exchange of financial information is generally the most valuable part of the FIU information exchange, as this information is usually only available from the FIUs or can often only be 27

obtained from them (especially so quickly). The fact that one paragraph (Art. 30 para. 2 AMLA) is explicitly and exclusively dedicated to the exchange of financial information illustrates its importance (personal data, on which the FIU exchange by MROS was mainly based before the introduction of Art. 30 AMLA, is only briefly mentioned in para. 1 of Art. 30 AMLA).

28 Paras. a–d are examples of financial information that can be exchanged under this law. The legislator deliberately kept the list of such financial information open. Art. 30 para. 1 AMLA already allows MROS to transmit **all available information** to its foreign partner authorities. A restriction to certain categories of financial information would run counter to the goal of making the most comprehensive use of all available information in the analysis phase. In addition to the content listed under Art. 30 para. 2 lit. a-d AMLA, there is further financial information that MROS can pass on to a foreign partner FIU under this law. The additional financial information most frequently requested in practice includes information on authorized signatories, authorized agents, controlling persons, the balance of the assets involved, and KYC (Know Your Customer) information.

29 MROS obtains this financial information in two ways. Firstly, it receives **suspicious activity reports** from Swiss financial intermediaries in accordance with Art. 9 para. 1 AMLA or Art. 305ter para. 2 SCC, or from dealers in accordance with Art. 9 para. 1bis AMLA, which are then forwarded to MROS. On the other hand, the Swiss FIU can request information from financial intermediaries or dealers under **Art. 11a AMLA**. MROS's exchanges with national authorities under Art. 29 para. 1 and 2 AMLA also constitute a source of information that can be transmitted to foreign FIUs.

B. Name of the reporting person (lit. a)

1. Maintaining anonymity

30 In order to exchange financial information in a meaningful and efficient way, it is often essential to pass on the name of the financial intermediary with whom a business relationship exists. A possible request for mutual assistance from a foreign country to a Swiss public prosecutor requires the name of the financial institution from which financial information is to be requested (otherwise the request could be considered a fishing expedition). If MROS does not provide this information to the foreign FIU, the entire legal assistance process is

slowed down or even made impossible. The **anonymity of** the employees of reporting financial intermediaries or dealers who provide information is a top priority, with Art. 30 para. 2 let. a AMLA being in line with Art. 9 para. 1ter AMLA and Art. 32 para. 3 AMLA. The purpose of this provision is to protect natural persons (i.e. employees of reporting financial intermediaries or those disclosing information) and dealers from possible reprisals as a result of such a report or such information. The Swiss reporting office must refrain from disclosing the name of the financial intermediary if this would compromise the anonymity of the person who submitted a report to the reporting office or who fulfilled an information disclosure obligation under the AMLA. This is particularly the case for smaller financial intermediaries with few employees. If there is a real risk of such a loss of anonymity, MROS must refrain from passing on any information that could be used to identify specific individuals. In case of doubt, MROS has the option of asking the potentially at-risk person for consent.

It must be emphasized in this context that the FIU information exchange is about exchanging **(financial) information** and **suspicious facts**. The person who submitted the report is not decisive for the FIU information exchange. The key information is that there is a suspicion, with which financial intermediary the business relationship is held, and the findings from the analysis. In practice, this means that the Swiss reporting office does not explicitly mention the name of the reporting financial intermediary, but only passes on the information regarding which financial intermediary maintains the business relationship (even if in most cases the reporting financial intermediary and the one who maintains the business relationship are the same). 31

2. Duty to provide information

Para. a also mentions the "duty to provide information". This refers to the duty of financial intermediaries and dealers to **transmit information** to MROS that the latter has requested on the basis of Art. 11a AMLA. In addition to suspicious activity reports, this duty to provide information under Art. 11a AMLA is the main national source of financial information. a) of the AMLA states that MROS may in theory pass on the name not only of the financial intermediary or trader who submitted a report to a foreign reporting office, but also of those who have been requested by the Swiss FIU to provide information in accordance with Art. 11a AMLA (to preserve anonymity, see Chapter III.B.1.). 32

In practice, the same procedure applies here as for reporting financial intermediaries or dealers: in principle, only information regarding the account-holding financial intermediary is forwarded to a partner FIU, and not specifically who has issued the information.

C. Further examples of financial information (lit. b–d)

33 Para. b–d list further **examples of financial information** that may be passed on to a partner FIU under this Act. The main information regarding the account holder's business relationships, account number, account balances, beneficial owners and information on transactions is mentioned, although this is not an exhaustive list. The financial information listed in b) to d) is an important part of the information exchanged between the Swiss reporting Office and its foreign partners.

IV. REPORTING FORM (PARA. 3)

34 The form of the information exchanged between MROS and foreign reporting offices is governed by Art. 30 para. 3 AMLA. This states that the Swiss FIU may only transmit information that it has or can obtain to a partner authority abroad in **report form**. Conversely, this means that MROS does not share any original documents with the foreign FIU – FIUs are bound by the prohibition on the use of evidence. This is due to the fact that under no circumstances should cooperation between reporting offices circumvent or replace international mutual legal assistance. Original documents for use as evidence must be obtained through mutual assistance, while for the FIU's analysis tasks, for the initiation of criminal proceedings or to enable or complete a mutual assistance request, information in report form is sufficient.

35 The Swiss reporting Office is required by the requirement of the report form to limit itself to the essential information. In addition to the created information report, the MROS shares in practice **attachments** with foreign FIUs. These are, among other things, publicly available information, such as excerpts from the Swiss commercial register (Zefix). Due to the often extensive and complex transactions that FIUs have to analyze, MROS also sends attachments with the relevant transactions that allow the foreign FIUs to process the information contained therein more efficiently.

V. FORWARDING TO A FOREIGN THIRD AUTHORITY (PARA. 4)

A. General

Para. 4, which can be understood together with para. 5 as the second thematic part of Art. 30 AMLA, lists the requirements that a **foreign third-party authority** must fulfill in order to receive information from MROS via a foreign FIU. In this context, the partner FIU must obtain the prior consent of MROS before forwarding information to foreign third-party authorities, as already provided for in Art. 30 para. 1 let. d AMLA (see N. 24). This provision is therefore a prerequisite for the general exchange of information between FIUs. The conditions for the authorization of the forwarding of information to foreign third-party authorities (Art. 30 para. 4 AMLA) and those for the exchange of information between FIUs (Art. 30 para. 1 AMLA) are similar. It should be emphasized that Art. 30 para. 4 AMLA contains the additional restriction that the information passed on may only be used to prosecute offenses that constitute a predicate offense to money laundering under Swiss law. 36

The ultimate goal of forwarding information that a foreign FIU has received from MROS and in turn forwards to a third-party authority is to **effectively combat criminal behavior**. With their analytical work on money laundering phenomena, the FIUs perform crucial preliminary work for the downstream prosecuting authorities, which require the intelligence provided by the FIUs to conduct criminal proceedings and international mutual legal assistance proceedings. The sharing of information with third-party authorities, such as a police force or public prosecutor, is therefore essential for the prosecution of money laundering and its predicate offences, organised crime and terrorist financing. 37

In practice, MROS gives its **consent to the forwarding of** information in response to a request from a foreign FIU, although under certain circumstances, proactive consent is also conceivable. This makes sense, for example, when spontaneously sending information to a foreign FIU or in urgent cases, so that the information transmitted abroad can be used efficiently and effectively. 38

B. Possible uses of the information by a foreign third authority (lit. a)

39 Under lit. a, nos. 1–2, the two **possible uses** of the information transmitted by MROS are set out. These are exhaustive alternative conditions to be met and at the same time specify what is meant by the term 'third authority'.

1. Forwarding for analysis

40 In no. 1, the forwarding to foreign third authorities for **analysis purposes** in the context of combating money laundering, its predicate offences, organized crime and terrorist financing is stipulated. In principle, the FIUs carry out their analysis tasks themselves. However, it may be that the foreign FIU calls on the support of third authorities in the analysis of information. In this context, the main consideration is specialized central offices of the criminal police that have expertise in certain types of financial crime. Intelligence authorities are not covered by this definition, which is why forwarding to them is not permitted. The purpose of forwarding the information is to detect or prosecute criminal offences and is not preventive in nature, as is the case, for example, when intelligence authorities are involved.

2. Forwarding for law enforcement purposes

41 No. 2 governs the disclosure to foreign third-party authorities for the purpose of either **initiating criminal proceedings** for money laundering, predicate offences, organized crime or terrorist financing, or to **substantiate a request for mutual assistance** in the context of such criminal proceedings. In this context, it is mainly the prosecuting authorities that fulfill these purposes intended by the legislator. MROS draws the foreign FIU's attention to the competencies that the third-party authority must have in the disclaimer attached to the information letter. It seems unrealistic in practice to check whether each foreign third-party authority corresponds to a Swiss prosecution authority in accordance with Art. 12 CrimPC. The wording of no. 2 is adopted in the disclaimer mentioned above, according to which the authority must be entrusted with combating money laundering, its predicate offenses, organized crime or terrorist financing.

C. Dual criminality (lit. b)

1. MROS practice

Art. 30 para. 4 lit. b AMLA states that MROS may not authorize a foreign reporting office to forward a report to a third-party authority if the suspicions obviously do not reveal any predicate offense to money laundering under Swiss law. The **double criminality** will be a definite requirement. The respective legal provisions do not have to be identical – it is sufficient if the actions described in the information letter are punishable under the applicable law of both countries (under Swiss law, it must be a crime or a qualified tax offense, otherwise it cannot be classified as a predicate offense to money laundering). Furthermore, the predicate offense does not have to be explicitly mentioned by the foreign FIU (even if this is preferred in practice) – it is sufficient if it is apparent from the facts of the information letter. In case of doubt, MROS always has the option of obtaining further information regarding the suspected predicate offense from the foreign partner authority. 42

2. Difference to Art. 30 para. 1 let. a AMLA

As soon as the matter concerns a transfer to a foreign third-party authority, the legislator is stricter than it is when it comes to the exchange of information between FIUs. As already mentioned in chapter II.C.2, the condition that the predicate offense to money laundering must be "under Swiss law" as stated in Art. 30 para. 4 let. b AMLA, is **not an explicit requirement** for the exchange of information between FIUs. Due to the fact that FIUs are involved in the analysis of suspicious cases at an early stage of the detection of criminal acts, MROS can generally provide the information to the foreign FIU for internal analysis (see Chapter II.C.). 43

D. Prohibition on using the information as evidence (c)

Art. 30 para. 4 let. c AMLA explicitly states that the information from MROS may not be used as evidence, but only for **information purposes**. This is particularly important for the prosecution authorities mentioned in Art. 30 para. 4 let. a no. 2 AMLA. Evidence must always be obtained through mutual assistance. It is also clearly stated that mutual assistance should never be circumvented. As stated in Art. 30 para. 4 let. a no. 2 AMLA, the exchange of information between FIUs supports mutual assistance, but in no way replaces it. 44

E. Official or professional secrecy (let. d)

45 Art. 30 para. 4 let. d AMLA is the equivalent of Art. 30 para. 1 let. c AMLA and stipulates that the foreign third-party authority must also maintain **official and professional secrecy** or that its personnel must be subject to it.

VI. REQUIREMENT FOR AUTHORIZATION IN THE EVENT OF SWISS CRIMINAL PROCEEDINGS (PARA. 5)

A. General

46 The fifth paragraph of Article 30 AMLA stipulates that the MROS must obtain permission from a **Swiss public prosecutor** to pass on information to a foreign third-party authority if criminal proceedings are pending with that public prosecutor on the same facts. It should be emphasized that Article 30 para. 5 AMLA does not apply to the exchange of information between the MROS and a foreign FIU. Rather, it concerns the transmission of information originating from MROS to a foreign third authority via a reporting office abroad. This provision must therefore always be considered in conjunction with Art. 30 para. 4 AMLA.

B. Priority of Swiss criminal proceedings

47 The idea of the legislator in this paragraph was to give Swiss criminal proceedings **priority over** foreign ones, in order to prevent information forwarded by MROS to a foreign FIU and then forwarded to a third authority from affecting ongoing criminal proceedings in Switzerland. Such a situation is conceivable based on the legal principle of "ne bis in idem". If a foreign prosecuting authority were to receive significant information on a matter that is already the subject of criminal proceedings in Switzerland, and if the foreign prosecuting authority were to reach a conclusion of proceedings more quickly than the Swiss authorities, the work of the Swiss public prosecutor's office would, under certain circumstances, have been in vain due to the ne bis in idem principle. Another conceivable scenario in which Art. 30 para. 5 AMLA generally gives priority to Swiss criminal proceedings is where the criminal proceedings are not yet public and coercive measures are planned. Forwarding the information to a foreign third authority could lead to the suspect be-

coming aware of the Swiss criminal proceedings, which could adversely affect them.

If the competent Swiss public prosecutor does not authorize the disclosure of the information by the foreign FIU to a third authority in the same country because it fears the above-mentioned influence on its criminal proceedings, the Swiss reporting office may not grant permission to forward the information in its information letter to the foreign FIU. In this case, it attaches the disclaimer without permission to forward information to third authorities. 48

C. Sources of information

The information that criminal proceedings are pending in Switzerland against a natural or legal person mentioned in the information letter from MROS to a foreign FIU is communicated to the Swiss FIU either by the **decisions to open proceedings**, which it receives from Swiss public prosecutors, or through its access to various **judicial and police databases**. However, due to the fragmentation of the databases of the Swiss law enforcement agencies, it is questionable whether MROS is actually aware of every ongoing criminal proceeding in Switzerland. This problem is exacerbated by the fact that the prosecuting authorities in Switzerland often do not provide the reporting office with sufficient information about all pending proceedings related to Art. 260ter, Art. 260^{quinquies} para. 1, Art. 305bis and Art. 305ter para. 1 SCC, as they should according to Art. 29a para. 1 AMLA . 49

D. MROS practice

When MROS is aware of a criminal proceeding in Switzerland involving natural or legal persons who are the subject of a letter from MROS to a foreign FIU, it contacts the prosecutor in charge. This contact is most often made by telephone. The purpose of this contact is to find out whether the subject of the pending criminal proceedings is the **same subject** as the one that is the subject of a request for forwarding. Only in such a case does the Swiss public prosecutor have the authority to actually refuse permission to forward the information to foreign third-party authorities. 50

In practice, MROS also contacts the relevant Swiss public prosecutor to find out whether the foreign prosecuting authority that is to receive the information according to the foreign FIU has already received or will receive this in- 51

formation through the **judicial assistance process** (based on an existing request for judicial assistance from abroad or based on spontaneous judicial assistance from a Swiss public prosecutor (Art. 67a IMAC)). If this is the case, MROS generally refrains from transmitting the information for reasons of efficiency. In such a scenario, MROS informs the foreign reporting office that the law enforcement agency in the corresponding country has received or will receive the requested information directly.

