FMA

Document No.: 04/2022

Publication date: 23.02.2022

FMA CIRCULAR

on

REPORTING OBLIGATIONS

FOR THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

Version: February 2022

Disclaimer: This circular does not constitute a legal regulation. It is intended to serve as guidance and reflects the FMA's legal interpretation. No rights and obligations extending over and above the provisions of the law can be derived from circulars.

TABLE OF CONTENTS

1 INTRODUCTION

1 The objective, on an international level within the Financial Action Task Force (FATF) and on a European level in Directive (EU) 2018/843 (5th Anti-Money Laundering Directive), is to prevent the financial system from being used for the purpose of money laundering and terrorist financing. It is intended to counteract the flow of monies and virtual currencies of a criminal origin and monies and virtual currencies determined for terrorist purposes, by means of obliged financial market participants being required to observe certain due diligence and reporting obligations.

2 In Austria the due diligence and reporting obligations contained in the Financial Markets Anti-Money Laundering Act (FM-GwG; Finanzmarkt-Geldwäschegesetz[1]) and the supplementary permissions about the beneficial owner in the Beneficial Owners Register Act (WiEReG; Wirtschaftliche Eigentümer Registergesetz[2]) form the central elements for an effective system for the prevention of money laundering and terrorist financing in the financial market. Such a system may however only be effectively implemented, where the obliged entities under the FM-GwG co-operate accordingly by fulfilling the due diligence and reporting obligations assigned to them. The observance of due diligence and reporting obligations by the obliged entities not only serves for the preventive combating of money laundering and of terrorist financing, but also for assisting the work of the criminal prosecution authorities by way of repressive measures.

3 Is it only possible to prevent money launderers and persons financing terrorism from abusing the financial system for these purposes when obliged entities collect sufficient information on the identity of their customers and the economic beneficiaries (trustors, beneficial owners), about the purpose and the nature of the desired business relationship and about the origin of the funds used, to update this information regularly and to continuously monitor the business relationship. This should therefore place obliged entities in a position to detect anomalies in relation to their customers, and if required to stop the corresponding transactions and pass on the necessary information to the Financial Intelligence Unit (Geldwäschemeldestelle).

4 This circular does not constitute a legal regulation. It is intended to serve as guidance and reflects the FMA's legal interpretation. No rights and obligations extending over and above the provisions of the law can be derived from circulars.

5 Obliged entities under the FM-GwG are:

- credit institutions pursuant to Article 1 para. 1 of the Austrian Banking Act (BWG[3]) and CRR-credit institutions pursuant Article 9 BWG that provide activities in Austria through a branch;
- financial institutions pursuant to Article 1 para. 2 nos. 1 to 6 BWG;

[1] Financial Markets Anti-Money Laundering Act (FM-GwG; Finanzmarkt-Geldwäschegesetz), published in Federal Law Gazette I No. 118/2016 as amended.
[2] Beneficial Owners Register Act (WiEReG; Wirtschaftliche Eigentümer Registergesetz), published in Federal Law Gazette I No. 136/2017 as amended.
[3] Austrian Banking Act (BWG; Bankwesengesetz), published in Federal Law Gazette No. 532/1993 as amended.

- insurance undertakings pursuant to Article 1 para. 1 no. 1 of the Insurance Supervision Act 2016 (VAG 2016; Versicherungsaufsichtsgesetz 2016[4]) and small insurance undertakings pursuant to Article 1 para. 1 no. 2 VAG 2016 respectively within the scope of their life insurance operations (classes 19 to 22 pursuant to Annex A of VAG 2016));
- investment firms pursuant to Article 3 para. 1 of the Securities Supervision Act 2018 (WAG; Wertpapieraufsichtsgesetz 2018[5]) and investment services providers pursuant to Article 4 para. 1 WAG 2018;
- AIFMs pursuant to Article 1 para. 5 and Article 4 para. 1 of the