VII. MEMORANDUM OF UNDERSTANDING (PARA. 6)

A. MROS's authority to conclude

52 Para. 6 of Art. 30 AMLA authorizes the Swiss reporting office to independently regulate the **modalities of cooperation** with foreign FIUs. In practice, this is a so-called Memorandum of Understanding (MoU, also known as a declaration of intent). Since Article 30 AMLA came into force, the head of MROS has signed such MoUs independently, whereas before November 1, 2013, a declaration of intent between the Swiss reporting office and a foreign FIU had to be approved by the Federal Council.

53 The Interpretative Note to FATF Recommendation 29 explicitly requires that FIUs have the authority to enter into MoUs **independently**: "The FIU should also be able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information."

B. Reasons for an MoU

54 There are various reasons why FIUs may wish to conclude MoUs with foreign partner authorities. These reasons can be divided into **two categories**:

(1) An FIU may need a memorandum of understanding with foreign partner authorities **by law**. Without such an agreement, the exchange of information is not possible;

(2) A FIU may need a memorandum of understanding with a foreign partner authority in order to exchange information by law. However, it would like to **specify the terms of** its cooperation with its counterparts. This can be done by resorting to a general MoU without specifically addressing the particulars of the exchange of information with the other FIU, or by specifying the

specifics arising from the cooperation with the foreign FIU in the memorandum of understanding (e.g. mentioning the fight against a specific predicate offense to money laundering).

C. MROS practice

MROS is in the comfortable position of being able to exchange a wide range of (financial) information, without the need for an MoU to govern the details of its cooperation with the foreign partner authority. In addition, the time required for MROS to conclude a memorandum of understanding should not be underestimated. Consequently, in practice the Swiss FIU mainly signs MoUs with foreign partner authorities that require such a **memorandum of understanding by law**. In such a case, a memorandum of understanding is also in the interests of MROS, as the foreign FIU cannot provide MROS with information without an MoU. 55

If a foreign FIU requests MROS to sign a memorandum of understanding, the Swiss reporting office first clarifies whether the foreign partner authority actually needs such a memorandum by law. MROS requests the relevant passage of law from the counterpart and decides whether the conditions required by the Swiss reporting office for the conclusion of an MoU are met. If the foreign FIU does not require such a declaration of intent by law, but would like to regulate cooperation in more detail, MROS clarifies whether this is also in its interest. In both cases, MROS reviews the memorandum of understanding proposed by the foreign FIU. In doing so, it ensures, above all, that the legal requirements (in particular Articles 30 and 31 AMLA) are met. Before the final signature by the head of the Swiss reporting office, MROS consults with the Federal Department of Foreign Affairs (FDFA) and the State Secretariat for International Finance (SIF). This ensures that the concluded MoUs are embedded in Switzerland's **foreign and foreign trade policy efforts**. 56

As of August 2024, MROS had signed MoUs with around **a dozen** foreign FIUs. 57

BIBLIOGRAPHY

Berger Corinne, Kommentierung zu Art. 30 GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Beuret Arnaud, Kommentierung zu Art. 30 GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar, Geldwäschereigesetz, Bern 2017.

MATERIALS

Botschaft zur Änderung des Geldwäschereigesetzes vom 27.6.2012, BBI 2012 S. 6941 ff., abrufbar unter https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2012/1031/de/pdf-a/fedlex-data-admin-ch-eli-fga-2012-1031-de-pdf-a.pdf, besucht am 1.8.2024 (zit. Botschaft GwG 2012).

Egmont Group of Financial Intelligence Units, Egmont Group of Financial Intelligence Units Charter, Juli 2013, https://egmontgroup.org/wp-content/uploads/2021/09/Egmont-Group-Charter-Revised-July-2023-Abu-Dhabi-UAE.pdf, besucht am 1.8.2024.

Egmont Group of Financial Intelligence Units, Principles for Information Exchange between Financial Intelligence Units, Oktober 2013, https://egmontgroup.org/wp-content/uploads/2022/07/2.-Principles-Information-Exchange-With-Glossary_April2023.pdf, besucht am 1.8.2024.

Egmont Group of Financial Intelligence Units, Annual Report 2020/2021, 2022, https://egmontgroup.org/wp-content/uploads/2022/10/EGMONT_21-267_2020%E2%80%932021_AR-E_WEB.pdf, besucht am 1.8.2024.

Financial Action Task Force (FATF), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, 2012, FATF Recommendations 2012.pdf.coredownload.inline.pdf (fatf-gafi.org), besucht am 1.8.2024.

Meldestelle für Geldwäscherei (MROS), Jahresbericht 2020, Mai 2021, https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/publikationen.html, besucht am 1.8.2024.

Meldestelle für Geldwäscherei (MROS), Jahresbericht 2022, Mai 2023, https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/publikationen.html, besucht am 1.8.2024.

Meldestelle für Geldwäscherei (MROS), Jahresbericht 2023, Mai 2024, https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/publikationen.html, besucht am 1.8.2024.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 31 AMLA

A commentary by Nathalie Kläy / Simon Zaugg

SUGGESTED CITATION

Nathalie Kläy/Simon Zaugg, Commentary of art. 31 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Kläy/Zaugg, art. 31 AMLA N. XXX.

Art. 31 Refusal to provide information

A request for information from a foreign reporting office shall not be granted if:

a. the request has no connection with Switzerland;

b. the request requires the application of procedural compulsion or other measures or acts for which Swiss law stipulates mutual assistance procedures or another procedure regulated in special legislation or an international treaty;

c. national interests or public security and order will be prejudiced.

CONTENT

I. General 595
II. Lack of connection to Switzerland (let. a) 596
A. MROS practice 596
B. MROS procedure for Art. 11a para. 2bis AMLA 596
III. Prohibition on circumventing international mutual assistance (lit. b) 597
A. For information purposes only 597
B. MROS practice 597
IV. Adverse effect on national interests or public security and order (lit. c) 598
A. Adverse effect on national interests 598
B. Adverse effects on public security and order 598
Bibliography 599
Materials 599

I. GENERAL

Art. 31 AMLA sets out the reasons for MROS to **refuse to provide information** in response to a request from a foreign FIU. This article was created as part of the partial revision of the AMLA and came into force on November 1, 2013. If one of the compelling reasons for refusal listed in this article applies, MROS may not provide information to a foreign FIU. This provision makes it clear that requests from partner FIUs that have no specific connection to Switzerland (so-called fishing expeditions), are aimed at circumventing mutual legal assistance or affect Switzerland's national interests or public security and order, will not be answered in terms of content. In order to refuse to provide information to a foreign FIU, the request must constitute a "serious abuse of the administrative assistance process". Each request for information from a foreign FIU is examined by MROS upon receipt from these points of view (case-by-case examination). The Swiss reporting office decides independently on the existence of one of these grounds for refusal, and no legal remedy can be taken against this decision. As already mentioned, the refusal to provide information must be a "serious abuse of administrative assistance". In less serious or unintentional cases (e.g. the foreign FIU simply forgot to mention the connection to Switzerland), MROS can allow the partner authority to amend its request. 1

The mandatory grounds for refusal listed in Article 31 AMLA are **national requirements** that restrict the international exchange of information with partner FIUs to a certain extent or subject it to national barriers. However, these national requirements also correspond to international guidelines issued by the Financial Action Task Force (FATF, also known by its French name Groupe d'Action Financière, or GAFI for short) and the Egmont Group. Art. 31 AMLA is modeled on Art. 2 para. 2 and Art. 12 para. 2 SIaG, whereby international mutual assistance is subject to Art. 1a and 2 IMAC, which contain provisions similar to Art. 31 let. a and c AMLA. 2

II. LACK OF CONNECTION TO SWITZERLAND (LET. A)

A. MROS practice

3 The reason for refusal mentioned in a, the lack of connection to Switzerland, is the one most frequently encountered in practice. A connection to Switzerland exists as soon as an involved natural person is a Swiss citizen, a natural or legal person is domiciled in Switzerland, details of a business relationship in Switzerland (IBAN or name of the account-holding financial intermediary incl. contracting party/account number) are given, or police findings indicate links to Switzerland. It is sufficient if one of these conditions is met. If none of these conditions is met, it is considered a **fishing expedition**, which violates Switzerland's territorial principle and is therefore prohibited. In its principles for cooperation between FIUs, the Egmont Group also requires that requests for information must have a connection to the respective country and must be sufficiently substantiated in this regard.

B. MROS procedure for Art. 11a para. 2bis AMLA

4 It is the responsibility of the requesting FIU to show the connection to Switzerland in the request, although the FIU cannot be required to present the facts completely and consistently. Cases in which there is a connection to Switzerland arise primarily in connection with the gathering of information from financial intermediaries in accordance with Art. 11a para. 2bis AMLA. For the Swiss reporting office, there is a **sufficient connection to Switzerland** if the owner of the business relationship and the account-holding Swiss financial intermediary are explicitly named by the foreign FIU, even if no more precise information about the business relationship (e.g. account number) is available. This procedure is important for efficient cooperation, since a foreign FIU – and thus also MROS – often only knows that a business relationship exists between a subject and a Swiss financial intermediary, without having more precise information such as account numbers or transactions. If, on the other hand, the partner FIU merely suspects the existence of a business relationship in Switzerland without mentioning a specific financial intermediary, MROS categorizes the request as a fishing expedition and asks the requesting FIU to specify the Swiss connection (e.g. Swiss IBAN or Swiss financial intermediary) or, if no further information is provided by the foreign FIU, not to respond to the content replied to.

III. PROHIBITION ON CIRCUMVENTING INTERNATIONAL MUTUAL ASSISTANCE (LIT. B)

A. For information purposes only

Lit. b, in addition to Art. 30 para. 1 lit. d and Art. 30 para. 4 lit. c AMLA, primarily enshrines the requirement that the exchange of information between FIUs must never circumvent **international mutual assistance**. International information sharing always takes place at the analysis stage and the information obtained is for information purposes only – never as evidence. If a foreign FIU attempts to obtain information through administrative assistance that, under Swiss law, may only be obtained through the use of coercive measures ordered by a judge, MROS must refuse to provide the information. The term "coercive measures" refers to the coercive measures under Swiss police and criminal procedural law (in particular the measures under the fifth title of the Swiss Criminal Procedure Code) and the coercive police measures under the respective cantonal police laws. The extension mentioned in b) to other proceedings regulated by special laws or international treaties is explained by the fact that the use of procedural coercion can also occur in certain administrative assistance agreements and this may not be circumvented either. 5

B. MROS practice

In addition to the type of use of the information (information for information purposes via the FIU channel and evidence via the mutual assistance channel), MROS must also clarify whether the requesting state has already submitted a mutual assistance request for the same facts or the same information and whether the Swiss authority responsible for mutual assistance has already responded or will respond to it. If this is the case, MROS refers the matter to the legal assistance channel and, for reasons of efficiency, does not respond to the request. If the request for legal assistance has been rejected by the competent Swiss authority, MROS must find out the reasons for this. If the request for legal assistance was simply not sufficiently substantiated, MROS provides the requested information via the FIU channel to enable the requesting state to complete the request. One of the main objectives of the exchange of information between FIUs is to **enable international legal assistance**. If the request for mutual assistance has been rejected for other reasons, in particular in connection with one of the grounds for refusal listed in Art. 2 IMAC, the Swiss re- 6

porting office will carefully check whether it is allowed to exchange information via the FIU channel based on Art. 31 AMLA.

IV. ADVERSE EFFECT ON NATIONAL INTERESTS OR PUBLIC SECURITY AND ORDER (LIT. C)

7 In c), the **impairment of** national interests or public security and order is stated as a ground for refusal. This ground for refusal was not originally provided for by the Federal Council, but was added by Parliament. This also explains why the dispatch on the 2012 amendment to the Anti-Money Laundering Act does not comment on c).

A. Adverse effect on national interests

8 MROS bases its application of lit. c on its long-standing internal practice, since it applied the ground for refusal of adverse effect on national interests under the then-current version of Art. 26 of the Money Laundering Act. Many possible scenarios are conceivable under the **impairment of national interests**, but in practice the prohibition of information to a home or country of origin of persons who have applied for asylum in Switzerland or are to be qualified as recognized refugees or persons in need of protection, as laid down in Art. 26 para. 1 MGwV, is of relevance. In addition, requests from foreign FIUs will also be rejected if the requested information could endanger the life or physical integrity of a person.

B. Adverse effects on public security and order

9 The term "public security" is a fundamental concept of police law. It refers to the protection of the inviolability of the objective legal system, the legal interests of individuals and state institutions. The term "public order" (ordre public) refers to "the fundamental principles of the values of a state" and thus the basic principles of the Swiss legal system. MROS examines requests for information from foreign FIUs in accordance with the principles set out in Art. 2 IMAC. For example, no information will be provided to a foreign FIU if it could lead to the **death penalty or torture** of a person concerned. Similarly, no information will be provided if the request is **politically motivated**. In practice, however, this is not always easy to determine and requires the Swiss reporting office to have a solid knowledge of the domestic affairs of the re-

questing state (e.g. its political system, institutions, the independence and impartiality of its judiciary, and respect for fundamental rights).

BIBLIOGRAPHY

Beuret Arnaud, Kommentierung zu Art. 31 GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar, Geldwäschereigesetz (GwG), Bern 2017.

Naegeli Vera, Kommentierung zu Art. 31 GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Ordolli Stiliano, Le Bureau de communication en matière de blanchiment d'argent: évolution récente et perspectives, in: Augsburger-Bucheli Isabelle (Hrsg.), Blanchiment d'argent : actualité et perspectives suisses et internationales, 2014, S. 45–80.

Thelesklaf Daniel/Ordolli Stiliano, Kommentierung zu Art. 31 GwG, in: Orell Füssli Kommentar, GwG Kommentar, 3. Aufl., Zürich 2019.

MATERIALS

Botschaft zur Änderung des Geldwäschereigesetzes vom 27.6.2012, BBI 2012 6941 ff., abrufbar unter https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2012/1031/de/pdf-a/fedlex-data-admin-ch-eli-fga-2012-1031-de-pdf-a.pdf, besucht am 1.8.2024.

Meldestelle für Geldwäscherei (MROS), Jahresbericht 2017, April 2018, https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/publikationen.html, besucht am 1.8.2024.

Meldestelle für Geldwäscherei (MROS), Jahresbericht 2023, Mai 2024, https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/publikationen.html, besucht am 1.8.2024.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 31a AMLA

A commentary by Nathalie Kläy / Simon Zaugg

SUGGESTED CITATION

Nathalie Kläy/Simon Zaugg, Commentary of art. 31a AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Kläy/Zaugg, art. 31a AMLA N. XXX.

Art. 31*a* Applicable provisions of the Federal Act of 7 October 1994 on Central Offices of the Federal Criminal Police

Unless this Act provides otherwise in relation to data processing and administrative assistance provided by the Reporting Office, the first and fourth sections of the Federal Act of 7 October 1994 on the Central Offices of the Federal Criminal Police apply by analogy.

CONTENT

I. Reference to the ZentG 603
II. Purpose and significance of the standard 603
Bibliography 604
Materialienverzeichnis 604

I. REFERENCE TO THE ZENTG

Art. 31a AMLA was created in the course of the 2012 revision of the AMLA and entered into force on November 1, 2013. It refers to the **first section** (General Provisions) and **fourth section** (Processing of Personal Data) of the Federal Act on the Criminal Police Central Offices of the Confederation and Joint Police and Customs Cooperation Centers with Other States (ZentG). This name of the law, which has been in force since August 1, 2014, has not yet been adapted in the Money Laundering Act – it still refers to the Federal Act on the Central Offices of the Federal Criminal Police. 1

II. PURPOSE AND SIGNIFICANCE OF THE STANDARD

With Art. 31a AMLA, the legislator wanted to ensure that MROS, firstly, does not lose **existing information gathering opportunities** (reference to the first section of the ZentG) and, secondly, based on Art. 13 ZentG in conjunction with Art. 12 of the Federal Act on the Prevention of Money Laundering in the Financial Sector), MROS can forward the information it has to the Federal Criminal Police for in-depth analysis by means of spontaneous administrative assistance (reference to the fourth section of the ZentG). 2

Regarding MROS's **national administrative assistance**, the reasons stated in the dispatch on the amendment of the Anti-Money Laundering Act of June 27, 2012, regarding the gathering of information (active administrative assistance) and forwarding of information to the Federal Criminal Police (passive administrative assistance) no longer apply. In its current practice, the Swiss reporting office bases its cooperation with domestic authorities on Art. 29, para. 2–2ter AMLA. Since Article 31a AMLA gives precedence to the Anti-Money Laundering Act, Article 31a AMLA is no longer relevant for MROS's national cooperation with other authorities. The reference to Section 4 of the ZENTG, which consists exclusively of Article 13 (forwarding of personal data), is no longer applicable. 3

According to the message on the amendment of the Anti-Money Laundering Act of June 27, 2012, the **reference to the first section** is necessary so that the Swiss reporting office does not lose existing information-gathering opportunities that arise from laws other than the Anti-Money Laundering Act, al- 4

though these laws are not mentioned by name. This could refer to those laws that give MROS access to the databases it requires.

BIBLIOGRAPHY

Beuret Arnaud, Kommentierung zu Art. 31a GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar, Geldwäschereigesetz (GwG), Bern 2017.

MATERIALIENVERZEICHNIS

Botschaft zur Änderung des Geldwäschereigesetzes vom 27.6.2012, BBI 2012 6941 ff., abrufbar unter https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2012/1031/de/pdf-a/fedlex-data-admin-ch-eli-fga-2012-1031-de-pdf-a.pdf, besucht am 1.8.2024.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 32 AMLA

A commentary by Nathalie Kläy / Simon Zaugg

SUGGESTED CITATION

Nathalie Kläy/Simon Zaugg, Commentary of art. 32 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Kläy/Zaugg, art. 32 AMLA N. XXX.

Art. 32 Cooperation with foreign prosecution authorities

[1] The cooperation of the Reporting Office with foreign prosecution authorities is governed by Article 13 paragraph 2 of the Federal Act of 7 October 1994 on the Central Offices of the Federal Criminal Police.

[2] ...

[3] The name of the person who made the report on behalf of the financial intermediary or the dealer or who complied with the duty to provide information under Article 11*a* may not be passed on by the Reporting Office to foreign prosecution authorities.

CONTENT

I. General 607
II. Cooperation with foreign law enforcement authorities (para. 1) 607
A. Exchange of personal data 607
B. Different from mutual assistance 608
C. Significance of the standard 608
III. Prohibition on disclosing the name of the reporting person (para. 3) 609
Bibliography 609
Materialis 610

I. GENERAL

Article 32 AMLA governs the cooperation of MROS with **foreign law enforcement authorities** and refers to the Federal Act on the Central Offices of the Federal Criminal Police and on Joint Police and Customs Cooperation Centers with Other States (CentG). Similarly to Art. 31a AMLA, the outdated terminology of the ZentG is also used in Art. 32 AMLA, although Art. 32 AMLA already existed before the Swiss reporting office was legally authorized to exchange financial information with foreign partner authorities. In fact, Art. 32 para. 1 AMLA has remained unchanged since the Anti-Money Laundering Act came into force on April 1, 1998. The fact that the then newly introduced Art. 30 and Art. 31 AMLA regulated the exchange of information between MROS and foreign reporting offices in a new and more precise way made Art. 32 para. 2 AMLA obsolete and repealed it with effect from November 1, 2013. Para. 3, on the other hand, came into force on February 1, 2009 and reflects the implementation of the then revised recommendations of the Financial Action Task Force (FATF, also known by its French name Groupe d'Action Financière, or GAFI for short). 1

II. COOPERATION WITH FOREIGN LAW ENFORCEMENT AUTHORITIES (PARA. 1)

A. Exchange of personal data

With regard to cooperation with foreign law enforcement authorities, para. 1 refers to Art. 13, para. 2, ZentG. Art. 13, para. 2, ZentG specifies that this cooperation involves the "disclosure of personal data". Consequently, cooperation between MROS and foreign law enforcement authorities is limited to the exchange of **personal data**. Financial information is not exchanged by MROS in this way. In terms of cooperation with foreign countries, this information should only be transmitted to the FIUs. As stated in Art. 13 para. 2 ZentG, cooperation with foreign law enforcement authorities is governed by Art. 349*a*–349*h* SCC, which came into force on March 1, 2019. Art. 349*a* et seq. SCC were introduced in the course of the implementation of Directive (EU) 2016/680 of April 27, 2016, on the protection of natural persons with regard to the processing of personal data. Consequently, the reference in Art. 13 para. 2 of the ZentG to the aforementioned articles in the SCC has only been in force 2

since March 1, 2019. Before that date, the conditions that had to be met for the disclosure of personal data were listed in Art. 13 para. 2 of the ZentG itself. Art. 349*a* et seq. SCC govern police assistance in general and lay down the broad criteria that must be observed for all forms of police assistance.

3 In addition to the SCC articles mentioned, Art. 13 of the Money Laundering Act (MLA) governs the transmission of personal data by MROS to foreign law enforcement authorities. This article sets out the **specific conditions** for the transmission of personal data by MROS to foreign law enforcement authorities. Art. 13 para. 1 MGwV states that for this specific form of information exchange, there must be a suspicion of money laundering, its predicate offences, organized crime or terrorist financing. In addition, personal data may only be exchanged by MROS with foreign law enforcement authorities if (alternatively):

- it is necessary for MROS to obtain the information required (Art. 13 para. 2 let. a MLO);
- the data is not related to international mutual assistance (Art. 13 para. 2 let. b MLO);
- the request for administrative assistance is justified (Art. 13 para. 2 let. c MLO).

B. Different from mutual assistance

4 As with Art. 30 AMLA, the exchange of information under Art. 32 AMLA serves to **prevent and analyse** money laundering, its predicate offences, organised crime and terrorist financing. It is essential that the personal data exchanged between MROS and the foreign law enforcement authorities are not subject to international mutual assistance. International mutual assistance must therefore not be circumvented in this constellation (FIU-law enforcement agency), in the same way as the international exchange of information between reporting offices (FIU-FIU). Precisely because the partner authorities in this context are law enforcement authorities, particular attention must be paid to this circumstance.

C. Significance of the standard

5 In practice, Art. 32 AMLA is of little significance. The focus of the cooperation between MROS and foreign partner FIUs is on the **exchange of financial in-**

formation. In this regard, Art. 30 f. AMLA is applied. The Egmont Group, with its network of now over 170 FIUs attached to the "Egmont Secure Web" communication channel, is of great relevance in this context. A certain level of trust exists between the member FIUs, which makes the international exchange of information between reporting offices easier. Direct contact with a law enforcement agency abroad would be conceivable if a particular FIU failed to respond to a request for information from MROS, if it has no access to police information or is unable to obtain it, or if there are concerns about the independence of the foreign FIU in connection with a specific case.

III. PROHIBITION ON DISCLOSING THE NAME OF THE REPORTING PERSON (PARA. 3)

Para. 3 stipulates that the Swiss reporting office may not disclose the **name of the person** who submitted the suspicious activity report to the financial intermediary or dealer or who fulfilled the duty to provide information in accordance with Art. 11a AMLA to foreign law enforcement authorities. This paragraph came into force on February 1, 2009 and reflects the implementation of the then revised FATF recommendations. Since its introduction, para. 3 has been substantively amended twice. On November 1, 2013, it was expanded due to the introduction of Art. 11a AMLA. On the other hand, the prohibition on transmitting the name of the financial intermediary was removed, as permission for MROS to pass on the name of the financial intermediary to foreign FIUs was simultaneously included in the law under Art. 30 para. 2 let. a AMLA. The second substantive amendment came into force on January 1, 2016, with the addition of the dealers newly subordinated to the AMLA at that time. 6

Art. 32 para. 3 AMLA is intended to protect employees of reporting financial intermediaries or dealers from **possible reprisals** due to a report or information provided. For a detailed discussion of this topic, please refer to the comments in Chapter III.B. in OK-Kläy/Zaugg, Art. 30 AMLA. 7

BIBLIOGRAPHY

Beuret Arnaud, Kommentierung zu Art. 32 GwG, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar, Geldwäschereigesetz (GwG), Bern 2017.

Mráz Michael, Kommentierung zu Art. 32 GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Thelesklaf Daniel/Ordolli Stiliano, Kommentierung zu Art. 32 GwG, in: Orell Füssli Kommentar, GwG Kommentar, 3. Aufl., Zürich 2019.

MATERIALIS

Botschaft zur Änderung des Geldwäschereigesetzes vom 27.6.2012, BBI 2012 6941 ff., abrufbar unter https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2012/1031/de/pdf-a/fedlex-data-admin-ch-eli-fga-2012-1031-de-pdf-a.pdf, besucht am 1.8.2024.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 33 AMLA

A commentary by Emmanuel Goldberg / Dominic Robert

SUGGESTED CITATION

Emmanuel Goldberg/Dominic Robert, Commentary of art. 33 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Goldberg/Robert, art. 33 AMLA N. XXX.

Chapter 5 Processing of Personal Data

Art. 33 Principle

The processing of personal data is governed by the Data Protection Act of 25 September 2020.

CONTENT

I. Introduction 613
II. Differences in Application 613
A. Private Individuals 614
1. Financial Intermediaries and Traders 614
2. Self-Regulatory Organizations 614
B. Federal Bodies 616
III. Types of Data Concerned 617
A. Personal Data 617
B. Sensitive Personal Data 618
C. Profiling / High-Risk Profiling 619
IV. Data Protection Principles for Processing 622
Bibliography 623
Materials 625

I. INTRODUCTION

The FADP and the AMLA are based on different guiding principles. On the one hand, there is the AMLA, which aims to prevent the misuse of the financial center for criminal activities (Art. 1 AMLA). To achieve this purpose, the processing—i.e., the collection and management—of personal data is required to a considerable extent. In contrast, data protection law pursues a different goal: It aims to protect the privacy and fundamental rights of individuals whose data is processed by private entities or federal authorities, and ensures that they retain control over their personal data. The comprehensive reference to the FADP in Art. 33 AMLA is **purely declaratory in nature**. Even without it, the FADP would apply without restriction. Accordingly, all information collected by financial institutions within the framework of the legal requirements of the AMLA is fully covered by the scope of the FADP. The reference also clarifies that the relevant provisions of the AMLA are not to be understood as a special regime that would supersede the scope of the FADP. 1

II. DIFFERENCES IN APPLICATION

The comprehensive processing of personal data extends across all levels of the institutions involved. First, financial intermediaries are obligated to collect and document certain customer data (e.g., the identity of the contracting party and beneficial owner, or special investigations in cases of suspected money laundering). Furthermore, the competent supervisory authorities (e.g., self-regulatory organizations) even assume a **dual role**: On the one hand, they have access to the information processed by financial intermediaries; on the other hand, they themselves process personal data regarding the financial intermediaries and their employees. Finally, selected data collected by both financial intermediaries and supervisory authorities is forwarded to the Money Laundering Reporting Office (MROS). The MROS then transmits the relevant information to the competent law enforcement authorities. In implementing this aspect, the Anti-Money Laundering Act distinguishes between financial intermediaries (private entities), to whom Art. 34 AMLA applies, and the MROS (a federal body), to which Art. 35 et seq. AMLA apply. 2

A. Private Individuals

1. Financial Intermediaries and Traders

3 Financial intermediaries and traders are classified as **private individuals** within the meaning of Art. 2 para. 1 lit. a FADP. The processing of personal data by them is generally permissible, provided that no applicable legal norms are violated. They are therefore subject to both the general provisions of Art. 1–29 FADP and the special provisions on data processing by private individuals pursuant to Art. 30–32 FADP.

2. Self-Regulatory Organizations

4 In addition to financial intermediaries, the Message on the Anti-Money Laundering Act (AMLA) also designated self-regulatory organizations (SROs) **as private individuals within the meaning of the FADP**. This classification under data protection law has caused uncertainty in legal scholarship: SROs are subject—despite their organization under private law as an association (Art. 60 et seq. CC)—to the supervision of FINMA (Art. 18 AMLA), which in turn is a federal body.

5 The primary purpose of an SRO is to **ensure compliance with the AMLA due diligence obligations** (public law) by its member financial intermediaries. In addition to the tasks listed in Art. 24 AMLA, SROs also act as industry representatives, which falls within the scope of private law.

6 If an SRO sanctions an affiliated financial intermediary for a violation, the sanction is, according to legal doctrine, case law, and the legislature, of a private-law nature (i.e., a contractual penalty within the meaning of para. 1 of Art. 160 of the CO or a measure under association law). However, even with this line of reasoning, it must be taken into account that the relationship between SROs and their affiliated financial intermediaries tends to be classified as **public law**—not least due to the introduction of the supervisory organization pursuant to Art. 43a FINMASA. Despite the explicit classification of the sanction mechanism of the SRO PolyReg as private law in the judgment 2C_887/2017 of March 23, 2021, the Federal Supreme Court simultaneously pointed to the growing trend of self-regulation under purely private law evolving into a public function. In the Federal Supreme Court's view, this leaves open the possibility of classifying money laundering fines as falling un-

der public law. At the same time, the Federal Supreme Court considered classifying the sanctions as falling under public law to be questionable, insofar as a formal legal basis for this might not be sufficient.

From a data protection perspective, the legal nature of the relationship between the data controller and the data subject plays a decisive role: if the relationship is governed by public law, the data controller must be classified as a public body. Compliance with AMLA regulations constitutes a public task of the Confederation, which is why classifying the SRO as a federal body (Art. 5(i) FADP) and applying stricter data protection provisions (Art. 33 et seq. FADP) would certainly be conceivable. Other legal opinions leave this question open. However, other activities of SROs would fall under the rules governing data processing by private entities. Furthermore, the primary task of an SRO **is not data processing on behalf of the federal government**. In our view, it is therefore correct to subject the legal relationship between the SROs and those individuals whose data is processed by affiliated financial intermediaries to the data protection provisions applicable to private individuals. If a data subject wishes to assert a legal claim against an SRO, they must consequently pursue civil remedies (Art. 32 FADP). 7

The opinion expressed here aligns with that of the Message on the Anti-Money Laundering Act (AMLA). While there are clear overlaps between private and public law, it must nevertheless be noted that private law continues to form the **core of the legal classification** of SROs. This also applies in light of the developments described above and the associated discussions regarding a possible classification of individual aspects under public law. A deviating classification under public law would be justified if this were enshrined in law. This is reinforced by the Message on the AMLA, which states that SROs and supervisory organizations are not actual authorities of the Confederation, the cantons, or the municipalities within the meaning of Art. 29 para. 2 AMLA. Recognized SROs within the meaning of Art. 24 AMLA are organizations that have been entrusted by the legislature with regulatory and supervisory duties for affiliated financial intermediaries. These organizations are agents performing a sovereign function. An argument to the contrary would unnecessarily undermine the Swiss self-regulation system, which also complies with international standards. 8

To conclusively clarify their legal nature, the legislature designated self-regulatory organizations as **associations under private law** to which a public- 9

law function has been entrusted. Consequently, SROs exercise supervision over their affiliated persons and may also impose sanctions in the event of a breach of due diligence obligations. On September 26, 2025, the Federal Assembly decided to expressly subject the legal relationship between SROs and their members to the provisions of private law in Art. 24b of the New Money Laundering Act (nGwG), whereby the liability of SROs, their bodies, and their staff is governed accordingly.

B. Federal Bodies

10 Federal bodies within the meaning of Art. 5(i) of the FADP are subject to both the general data protection provisions of Art. 1–29 FADP and the special provisions of Art. 33–42 FADP. The distinction between private individuals and federal bodies is significant in that the principles enshrined in Art. 6 FADP are **interpreted and applied differently**. While, for example, a private individual complies with the principle of lawfulness under Art. 6 para. 1 FADP simply by ensuring that their data processing does not violate any applicable legal norms, the actions of a federal body must be based on a formal legal basis (Art. 34 para. 1 FADP). The principle of legality illustrates, for example, that the actions of federal bodies must always be based on a legal foundation.

11 According to Art. 5(i) FADP, federal authorities and agencies, as well as individuals to the extent that they are **entrusted with public tasks of the Confederation**, fall under the definition of federal bodies; these include FINMA, the Office of the Attorney General of Switzerland, the Federal Gaming Board (ESBK), and MROS. The latter is affiliated with the Federal Office of Police (fedpol) pursuant to Art. 23 para. 1 AMLA, which in turn is an administrative central office for combating organized and internationally active crime within the meaning of the Federal Act on Federal Criminal Police Central Offices and Joint Centers for Police and Customs Cooperation with Other States (ZentG).

12 The cantonal law enforcement authorities are not subject to the FADP, as they are cantonal bodies rather than federal ones. From the time criminal proceedings are initiated until their conclusion, the provisions of the Swiss CrimPC (Art. 95 et seq. CrimPC) apply pursuant to Art. 2 para. 3 FADP. This applies both to data processing by the court in the context of the proceedings and to that of the other parties to the proceedings, namely the parties. **Upon conclusion of the proceedings**, the CrimPC again declares the FADP appli-

cable (Art. 99 CrimPC). From this point on, the processing of personal data is thus once again governed by the provisions of the FADP.

III. TYPES OF DATA CONCERNED

The fulfillment of due diligence obligations by financial intermediaries necessarily involves the processing of personal data. This refers to "all information relating to an identified or identifiable natural person" (Art. 5(a) FADP). The term is deliberately very broad and encompasses any information containing **information content** that relates to or can be linked to one or more natural persons. A subcategory of personal data consists of sensitive personal data. Also worth mentioning in connection with the due diligence obligations of financial intermediaries is profiling, both high-risk and non-high-risk. 13

With these types of data, **different levels of protection** must always be assumed: they range from publicly available data through various categories of ordinary personal data to sensitive personal data. These gradations shape the risk assessment and determine both the required level of data security and the scope of the duty to provide information. While the processing of ordinary personal data generally poses no difficulties, stricter requirements apply to personal data requiring special protection, as explained in more detail below. Special rules also apply to profiling, which will be discussed subsequently. 14

A. Personal Data

For data to qualify as personal data, the data subject must be **identified or at least identifiable**. It does not matter whether the person is clearly identified or merely identifiable. 15

Among the most fundamental due diligence obligations of a financial intermediary are the identification of the contracting party (Art. 3 AMLA), the determination of the beneficial owner (Art. 4 AMLA), and the fulfillment of other special due diligence obligations (Art. 6 AMLA). The information collected in this context (such as name, address, and contractual or financial information) constitutes personal data within the meaning of Art. 5(a) of the FADP. It is subject to the documentation requirement under Art. 7 of the AMLA. 16

B. Sensitive Personal Data

17 Sensitive personal data constitutes a subcategory of personal data. This exhaustive list provided by law includes, among other things, health data, biometric data, or data regarding administrative and criminal proceedings or sanctions (Art. 5(c) FADP). Data subject to special protection are those whose processing is subject to stricter legal requirements in some respects compared to ordinary personal data. This classification is based on the fact that, according to the legislature's intent, these categories of data "affect the personality of the data subjects so significantly" that their processing is in every case considered an **infringement of personality**.

18 Personal data collected by financial intermediaries in fulfillment of their reporting obligation or reporting right may be regarded as **particularly sensitive**. Special data protection provisions have been enacted for personal data requiring special protection within the meaning of Art. 5(c) FADP, both for financial intermediaries (Art. 34 AMLA) and for MROS (Art. 35 AMLA).

19 Depending on the risk, a transaction or business relationship must be subject to **more extensive or detailed** due diligence (Art. 6 AMLA). Examples of data requiring special protection—which are collected as part of the special due diligence—include possible criminal proceedings against a client, political views, and the role of a politically exposed person (PEP).

20 In this context, the proportionality of data processing under data protection law must be examined, for example, if the special investigations have led to the refutation of an initial suspicion. The personal data collected would thus have fulfilled its purpose and would have to be deleted in accordance with para. 6(4) of the FADP, whereby the reason for deletion would have to be recorded in a file note. However, processing and retaining this data appears proportionate and appropriate. This is for the following reason: In everyday practice, anti-money laundering units process systemically generated hits from their monitoring software (e.g., Compliance Suite) for both new applications and existing customers. Although these hits are predominantly so-called false positives (no actual match), a comparison must nevertheless be made between the generated hit and the customer based on the personal data already collected about them (Art. 5(a) FADP). Personal data is also collected through investigations into both the customer and the match—which does not necessarily have to be an existing customer of the financial intermediary in ques-

tion. This data, in turn, serves as evidence that a verification has taken place and identifies the specific characteristics based on which the match corresponds to or does not correspond with the respective customer. The purpose served by this personal data appears significantly more generic in this case, namely compliance with the financial intermediary's due diligence obligations, and not (merely) to dispel an initial suspicion or to forward a suspicious activity report to MROS. The financial intermediary's due diligence obligations under anti-money laundering law also include the documentation of the clarifications carried out (Art. 7 AMLA). The personal data collected in this context therefore also serves to provide a verifiable account that the statutory due diligence obligations have been fulfilled. In our view, the documentation of the due diligence measures taken can be understood as an **independent processing purpose** within the meaning of Art. 6 FADP. This applies in particular with regard to the audit activities of internal and external auditors, as well as potential administrative or criminal proceedings in which the financial intermediary must be able to demonstrate in a verifiable manner why no reportable circumstances were assumed and why the due diligence obligations were complied with. It therefore appears proportionate and appropriate not to delete this data immediately for evidentiary purposes, but to continue storing it.

C. Profiling / High-Risk Profiling

Profiling is a specific type of processing of personal data. It refers to the automated process in which a person's personal characteristics are analyzed and evaluated. An evaluation occurs as soon as the available data is interpreted, thereby resulting in a subjective assessment. In contrast, a mere statement of facts—that is, an objective recording of actual circumstances—does not constitute profiling. "Automated" describes a processing operation using technical means. The evaluation process is **fully automated**. So-called high-risk profiling is a specific form of profiling. It is characterized by the linking of data, thereby processing essential aspects of a natural person's personality. This poses a high risk to the personality or fundamental rights of the data subject. 21

Compliance with the due diligence obligations under Art. 6 AMLA may, under data protection law, require or entail so-called "profiling." Profiling is defined as the evaluation of certain personal aspects of an individual based on automatically processed personal data. These are consequently evaluated auto- 22

matically in order to draw conclusions—also automatically—about characteristics of an individual. High-risk profiling occurs when the **automated linking of data** enables the assessment of essential aspects of a natural person's personality, ultimately resulting in a personality profile. The mere collection of personal data within the framework of KYC does not in itself constitute profiling.

23 Profiling occurs, for example, when a business relationship is assigned a money laundering risk. In fulfilling the second partial obligation of Art. 6 AMLA, the so-called "filtering," the financial intermediary establishes criteria that distinguish between transactions that are either typical or atypical for the business relationship in question—in other words, those requiring further clarification. For private individuals, there are generally **no specific additional legal consequences** as in the public sector, subject to the corresponding transparency and information obligations (Art. 6 para. 3 in conjunction with Art. 19 of the FADP). It should be noted that the identification of criminal structures or patterns in connection with money laundering and terrorist financing constitutes a consistent element of the global defense mechanism against money laundering.

24 A more sensitive form is "high-risk profiling" (Art. 5(g) FADP). The high risk does not refer to the money laundering risk of a business relationship, but to the risk that the collected data will be used to analyze or even predict certain personal aspects of a customer (personality profile). Such profiling exists only if two additional conditions are met: First, different data must be linked together; second, the insights gained from this must relate to **essential aspects of personality** or at least be directed toward them. If both elements are present, the high risk is conceptually deemed to exist.

25 In the context of due diligence obligations under money laundering law, it is occasionally assumed that transaction monitoring in particular could fulfill this requirement. While it cannot be ruled out that the analysis of transaction data constitutes profiling within the meaning of Art. 5(f) FADP, Art. 5(g) FADP requires, for high-risk profiling, an additional linking of data that allows for an assessment of essential aspects of a person's character and can be consolidated into a comprehensive customer profile. By contrast, the due diligence obligations under Art. 6 AMLA pursue a **functionally limited purpose**, namely the identification of the nature and purpose of the business relationship as well as the investigation of unusual or high-risk transactions. Even though var-

ious pieces of information regarding the business relationship are taken into account here, the analysis focuses primarily on the plausibility of transactions and the identification of atypical transaction patterns in payment transactions. While the resulting data sets may be extensive, what is decisive is not the volume of data processed, but whether this data can be consolidated into a profile of the data subject's personality. This is generally not associated with the cross-domain linking of data with the aim of creating a comprehensive profile of the data subject's personality. By way of comparison, high-risk profiling occurs, for example, when data from different areas of life—such as consumption, location, online, or health data—are linked together to form a comprehensive profile of the data subject's personality. Whether such a profile exists must ultimately be assessed on a case-by-case basis.

Finally, it should be noted that in the case of high-risk profiling, there may be 26
an obligation to conduct a data protection impact assessment (DPIA) (Art. 22 FADP). A DPIA serves as a **self-assessment** of processing operations that appear sensitive from a data protection perspective. In this process, the planned project is first described from the perspective of data processing. It then describes the potential adverse consequences that this processing could have for the data subjects with a certain degree of probability. Based on these findings, the technical and organizational measures already implemented as well as those still planned are then outlined, which are intended to prevent or at least mitigate such negative effects.

For financial intermediaries, a DPIA is particularly relevant when they use au- 27
tomated procedures—including AI-based systems—in connection with compliance with anti-money laundering due diligence obligations that analyze or predict personal aspects based on customer data. In such cases, an increased risk to the privacy of the data subjects may arise, which may necessitate the conduct of a DPIA pursuant to Art. 22 of the FADP. It should be noted, however, that a breach of the obligation to conduct a DPIA does **not entail direct sanctions** and does not constitute a violation of privacy.

IV. DATA PROTECTION PRINCIPLES FOR PROCESSING

28 The principles of data processing under the FADP are mandatory, regardless of whether the processing is carried out by a private controller or a federal body. The principles listed in Art. 6–8 FADP include:

- Lawfulness
- Good faith
- Proportionality
- Purpose limitation (transparency)
- Destruction and anonymization
- Accuracy
- Consent (including explicit consent)
- Data security

29 The right of access is of crucial importance, i.e., the right of a data subject to inspect the personal data concerning them (Art. 25 FADP). The AMLA contains special provisions in this regard as a *lex specialis*: For data maintained in the separate data collections pursuant to para. 3 of Art. 34 of the AMLA, the right of access may be asserted **exclusively against MROS**. Finally, it should be emphasized that the right of access under data protection law does not establish a claim to the surrender of the original documents: Under Art. 25 para. 2(b) of the FADP, only the personal data contained therein must be provided *as such*, but not complete documents such as emails, contracts, or reports.

30 For further details on the aforementioned principles, reference is made here to the literature on data protection law. In addition to the processing principles, there are further **governance obligations**, the violation of which generally does not constitute an infringement of personal rights. These include the obligation to maintain a record of processing activities (Art. 12 FADP), the engagement of processors (Art. 9 FADP), and, where applicable, a DPIA (Art. 22 FADP). In addition, reference should be made to the investigative powers of the FDPIC (Art. 49 et seq. FADP) as well as the sanctions pursuant to Art. 60 et seq. FADP.

BIBLIOGRAPHY

Alberini Adrien, Kommentierung zu Art. 33 GwG, in: Ursula Cassani, Christian Bovet, Katia Villard (Hrsg.), Commentaire romand, Loi sur le blanchiment d'argent, Basel, 2022.

Caroline Kindler, Kommentierung zu Art. 25 GwG in: Damian K. Graf/Doris Hutzler (Hrsg.), Onlinekommentar zum Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung – Version: 16.01.2025: https://onlinekommentar.ch/de/kommentare/gwg25 (besucht am 8.10.2025), DOI: 10.17176/20250319-201115-0.

Christen Marquard/Kuert Matthias, Kommentierung zu Art. 25 GwG, in: Peter Ch. Hsu/Daniel Flühmann (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

De Capitani Werner, Kommentierung zu Art. 33 GwG, in: Schmidt Niklaus (Hrsg.), Kommentar Einziehung – Organisiertes Verbrechen – Geldwäscherei, Bd. I, 2. Aufl., Zürich et al. 2007.

Derungs Corsin/Gmünder Eliane, Kommentierung zu Art. 33 GwG, in: Kunz Peter V./Jutzi Thomas/ Schären Simon (Hrsg.), Stämpflis Handkommentar, Geldwäschereigesetz (GwG), Bern 2017.

Fiechter Eric/Maiko Günther, Sphère privée et diligence bancaire – des droits bafoués et des limites ignorées ? – Relation entre la loi sur le blanchiment d'argent et la loi sur la protection des données, in: SJZ 2010, S. 338-343.

Gaul Caroline/Isler Michael/Vasella David, Kommentierung zu Art. 33 GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Glatthaar Matthias/Schröder Annika, Kommentierung zu Art. 5 lit. f und g DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz – Version: 21.08.2023: https://onlinekommentar.ch/de/kommentare/dsg5fundg (besucht am 12.3.2026), DOI: 10.17176/20230819-101936-0.

Graber Christoph K./Oberholzer Dominik, Das neue GwG, 3. Aufl., Zürich 2009.

Häfelin Ulrich/Müller Georg/Uhlmann Felix, Allgemeines Verwaltungsrecht, 8. Aufl., Zürich et al. 2020.

Heierli Christian Marcus, Das Konzept der Selbstregulierung im GwG, in: GesKR 2010, S. 38 ff.

Kilgus Sabine, Datenschutz und Geldwäschereibekämpfung – Wer schützt wen wovon wofür?, in: Persönlichkeitsschutz zwischen Mensch und Maschine, 25 Jahre Datenschutz-Forum Schweiz, 2024, S. 135-153.

Kuster Matthias, Zur Rechtsnatur der Sanktionsentscheide von Selbstregulierungsorganisationen und der Schweizer Börse, in: AJP 2005, S. 1502 ff.

Maurer-Lambrou Urs/ Kunz Simon, Kommentierung zu Art. 2 DSG, in: Maurer-Lambrou Urs/Blechta Gabor-Paul (Hrsg.), Datenschutzgesetz / Öffentlichkeitsgesetz, Basler Kommentar, 3. Aufl., Basel 2014.

Rosenthal David, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020.

Rudin Beat, Kommentierung zu Art. 2 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Derselbe, Kommentierung zu Art. 5 DSG, in: Baeriswyl Bruno/Pärli Kurt/Blonski Dominika (Hrsg.), Datenschutzgesetz, Stämpflis Handkommentar, 2. Aufl., Bern 2023.

Taube Tamara, Entstehung, Bedeutung und Umfang der Sorgfaltspflichten der Schweizer Banken bei der Geldwäschereiprävention im Bankenalltag, in: SGFM – St. Galler Schriften zum Finanzmarktrecht Band/Nr. 9, Zürich et al. 2013.

Thelesklaf Daniel, Kommentierung zu Art. 33 GwG, in: Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell Füssli Navigator Kommentar, GwG Kommentar/AMLA Commentary, 3. Aufl., Zürich 2019.

Vasella David, Überlegungen zum Profiling mit hohem Risiko, datenrecht.ch, 23.11.2020, abrufbar unter https://datenrecht.ch/ueberlegungen-zum-profiling-mit-hohem-risiko/, besucht am 12.3.2026 (zit. Vasella, Profiling).

Wyss David, FINMA-Bussenkompetenz – ein wirksames Mittel zur Abschreckung?, in: GesKR 2024, S. 129 ff.

Zysset Pascal, Kommentierung zu Art. 25 GwG, in: Peter V. Kunz/Thomas Jutzi/Simon Schären (Hrsg.), Stämpflis Handkommentar zum Geldwäschereigesetz (GwG), Bern et al. 2017.

MATERIALS

Beschluss des Parlaments vom 26.9.2025 (Referendumsvorlage), BBl 2025 2899, abrufbar unter https://www.fedlex.admin.ch/eli/fga/2025/2899/de, besucht am 22.1.2026.

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.3.1988, BBl 1988 II 413 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1988/2_413_421_353/de, besucht am 9.8.2025.

Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor vom 17.6.1996, BBl 1996 III 1154 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1996/3_1101_1057_993/de, besucht am 21.8.2025.

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 15.9.2017, BBl 2017 6941 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2017/2057/de, besucht am 15.12.2025.

Botschaft zur Änderung des Geldwäschereigesetzes (GwG) vom 26.6.2019, BBl 2019 5451 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2019/1932/de, besucht am 9.10.2025.

Botschaft zum Bundesgesetz über die Transparenz juristischer Personen und die Identifikation der wirtschaftlich berechtigten Personen (TJPG) vom 22.5.2024, BBl 2024 1607 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2024/1607/de, besucht am 22.1.2026.

Geschäftsbericht 2021 des Bundesgerichts vom 17.2.2022, abrufbar unter https://www.eidgenoessischegerichte.ch/de/files/geschaeftsberichte/GB_2021_d.pdf, besucht am 23.8.2024.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 34 AMLA

A commentary by Emmanuel Goldberg / Dominic Robert

SUGGESTED CITATION

Emmanuel Goldberg/Dominic Robert, Commentary of art. 34 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Goldberg/Robert, art. 34 AMLA N. XXX.

Art. 34 Databases and files in connection with the reports and the information submitted to the Reporting Office

[1] Financial intermediaries must maintain separate databases and files containing all documentation relating to reports made in accordance with Article 9 of this Act or Article 305ter paragraph 2 of the SCC and to enquiries made by the Reporting Office in accordance with Article 11*a*.

[2] They may pass on data from these databases and files solely to FINMA, the FGB, the intercantonal authority, the Central Office, supervisory organisations, self-regulatory organisations, the Reporting Office and the prosecution authorities.

[3] The right to information of data subjects in accordance with Article 25 of the Data Protection Act of 25 September 2020 on must be asserted vis-à-vis the Reporting Office (Art. 35).

[4] The data must be destroyed five years after the report is filed.

CONTENT

I. Introduction 630
II. Databases and files relating to suspicious activity reports (para. 1) 630
A. Addressees of the standard 630
B. Relevant files 631
C. Need-to-know principle 632
D. No-AML reports 632
1. Documentation requirements 632
2. Maintenance of a separate database for no-AML reports 633
E. Requests from the reporting office pursuant to Art. 11a AMLA 633
1. Disclosure of additional information 634
2. Third-party intermediaries and foreign FIUs 634
III. Disclosure of data and files (para. 2) 635
IV. Right of access of data subjects (para. 3) 636
V. Destruction of data after five years (para. 4) 638
Bibliography 640
Materialis 641

I. INTRODUCTION

1 With the entry into force of the revised Anti-Money Laundering Act (AMLA) on January 1, 2023, Art. 34 AMLA was significantly amended in the interests of legal consistency. Firstly, the heading of Art. 34 AMLA was amended to reflect the content, which concerns data collection in connection with both the reporting obligation (Art. 9 AMLA) and the right to report (Art. 305ter para. 2 SCC). This was done primarily with a view to providing a more comprehensive formulation and extending the scope to include information that may be disclosed to the Money Laundering Reporting Office (MROS) in accordance with Art. 11*a* AMLA. It now bears the title: *"Databases and files relating to reports and information provided to the reporting office"*. Secondly, the previous AMLA supervisory authorities have been expanded to include the Central Office.

II. DATABASES AND FILES RELATING TO SUSPICIOUS ACTIVITY REPORTS (PARA. 1)

A. Addressees of the standard

2 According to Art. 34 para. 1 AMLA, financial intermediaries must maintain **separate databases and files** containing all documents relating to the reporting obligation (Art. 9 AMLA) or the right to report (Art. 305ter para. 2 SCC) as well as to inquiries from the Reporting Office (MROS) pursuant to Art. 11*a* AMLA. By explicitly listing both types of reporting, the legislator made it clear that the right to report continues to fall within the scope of Art. 34 AMLA and that the same rules apply to the separate data collections for all reports. The storage of databases and files within the meaning of Art. 34 AMLA applies exclusively to financial intermediaries – thus, the standard does not refer to the storage of such documentation by MROS itself. This provision is a *lex specialis* to the data protection regulations governing the handling of documentation, the access rights of the customers concerned, and the retention periods that apply in connection with a suspicious activity report.

B. Relevant files

Financial intermediaries already collect a considerable amount of customer data at the beginning and in the course of the usual business relationship as part of their due diligence obligations. If the financial intermediary decides to report to MROS, it would be impractical, even disproportionate, to **subsequently separate** all electronic and physical data in the customer file that is related to the internal investigations and the report. The mere customer data collected in the course of the normal business relationship can be stored separately as a copy or as an attachment to the suspicious activity report in accordance with Art. 34 para. 1 AMLA. 3

The documents collected during the reporting process primarily include the **reporting form** completed by the financial intermediary (which, since 2020, has been submitted electronically via the "goAML" information system) **as well as relevant supporting documents and file notes** containing a detailed analysis of the reasonable grounds for suspicion and the in-depth investigations carried out (Art. 6 AMLA). The latter consist of investigations by the compliance department or the anti-money laundering unit based on publicly or restrictedly accessible databases (e.g., relevant media articles, PEP comparisons using databases such as World-Check, or detailed evidence of suspicious transactions) and the results of these investigations. If these do not dispel the initial suspicion, KYC documents or, if applicable, the communication between the customer and the customer advisor or the money laundering unit with the customer advisor must be attached. In addition, correspondence or reports prepared by a qualified third party (such as external compliance service providers or specialized lawyers) may also be attached. This must enable MROS to make a decision based on the report file. As a result, such documents are no longer merely business documents collected as part of the usual due diligence obligations (Art. 3, 4, and 5 AMLA), but rather files of increased sensitivity. 4

The MROS maintains a **non-exhaustive list** of documents that must be submitted for reports in accordance with the Ordinance on the Money Laundering Reporting Office (MGwV). 5

C. Need-to-know principle

6 In order to ensure the proper management of risks relating to the confidentiality of electronic and physical customer data, the "need-to-know" principle must be strictly applied. This fundamental principle of data protection means that individuals may only be given access to information or functionalities **that are necessary for the performance of their duties**. Consequently, only the anti-money laundering unit of the respective financial intermediary should be given access to the separate data collection and be entrusted with its processing and management. In practice, the anti-money laundering unit creates a report dossier for each completed suspicious case and archives a copy of it with restricted access in a separate internal database. It should be noted that the documentation of the customer file with the usual business documents remains unaffected by this.

D. No-AML reports

7 According to the wording, only reports actually submitted to MROS fall within the scope of Art. 34 para. 1 AMLA. In practice, however, it may happen that, after in-depth investigations of the suspected money laundering, certain **suspicious circumstances can be ruled out** – for example, if the unusual or conspicuous behavior of the customer can be explained or if there is simply no predicate offense to money laundering. This gives rise to a documentation obligation in the form of a "no-AML report," which, following the partial revision of the GwV-FINMA, has been newly regulated in Art. 22a para. 2 GwV-FINMA since January 1, 2023.

1. Documentation requirements

8 Accordingly, if a financial intermediary decides not to file an MROS report because the suspicion has been dispelled by additional investigations, it must document the reasons for this decision. There is no reporting obligation within the meaning of Art. 9 AMLA, as there is no "reasonable suspicion." The financial intermediary must document the clarifications carried out as part of the No-AML report in accordance with the requirements of Art. 7 AMLA, but primarily in order to be able to prove that the reporting obligation was not violated by not filing a report. The requirements for this **documentation obligation** are designed in such a way that even expert third parties can form a reliable opinion on compliance with the due diligence obligations.

Because "**hindsight bias**" can often occur in the retrospective assessment of decisions – i.e., the risk that the facts appear clearer and more complete in retrospect than they actually were at the time of the decision – particularly high requirements must be placed on the content of a No-AML report. This is the only way to prevent administrative, supervisory, or even criminal consequences. 9

2. Maintenance of a separate database for no-AML reports

No-AML reports differ from actual MROS reports only in their **outcome** – the additional clarifications carried out and the sensitivity of the data remain the same. In practical terms, such cases are also documented and archived in a separate database by the anti-money laundering unit. For this reason, it can be logically assumed – despite not being explicitly mentioned – that such data collections fall within the scope of Art. 34 AMLA. 10

From a practical point of view, it seems obvious to place no-AML reports within the scope of Art. 34 para. 1 AMLA, as further grounds for suspicion may arise in the course of the business relationship in question. In this case, additional clarifications must be carried out and, if necessary, new sensitive customer data must be collected, documented, and stored in a separately maintained database. A no-AML report from a non-reporting financial intermediary could also constitute part of the additional information requested by MROS on the basis of a suspicious activity report from a reporting financial intermediary pursuant to Art. 11*a* AMLA. This would mean that the no-AML report is related to a suspicious activity report, which is why the same rules must apply as for the suspicious activity report itself. Due to the close relationship between the no-AML report and the MROS report described above, it seems justified to deny the customer the right to information under the FADP with regard to the sensitive customer data associated with the no-AML report. 11

E. Requests from the reporting office pursuant to Art. 11*a* AMLA

With the partial revision of the AMLA, since January 1, 2023, a financial intermediary must maintain separate databases and files with all documents related to requests from the reporting office pursuant to Art. 11*a* AMLA. 12

1. Disclosure of additional information

13 If MROS requires additional information for the analysis of a report received by it pursuant to Art. 9 AMLA or Art. 305ter para. 2 SCC, the reporting financial intermediary must disclose this information to MROS upon request pursuant to Art. 11*a* para. 1 AMLA, insofar as it is available to the financial intermediary. This means that any additional information obtained by MROS from a reporting financial intermediary is assigned to the report file in accordance with Art. 34 para. 1 AMLA. This does not include information that goes beyond the suspicious activity report, but is **closely related** to it.

2. Third-party intermediaries and foreign FIUs

14 If, on the basis of this analysis, MROS determines that, in addition to the reporting financial intermediary, other financial intermediaries **are or were** involved in a transaction or business relationship, the financial intermediaries involved must, upon request, provide the reporting office with all related information in their possession, in accordance with Art. 11*a* para. 2 AMLA.

15 Prior to the partial revision on January 1, 2023, non-reporting financial intermediaries were not required to maintain additional information requested by MROS under Art. 11*a* para. 2 AMLA in a separate database within the meaning of Art. 34 para. 1 AMLA. Considering that the additional information provided by a non-reporting financial intermediary is **highly sensitive data** in connection with a suspicious activity report – and not regular KYC information – the unequal treatment did not appear to be objectively justified.

16 If, based on the analysis of information from a **foreign reporting office** ("Financial Intelligence Unit" [FIU]), it becomes apparent that financial intermediaries subject to the AMLA are or were involved in a reported transaction or business relationship, the financial intermediaries involved must, in accordance with Art. 11*a* para. 2bis AMLA, provide MROS with all related information upon request, insofar as they have it at their disposal.

17 Before the entry into force of para. 2bis on July 1, 2021, MROS was only able to obtain additional information if this was required for the analysis of a suspicious activity report from a financial intermediary operating exclusively **within Switzerland**. Such a locally bound requirement constituted an obstacle in the cross-border fight against money laundering and terrorist financing: The MROS was not yet able to request additional information from Swiss financial

intermediaries on the basis of a request or ad hoc information provided by a foreign FIU. Only if a suspicious activity report from a Swiss financial intermediary was already in its database could the MROS deepen its analysis and request additional information. Financial intermediaries are not informed whether the MROS's request for information is based on para. 2 or para. 2bis, which is why the information must be stored in separate databases in accordance with Art. 34 para. 1 AMLA.

III. DISCLOSURE OF DATA AND FILES (PARA. 2)

Financial intermediaries may only disclose data from the aforementioned separately maintained databases and files to FINMA, the ESBK, the intercantonal authority, the central office, the supervisory and self-regulatory organizations, MROS, and law enforcement authorities. This list is **exhaustive**. The explicit mention of the reporting office and the law enforcement authorities is considered unfortunate by some scholars, as it makes the other competent data recipients appear to be of equal importance, even though they should be viewed differently. This is because MROS receives the report file with the suspicious activity report in accordance with Art. 9 AMLA or Art. 305ter para. 2 of the SCC and forwards it to the law enforcement authorities if there is reasonable suspicion in accordance with Art. 23 para. 4 AMLA. 18

It should therefore be clarified that Art. 34 para. 2 AMLA is a **mandatory provision** with regard to the disclosure of this data to MROS. With regard to the other authorities mentioned in the paragraph, financial intermediaries are not generally obliged to automatically forward every suspicious activity report together with the complete report dossier. If the report concerns a business relationship involving significant assets, the reporting financial intermediary must inform the authorities of the report (Art. 22*a* GwV-FINMA). It should also be noted that some self-regulatory organizations require their affiliated financial intermediaries to immediately forward a copy of each report submitted. However, an obligation to disclose information to a supervisory authority only arises if the latter expressly requests access to the report file after being informed by the financial intermediary that a suspicious activity report has been submitted. 19

Since January 1, 2020, financial intermediaries have been submitting their suspicious activity reports predominantly by electronic means. The MROS data processing system used to date has been replaced by the "goAML" informa- 20

tion system. Law enforcement authorities also receive the information reported to MROS via "goAML," supplemented by an analysis report from MROS. To date, however, MROS must also accept suspicious activity reports in paper form. With the upcoming partial revision of the AMLA, this option will be eliminated (Art. 23 para. 7 E-AMLA).

21 The disclosure of particularly sensitive personal data to third parties is prohibited under Art. 30 para. 2 lit. c of the FADP, unless there is a justification under Art. 31 para. 1 FADP. This justification is provided by Art. 34 para. 2 AMLA. Under data protection law, there is generally **no additional justification** required vis-à-vis MROS, as the statutory reporting obligation already requires the disclosure of the relevant data. Art. 34 para. 2 AMLA also clearly regulates which recipients have access to the data contained in the report file, regardless of how sensitive the data is. Additional justifications under Art. 31 para. 1 FADP are therefore excluded.

IV. RIGHT OF ACCESS OF DATA SUBJECTS (PARA. 3)

22 In the context of data protection, the right of access plays the most important role. It allows the data subject – i.e. the person whose data is being processed – to assert their data protection rights. This is because the prerequisite for safeguarding the rights of the data subject is their **knowledge of the data** being processed about them.

23 With regard to the right to information under data protection law, the AMLA now provides for special provisions with regard to its assertion in the sense of a *lex specialis*: According to Art. 34 para. AMLA, the right of access of a data subject (Art. 25 FADP) must be exercised **vis-à-vis MROS** – and not, for example, vis-à-vis the financial intermediary (Art. 35 AMLA). The actual processing by MROS – i.e., the modalities of data processing, the data subject's right to information, and any restrictions on the information – is regulated by Art. 35 AMLA in accordance with Art. 8 of the Federal Act on Federal Police Information Systems (BPI).

24 The financial intermediary's prohibition on disclosure under Art. 10*a* aGwG had been indefinite since the partial revision on January 1, 2016. However, this was still contrasted by the exclusion of the right to information, which remained **limited in time** under Art. 34 para. 3 aGwG (during the MROS's analysis or the freezing of assets under Art. 10 aGwG).

This contradiction led to legal uncertainty for financial intermediaries, as on the one hand they could not refuse to provide an affected person with information about their report file under Art. 34 para. 3 AMLA. On the other hand, however, by disclosing the report file to the affected person, they would have violated the information prohibition under Art. 10*a* AMLA. However, both after the analysis had been completed and after the asset freeze had been lifted, the persons concerned still had the opportunity to assert their right to information. At that point in time, the report file would still have been the subject of preliminary investigations by the criminal prosecution authorities. Conversely, this would mean that the person concerned would learn of both the suspicious activity report and the involvement of the criminal authorities. If the person concerned decided to withdraw their assets, which in the worst case scenario would not yet be subject to a freezing order, the criminal proceedings would be immediately jeopardized. Furthermore, there was a risk that the customer would terminate the customer relationship and take legal action against the financial intermediary if the latter disclosed information about the report file. Although the financial intermediary would be protected under the provisions of Art. 11 AMLA, it could still face reputational damage as well as civil and criminal proceedings. 25

The current legal provision not only ensures consistency between Art. 34 and Art. 10*a* AMLA by **indefinitely excluding** the right to information under data protection law, but also improves the effectiveness of the suspicious activity reporting system. A data subject may only exercise their right to information on data in the separate data collections at MROS. The reporting office can therefore provide information to the data subject at its own discretion in accordance with Art. 35 para. 1 AMLA and in compliance with the procedural requirements relating to police collections of suspicious activity data. This ensures that information relevant to suspicions is processed in accordance with data protection regulations without jeopardizing the interests and procedures of the law enforcement authorities, which in turn increases legal certainty. 26

Data collected in connection with additional inquiries by reporting offices pursuant to Art. 11*a* AMLA from reporting and non-reporting financial intermediaries is also subject to the indefinite exclusion of the right to information. Financial intermediaries may not provide the person concerned with **any information** about this data (Art. 10*a* para. 1 AMLA). 27

V. DESTRUCTION OF DATA AFTER FIVE YEARS (PARA. 4)

28 According to Art. 34 para. 4 AMLA, data collected in connection with a report and forwarded to MROS must be destroyed **five years** after the report was made. This provision thus deviates from the ten-year retention period for business records under Art. 7 para. 3 AMLA and that under Art. 958f para. 1 CO.

29 Some legal scholars agree that the five-year retention period under Art. 34 para. 4 AMLA is a **coordination error on the part of the legislator**. In accordance with the recommendations of the Financial Action Task Force (FATF) and the EEC Money Laundering Directive, a retention period of five years was originally envisaged for Art. 7 para. 3 AMLA. However, during the parliamentary deliberations, the period in Art. 7 para. 3 AMLA was extended to ten years, as the documents in question often also constitute business documents and are therefore subject to the civil law retention obligation. However, Art. 34 para. 4 AMLA was not amended, even though it would also be appropriate to align it with the ten-year period. The opinion expressed here concurs with the recommendation of the majority of legal scholars, namely that – contrary to the current legal provision – Art. 34 para. 4 AMLA should be interpreted in line with the ten-year period specified in Art. 7 para. 3 AMLA.

30 The reporting office points out that the documents to be deleted are only copies of documents that were submitted to the reporting office in the context of a suspicious activity report or on the basis of a request (Art. 11*a* AMLA) and are **not original documents** within the meaning of Art. 7 para. 3 AMLA. However, this does not change the shortened retention period and the associated unsatisfactory situation for financial intermediaries in terms of supervisory law.

31 Another part of the doctrine considers that this approach can no longer be maintained because the five-year period in Art. 34 para. 4 AMLA has remained unchanged despite the recent amendment of the other paragraphs of Art. 34 AMLA and has not been extended to ten years. A shorter retention period is understandable from a data protection perspective, as personal data may only be retained for as long as is necessary for the **purpose of processing** (Art. 6 para. 4 FADP). This principle was already indirectly included in the principle of proportionality prior to the revision of the FADP. Once the suspi-

cious activity report has been forwarded to MROS, the latter has all the relevant information and documents in accordance with Art. 34 para. 1 AMLA, so it can be assumed that these are no longer needed by the financial intermediary after five years. However, there is currently no apparent obligation under data protection law to delete the data after five years at the latest. Furthermore, para. 4 explicitly states that the data must be deleted after five years and not that it must be retained for at least five years. This can be interpreted as a clarification of the principle of data minimization (Art. 6 para. 2 FADP). Once the data has served its purpose, the financial intermediary has the option of deleting it earlier. In our opinion, this data fulfills its purpose from the perspective of MROS – however, from the perspective of the reporting financial intermediaries, this must be critically questioned. With regard to internal and external audit activities, however, financial intermediaries are advised not to delete the relevant documents prematurely. The statute of limitations for criminal prosecution, for example in the case of a breach of the reporting obligation under Art. 37 AMLA, which is seven years (Art. 52 FINMASA), must also be taken into account. It is not uncommon for an even longer period of time to elapse between the beginning of the breach of the reporting obligation and a criminal conviction. In this context, it is questionable whether and how a financial intermediary concerned can substantiate its defense without access to the relevant data in the report file.

From a practical point of view, financial intermediaries and the money laundering unit are already obliged to maintain a separate database with restricted access for documents and files in a report file. If the approach taken by the law is followed, the respective report files must be systematically assigned a five-year deadline, which either reminds the financial intermediary to manually delete the report files or automatically deletes them, resulting in additional **administrative effort**. This effort will be particularly noticeable in the banking sector: according to the MROS's annual statistics for 2024, 92.3% of the total 15,141 suspicious activity reports submitted came from the banking sector. This corresponds to approximately 59 reports per working day. 32

Furthermore, the practical purpose of storing personal data in the context of a suspicious activity report is not exclusively external, i.e., it is not merely to forward the data to MROS. In **internal relations**, business relationships that are reported to MROS on suspicion of money laundering and are not terminated should be categorized as having an increased risk of money laundering 33

and be subject to special due diligence obligations (Art. 6 AMLA). The deletion of the report file after the five-year period or even earlier is not consistent with the risk assessment by the financial intermediary if the business relationship continues. If the business relationship does not involve any other risk-increasing factors (e.g., residence in a country with increased risk), a financial intermediary would be disposing of what is probably its only internal evidence of clarification and justification for the increased risk categorization.

34 In this context, it is also questionable how to deal with subsequent reports after the original report file has been deleted if new suspicions arise. A legal **adjustment to the ten-year retention period** would give the competent money laundering unit more time to follow up on information that has already been reported. This would improve traceability and the depth of documentation and would be useful to both the reporting office and the law enforcement authorities.

BIBLIOGRAPHY

Bloch Juerg/Bühler Simon, Kampf gegen Terrorismusfinanzierung in der Schweiz: Herausforderungen für Finanzintermediäre, in: GesKR 2024, S. 53-73.

De Capitani Werner, Kommentierung zu Art. 34 GwG, in: Schmidt Niklaus (Hrsg.), Kommentar Einziehung – Organisiertes Verbrechen – Geldwäscherei, Bd. I, 2. Aufl., Zürich et al. 2007.

Derungs Corsin/Gmünder Eliane, Kommentierung zu Art. 34 GwG, in: Kunz Peter V./Jutzi Thomas/ Schären Simon (Hrsg.), Stämpflis Handkommentar, Geldwäschereigesetz (GwG), Bern 2017.

Gaul Caroline/Isler Michael/Vasella David, Kommentierung zu Art. 34 GwG, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar, Geldwäschereigesetz, Basel 2021.

Graber Christoph K./Oberholzer Dominik, Das neue GwG, 3. Aufl., Zürich 2009.

Gramigna Ralph, Kommentierung zu Art. 25 DSG, in: Blechta Gabor P., Vasella David (Hrsg.), Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz, 4. Aufl., Basel 2024.

Hutzler Doris, EFD-Verurteilungen wegen Meldepflichtverletzung: Verantwortlichkeit in der Praxis, in: SZW 2025, S. 278-289.

Kilgus Sabine, Datenschutz und Geldwäschereibekämpfung – Wer schützt wen wovon wofür?, in: Persönlichkeitsschutz zwischen Mensch und Maschine, 25 Jahre Datenschutz-Forum Schweiz, 2024, S. 135-153.

Luchsinger Roland J./Blaser Julia, Neuerungen und offene Fragen der revidierten Geldwäschereivorschriften im Bereich des Nachmeldeverfahrens von Finanzintermediären, in: SZW 2022, S. 556-571.

Ordolli Stiliano, Kommentierung zu Art. 34 GwG, in: Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell Füssli Navigator Kommentar, GwG Kommentar/AMLA Commentary, 3. Aufl., Zürich 2019.

Rosenthal David, Das neue Datenschutzgesetz, in: Jusletter 16. November 2020.

MATERIALIS

Association Romande des Intermediaires Financiers (ARIF), Richtlinie 13 zur Melde-, Sperr- und Geheimhaltungspflicht, abrufbar unter https://arif.ch/IMG/pdf/directives_2-13_d.pdf, besucht am 11.1.2026.

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.3.1988, BBl 1988 II 413 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1988/2_413_421_353/de, besucht am 29.08.2025.

Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor vom 17.6.1996, BBl 1996 III 1154 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1996/3_1101_1057_993/de, besucht am 21.08.2025.

Botschaft zur Änderung des Geldwäschereigesetzes vom 27.6.2012, BBl 2012 6941 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2012/1031/de, besucht am 27.8.2025.

Botschaft zur Umsetzung der 2012 revidierten Empfehlungen der Groupe d'action financière (GAFI) vom 13.12.2013, BBl 2014 605 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2014/100/de, besucht am 31.8.2025.

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetztes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.9.2017, BBl 2017 6941 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2017/2057/de, besucht am 1.9.2025.

Botschaft zur Genehmigung und zur Umsetzung des Übereinkommens des Europarats zur Verhütung des Terrorismus mit dem dazugehörigen Zusatzprotokoll sowie zur Verstärkung des strafrechtlichen Instrumentariums gegen Terrorismus und organisierte Kriminalität vom 14.9.2018, BBl 2018 6427 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2018/2301/de, besucht am 26.8.2025.

Botschaft zur Änderung des Geldwäschereigesetzes vom 26.6.2019, BBl 2019 5451 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2019/1932/de, besucht am 18.8.2025.

Botschaft zum Bundesgesetz über die Transparenz juristischer Personen und die Identifikation der wirtschaftlich berechtigten Person vom 22.5.2024, BBl 2024 1607 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/2024/1607/de, besucht am 22.11.2025.

Eidgenössische Finanzmarktaufsicht FINMA, Rundschreiben 2008/21 Operationelle Risiken – Banken, Eigenmittelanforderungen und qualitative Anforderungen für operationelle Risiken bei Banken, vom 20.11.2008, abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/rundschreiben-archiv/2008/rs-08-21/finma-rs-2008-21-20160922.pdf?sc_lang=de&hash=508C674329EF83C44FE1F53784637529, besucht am 23.8.2025.

Eidgenössische Finanzmarktaufsicht FINMA, Erläuterung zur Teilrevision der Geldwäschereiverordnung der FINMA (GwV-FINMA) vom 27.10.2002, abrufbar unter https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/anhoerungen/abgeschlossene-anhoerungen/20221102-gwv-finma/erlaeuterungen_gwv_finma_20221027_de.pdf?sc_lang=de&hash=B2A5602EF279E721D833637EB4E92F38, besucht am 23.8.2025.

Eidgenössisches Justiz- und Polizeidepartement EJPD, Bundesamt für Polizei fedpol, Meldestelle für Geldwäscherei (MROS), Jahresbericht 2021, Bern 2022, abrufbar unter https://www.fedpol.admin.ch/dam/fedpol/de/data/krimi-

nalitaet/geldwaescherei/jabe/jb-mros-2021.pdf.download.pdf/jb-mros-2021-d.pdf, besucht am 1.9.2025.

Eidgenössisches Justiz- und Polizeidepartement EJPD, Bundesamt für Polizei fedpol, Meldestelle für Geldwäscherei (MROS), Jahresbericht 2024, Bern 2022, abrufbar unter <https://www.fedpol.admin.ch/dam/fedpol/de/data/kriminalitaet/geldwaescherei/jabe/jb-mros-2024.pdf.download.pdf/jb-mros-2024-d.pdf> (besucht am 13.10.2025)

Eidgenössisches Justiz- und Polizeidepartement EJPD, Bundesamt für Polizei fedpol, Meldestelle für Geldwäscherei (MROS), Hilfreiche Dokumente und Links, Verdachtsmeldung gemäss Art. 9 GwG, abrufbar unter https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/meldung.html, besucht am 3.9.2025.

PolyReg Allg. Selbstregulierungs-Verein, Reglement der SRO PolyReg gemäss Art. 25 GwG, abrufbar unter https://www.polyreg.ch/uploads/20230216.reglement.final.de.pdf, besucht am 11.1.2026.

Schweizerischer Versicherungsverband, Kommentar zum Reglement der Selbstregulierungsorganisation zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung vom 12.2019, abrufbar unter https://www.sro-svv.ch/de/regelwerk/regulatorischer-auftrag/kommentar-zum-reglement-sro-svv, besucht am 8.9.2025.

ATTENTION: This version of the commentary is an automatically generated machine translation of the original. The original commentary is in German. The translation was done with www.deepl.com. Only the original version is authoritative. The translated form of the commentary cannot be cited.

COMMENTARY ON

Art. 38 AMLA

A commentary by Thomas Nagel / Denis Parvex

SUGGESTED CITATION

Thomas Nagel/Denis Parvex, Commentary of art. 38 AMLA, in: Damian K. Graf/Doris Hutzler (eds.), Online Commentary of the Federal Act on Combating Money Laundering and Terrorist Financing

Short citation: OK-Nagel/Parvex, art. 38 AMLA N. XXX

Art. 38 Violation of the duty to verify

[1] Any dealer that wilfully violates the duty under Article 15 to appoint an audit firm shall be liable to a fine not exceeding 100,000 francs.

[2] If the dealer acts through negligence, it shall be liable to a fine not exceeding 10,000 francs.

CONTENT

I. General 647
II. Objective elements 647
A. Persons liable 647
B. Offence 648
III. Subjective elements of the offence 649
A. Intent (para. 1) 649
B. Errors 650
C. Negligence (para. 2) 650
IV. Criticism of the offence 651
V. Criminal penalty 652
VI. Concurrent offences 652
VII. Limitation 653
VIII. Insurability 653
Bibliography 655
Materials 656

I. GENERAL

Art. 38 AMLA was introduced as part of the Federal Act for Implementing the Revised FATF Recommendations of 2012 and thus with the first-time coverage of dealers by AMLA. The provision came into force on 1 January 2016. Initially, a ban on cash payments of more than CHF 100,000 and criminal liability for merchants accepting such amounts in cash were proposed. This plan was rejected on various grounds. The offence established in Article 38 AMLA is therefore a **legislative compromise**. 1

The provision aims to **ensure that dealers** comply with their due diligence obligations in the fight against money laundering. In other words, it is intended to ensure that private individuals participate in the administration of justice by complying with the provisions of the AMLA that apply to them (for the purpose of the AMLA, see OK-Nagel, Art. 1 AMLA N. 1 ff.). It is not the violation of the dealer's obligations under Article 8*a of the* AMLA that is penalised, but the failure to appoint an auditor to check that dealers comply with these obligations (see below, N. 7 et seq.). In addition to violating the duty to check, dealers may also be liable to prosecution if they violate the duty to report (see OK-Hutzler, Art. 37 AMLA and OK-Nagel, Art. 15 AMLA). 2

In the event of criminal proceedings under Art. 38 AMLA, the **FDF** is responsible for prosecuting and judging violations (see Art. 50 para. 1 and Art. 1 para. 1 let. f FINMASA), whereby the AACA applies (Art. 1 AACA). The general section of the SCC applies on a subsidiary basis. If the accused requests a court ruling, the Federal Criminal Court is responsible (Art. 50 para. 2 FINMASA in conjunction with Art. 21 para. 1 DDA). 3

II. OBJECTIVE ELEMENTS

A. Persons liable

The punishable offence under Article 38 AMLA is the **failure to appoint an auditor** to verify that a dealer within the meaning of Article 2 para. 1 AMLA is complying with the obligations under the AMLA. This makes Article 38 AMLA a special offence that can only be committed by a dealer within the meaning of Article 2 para. 1 let. b AMLA. For a potential group of perpetrators, reference can thus be made to the comments in the commentaries on Art. 2 para. 1 4

AMLA and Art. 8a AMLA. In a nutshell, dealers (and thus potential perpetrators within the meaning of Art. 38 AMLA) are persons who engage in commercial goods trading within the meaning of Art. 13 et seq. AMLO, i.e. the purpose is an independent economic activity aimed at making a permanent profit, in the course of which one or more goods worth more than CHF 100,000 are sold for cash in a single transaction without involving a financial intermediary (Art. 8*a.* Para. 4 AMLA *e contrario*). Persons who are not dealers themselves may, where applicable, be involved as participants in the intentional offence (para. 1); instigators and accomplices are punishable under Art. 50 para. 1 FINMASA in conjunction with Art. 5 VStrR.

5 If Art. 38 AMLA is violated in a **business operation**, any natural person who, when managing the affairs of a sole proprietorship or otherwise in the course of business or official duties for another – actively or by omission – (Art. 50 para. 1 FINMASA in conjunction with Art. 6 para. 1 VStrR). In addition, principal's liability may apply in accordance with Art. 6 para. 2 Due Diligence Act. Within the company, the executive body is generally responsible for commissioning an audit firm. This responsibility can be delegated, but not the authority to do so (see OK-Nagel, Art. 15 AMLA N. 4). In the case of a joint-stock company, the board of directors would be responsible for the mandate on the basis of the catch-all competence of Art. 716 para. 1 CO, provided that this competence has not been transferred to another body (e.g. the executive board). The bodies that have been assigned the responsibility and bear the responsibility can be punished in accordance with Art. 38 AMLA.

6 Art. 102 SCC cannot be applied in the event of a violation of Art. 38 AMLA (without the fulfilment of other criminal offences), since this offence is an **infraction.** The punishment of a legal entity as the perpetrator within the meaning of Art. 38 AMLA is therefore excluded. According to Art. 6 of the AACA, the natural persons acting for the company are to be punished. At most, subsidiary default liability under Art. 7 of the AACA in conjunction with Art. 49 of the FINMASA may be applied.

B. Offence

7 The offence under Article 38 AMLA is the **failure to commission an audit or to allow an audit** to be carried out, and thus a violation of the duty to commission an audit firm (Article 15 AMLA). It is therefore a genuine offence of omission. The offence begins and is simultaneously completed as soon as

the auditor should have been appointed pursuant to Art. 15 AMLA at the latest in order to ensure a proper and timely audit. However, the law does not state that the audit of dealers must be carried out annually. Accordingly, in practice it may be difficult to accuse a merchant of violating Art. 15 AMLA – in our opinion, it is unclear when this violation begins. EXPERTsuisse and Wyss take the view that the audit should be carried out at the latest when the merchant would have to have an audit of the annual financial statements carried out if they had to carry out an audit in accordance with the CO. This would mean that, for example, the audit of a joint-stock company would have to be carried out within six months of the end of the financial year (in line with Art. 699 para. 2 CO). This view seems logical, but it is questionable whether this analogy is sufficient to actually hold a culpable dealer criminally liable. In our opinion, this seems at least questionable due to the lack of a legal basis for the temporal aspects (*nulla poena sine lege*, Art. 1 SCC; see also OK-Nagel, Art. 15 N. 9).

Since the **beginning and the end of the offence coincide**, it is not possible to distinguish between the attempt (or threshold of the offence) and the completion. An attempted violation of Article 38 AMLA would not be punishable, as the penal provision only constitutes an offence. 8

Art. 38 AMLA does not cover non-compliance with the due diligence requirements for dealers in accordance with Art. 8*a.* AMLA or non-fulfilment of the obligations towards the auditors in accordance with Art. 15 para. 3 AMLA, including the provision of false information and the non-disclosure of documents or information. In the event of false information, the right is reserved to prosecute for document fraud (see Art. 251 SCC). 9

III. SUBJECTIVE ELEMENTS OF THE OFFENCE

A. Intent (para. 1)

Pursuant to Art. 38 para. 1 AMLA, anyone who **wilfully** violates the duty to mandate an audit firm in accordance with Art. 15 AMLA shall be punished. Thus, intent is required, which at least constitutes conditional intent, i.e. the trader must decide to remain inactive by considering the realisation of the offence to be possible and accepting it. The (conditional) intent must relate to all objective elements of the offence, i.e. the offender must have intent with regard to his qualification as a dealer, the existence of the testing obligation 10

and the non-fulfilment of the commissioning obligation. The offender does not need to be fully aware of the legal aspects of the duty to conduct due diligence. It is sufficient for him to be a layperson and to make a parallel assessment that makes him aware that he is violating a legal duty.

B. Errors

11 The following **errors** are possible:

a) The offender fails to recognise the situation that triggers the applicability of Article 38, para. 1 AMLA. This is a factual error that precludes a penalty under Art. 38 para. 1 AMLA. If this error could have been avoided with due diligence, a penalty is possible under Art. 38 para. 2 AMLA.

b) The offender does not realise, even though he has correctly understood the facts of the case, that he is subject to Art. 15 AMLA. In this case, it is a matter of an error of law. Errors of law are cautiously assumed by courts and only if they are unavoidable. If they are unavoidable, an error of law is not punishable due to lack of guilt. If the error of command is avoidable, this will lead to a reduction in sentence.

c) The offender is not aware of the prohibition (so-called error of prohibition). The potential offender must be aware of the reference standards (chain of reference from Art. 38 AMLA to Art. 15 AMLA to Art. 8a AMLA) at least in terms of the injustice. Due to the general mistrust of cash transactions and the public debate in the media about the corresponding due diligence obligations of traders, an error of prohibition is unlikely to occur.

C. Negligence (para. 2)

12 Pursuant to Art. 38 para. 2 AMLA, anyone who fails to fulfil an obligation within the meaning of Art. 15 AMLA, but does so **through negligence**, shall be liable to the penalties provided by law. Negligence may mean that the offender (i) fails to consider the consequences of his conduct resulting from a lack of caution in breach of duty (so-called unconscious negligence). Acting in breach of duty means that the offender fails to exercise the caution that would be expected of him in the circumstances and in his personal circumstances. However, negligence may also be deemed to exist if (ii) the offender, having recognised the consequences, fails to take them into account. This is known as conscious negligence.

IV. CRITICISM OF THE OFFENCE

The design of Art. 38 AMLA has been criticised by some scholars as falling short on the one hand, and as overshooting the mark on the other. This is because the actual aim should be to ensure that dealers comply with their due diligence obligations under the AMLA. However, an auditing requirement is not demonstrably suitable for inducing dealers to comply with their due diligence obligations, or it degenerates into an end in itself. The criminal liability for not appointing an auditor could lead to the bizarre result that dealers would fulfil all the due diligence requirements applicable to them under Article 8*a of the* AMLA but still be liable to prosecution. Dealers would thus be punished for not having their due diligence checked by an auditor. In this regard, according to voices in the doctrine, the penalty is excessive. Conversely, it could result in a dealer violating the due diligence requirements but having commissioned an auditor to carry out the audit and thus remaining unpunished. These examples show that a lesser degree of wrongdoing would be punished more severely. 13

In our opinion, the points of criticism from the literature listed above are generally understandable. However, in practice it is unlikely that a dealer who has consciously violated the duties will be audited. The punishability of not commissioning an auditor seems to be a legislative compromise (see above, N. 1), which has some undesirable consequences (probably not considered by the legislator). In our opinion, the question of whether criminal liability is necessary at all is justified, particularly with regard to the offence of negligence within the meaning of Art. 38 para. 2 AMLA. However, it is common practice in financial market law to punish those subject to the law for not obtaining licences or not carrying out audit procedures and to allow FINMA's supervisory instruments to be applied. For example, FINMA can explicitly use the supervisory instruments in accordance with Art. 29–37 FINMASA by law against persons who do not belong to a self-regulatory organisation (see Art. 20 para. 1 AMLA), and the criminal provisions of Art. 44 FINMASA may also apply. Traders do not require a licence or affiliation to a self-regulatory organisation, which is why FINMA's supervisory instruments cannot be applied to them due to the lack of an express legal provision. The fact that traders, unlike financial intermediaries, are not covered by the provisions of Article 305ter, para. 1 SCC (lack of due diligence in financial transactions) suggests that they may be liable to prosecution. This offence applies *expressis verbis* only to 14

'anyone who professionally accepts, holds, invests or helps transfer assets belonging to third parties and fails to exercise due diligence in determining the identity of the beneficial owner'. The definition of Art. 305ter para. 1 SCC is thus linked to the definition of Art. 2 para. 3 AMLA and only covers financial intermediaries (see OC commentary on Art. 2 para. 3 AMLA). In our opinion, it would appear appropriate to at least make punishable the intentional violation of the audit requirement or of compliance with the due diligence requirements. From our point of view, the latter would have been preferable. However, the question of criminal liability for dealers and its design is complex and not easy to answer.

V. CRIMINAL PENALTY

15 A dealer who **intentionally** violates the obligation under Article 15 AMLA to engage an audit firm shall be punished with a **fine of up to 100,000 francs**. If he acts **through negligence**, he shall be punished with a **fine of up to 10,000 francs**. Both intentional and negligent conduct are thus designed as offences under Art. 103 et seq. SCC. In the literature, it is criticised that the strong gradation of the penalties (up to ten times the amount of the fine for intent compared to negligence) does not take sufficient account of the borderline between conditional intent and negligence. Furthermore, the level of the penalty for the offence of intent is criticised. A fine of up to CHF 100,000 is disproportionate in view of the fact that it is an offence punishable by an act that does not actually enable money laundering.

16 If a fine of no more than CHF 50,000 is considered (and the investigation of the persons liable to prosecution requires investigative measures that would be disproportionate in view of the penalty imposed), the **business operation** may be ordered to pay the fine.

VI. CONCURRENT OFFENCES

17 If a dealer violates both the duty to verify in accordance with Art. 15 AMLA and the duty to report in accordance with Art. 9, para. 1bis AMLA, he is liable to prosecution in accordance with **Art. 37** and Art. 38 AMLA. The two offences are genuinely concurrent. The Federal Supreme Court has affirmed that the clarification and reporting obligations of Art. 6 and Art. 9 AMLA establish a guarantor obligation for financial intermediaries and that money

laundering by omission can therefore take place within the meaning of Art. 305bis in conjunction with Art. 11 SCC. However, the ruling has been heavily criticised in legal literature. In line with the Federal Supreme Court ruling, the reporting requirement under Article 8*a of the* AMLA and the requirement to appoint an auditor would have to establish such a duty of guarantee for dealers. If a trader, by failing to appoint an auditor, is also abetting money laundering (and is therefore liable to prosecution under Art. 305bis SCC), it is debatable whether this constitutes a genuine or a non-genuine (ideal) concurrence.

VII. LIMITATION

The prosecution limitation period is seven years (Art. 52 FINMASA). The enforcement limitation period, on the other hand, is five years according to Art. 11 para. 4 VStrR. Art. 38 AMLA is a continuing offence, which is why the statute of limitations only begins to run when the violation of Art. 38 AMLA ceases (i.e. as soon as there is no longer an obligation to mandate an auditor in accordance with Art. 15 AMLA, or an audit firm is (belatedly) appointed). 18

VIII. INSURABILITY

In practice, the **question sometimes arises as to whether insurance (e.g. professional liability insurance or directors' and officers' liability insurance, which cover pure financial losses and do not cover property damage or personal injury) can cover fines imposed under AMLA**. This question arises in particular from the fact that many insurers offer cover for penalties and fines imposed on a governing body (directors and officers liability insurance) or an employee (professional liability insurance). These extensions of cover are subject to the proviso that the insurance of such penalties and fines is legally permissible. Conversely, certain insurers explicitly exclude penalties or fines in their terms and conditions of insurance. 19

Within the limits of the mandatory provisions of the VVG and the restrictions on content pursuant to Art. 19 para. 2 and Art. 20 para. 1 CO in conjunction with Art. 100 VVG, insurers are in principle free to design their contracts as they wish. According to Art. 20 para. 1 CO, contracts are null and void if they have an impossible or unlawful content or are contrary to good morals. 20

21 According to case law, the **fine is of a highly personal nature**, which is why it is not accessible to a contractual agreement that obliges a third party to pay the fine in whole or in part, and is therefore unlawful within the meaning of Art. 20 para. 1 CO. It is to be qualified as a non-compensable reduction in the assets of the person fined under civil law. The same applies if someone is fined under criminal law due to their own fault. According to doctrine, there is an 'unwritten prohibition of coverage' with regard to the insurance of public law fines. In the doctrine, in connection with fines for data protection violations, it is sometimes argued that, depending on the insurance, it is possible to insure fines for negligence. Some hold the view that these fines can neither be insured nor passed on to the companies concerned, nor can they be paid by them. However, the question of whether AMLA or FADP fines can be insured has not been decided by the highest court.

22 In our opinion, the above-mentioned case law can be readily applied to fines under Article 38 AMLA. Fines under Article 38 AMLA do not constitute a compensable financial loss within the meaning of substantive liability law and **do not give rise to an insurance claim** under directors' and officers' liability insurance or professional liability insurance. The agreement of a financial obligation for fines pursuant to Art. 38 AMLA is **unlawful and therefore void** within the meaning of Art. 20 para. 1 CO. They are therefore not insurable and cannot be passed on to the insurance company. A corresponding claim for compensation by the policyholder against the insurance company would not be enforceable. Furthermore, the fines should remain strictly personal in accordance with Art. 38 AMLA, as otherwise the punitive function would be thwarted. A possible assumption of the fines by the insurance company could, under certain circumstances, be qualified as criminally relevant favouring in accordance with Art. 305 SCC. In our opinion, it is irrelevant whether the fine was imposed for intent (Art. 38 para. 1 AMLA) or negligence (Art. 38 para. 2 AMLA). One argument in favour of such a distinction is that Art. 14 VVG allows the insurer to refuse or reduce benefits in accordance with certain degrees of fault. The distinction based on the degree of fault could only be relevant for further compensation payments by the insurance company (e.g. advance of defence, court or expert costs), especially since standard market insurance conditions generally exclude intentional violation of legal provisions in any case. This exclusion is partly mitigated by the granting of legal protection, in that the insurance company bears the costs of defence, or by an extension of cover in the event of gross negligence, in that the insurance

company waives its right of reduction under Art. 14 para. 2 VVG. Finally, costs incurred by a dealer in connection with participating in criminal proceedings under Art. 38 AMLA are insurable. In our view, the same applies to legal costs imposed on a dealer; these are also insurable.

This article reflects the personal opinion of the authors and does not bind their employers.

BIBLIOGRAPHY

Delnon Vera/Rüdy Bernhard, Kommentierung zu Art. 305, in: Niggli Marcel A./Wiprächtiger Hans (Hrsg.), Basler Kommentar Strafrecht, Basel 2019 (zit. BSK-Delnon/Rüdy, Art. 305 StGB).

Eckert Martin, Wer wird bei Verstössen gegen das neue Datenschutzgesetz bestraft?, https://www.mme.ch/de-ch/magazin/artikel/wer-wird-bei-verstoessen-gegen-das-neue-datenschutzgesetz-bestraft, besucht am 31.8.2024 (zit. Eckert, Datenschutzverstösse).

Garbarski Andrew M./Macaluso Alain, Kommentierung zu Art. 37, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz, Basel 2021 (zit. BSK-Garbarski/Macaluso, Art. 37 GwG).

Hilf Marianne, Kommentierung zu Art. 38, in: Kunz Peter V./Jutzi Thomas/Schären Simon (Hrsg.), Stämpflis Handkommentar zum Geldwäschereigesetz (GwG), Bundesgesetz vom 10.10.1997 über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung, Bern 2017 (zit. SHK-Hilf, Art. 38 GwG).

Hutzler Doris, Strafrechtliche Verantwortlichkeit des Compliance Officers – it's happening!, in: Jean-Richard-dit-Bressel Marc/Zollinger David (Hrsg.), EIZ, 14. Schweizerische Tagung zum Wirtschaftsstrafrecht: Tagungsband 2023, Zürich 2024, S. 13–39 (zit. Hutzler, Verantwortlichkeit).

Nagel Thomas, Der persönliche und sachliche Geltungsbereich des schweizerischen Geldwäschereigesetzes: Mit rechtsvergleichenden Hinweisen zu internationalen Standards, dem Recht der Europäischen Union und dem deutschen Recht, Zürich et al. 2020 (zit. Nagel).

Mráz Michael, Kommentierung zu Art. 38, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz, Basel 2021 (zit. BSK-Mráz, Art. 38 GwG).

Ramelet Nicolas, Kommentierung zu Art. 15, in: Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz, Basel 2021 (zit. BSK-Ramelet, Art. 15 GwG).

Ramelet Nicolas, Geldwäschereibekämpfung bei Barzahlungsgeschäften – Staatliche Sterbehilfe für das Bargeld?, SZW 2016, S. 76–83 (zit. Ramelet, SZW 2016).

Rosenthal David/Gubler Seraina, Die Strafbestimmungen des neuen DSG, SZW 2021, S. 52–64 (zit. Rosenthal/Gubler, SZW 2021).

Specogna Rhea, Kommentierung zu Art. 100 Abs. 1, in: Grolimund Pascal/Loacker Leander D./Schnyder Anton K. (Hrsg.), Basler Kommentar Versicherungsvertragsgesetz, Basel 2023 (zit. BSK-Specogna, Art. 100 Abs. 1 VVG).

Trechsel Stefan/Pieth Mark, Kommentierung zu Art. 305, in: Trechsel Stefan/Pieth Mark (Hrsg.), Praxiskommentar StGB, Zürich 2018 (zit. PK-Trechsel/Pieth, Art. 305 StGB).

Wyss Ralph, Kommentierung zu Art. 15, in: Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano (Hrsg.), Orell Füssli Kommentar zum Schweizerischen Geldwäschereigesetz mit weiteren Erlassen (GwG), 3. Aufl., Zürich 2019 (zit. OFK-Wyss, Art. 15 GwG).

Zulauf Urs/Hutzler Doris, Der begründete und der einfache Verdacht: Ein Vorschlag zur Reform des Geldwäschereimeldewesens in der Schweiz, recht 4 (2019), S. 221–239 (zit. Zulauf/Hutzler, recht 2019).

MATERIALS

Amtliches Bulletin Nationalrat 2014, abrufbar unter https://www.parlament.ch/centers/documents/de/NR_4916_1412.pdf, besucht am 31.8.2024 (zit. AB 2014 NR 2014).

Amtliches Bulletin Ständerat 2014, abrufbar unter https://www.parlament.ch/centers/documents/de/SR_4916_1412.pdf, besucht am 31.8.2024 (zit. AB 2014 SR).

Botschaft zur Umsetzung der 2012 revidierten Empfehlungen der Groupe d'action financière (GAFI), BBl 2014 605 ff. (zit. Botschaft GAFI 2013).

EXPERTsuisse, Ausgewählte Fragen und Antworten zu den Auswirkungen der Anpassungen des Geldwäschereigesetzes auf die Prüfung von Händlerinnen und Händlern, 23.6.2016 (zit. EXPERTsuisse).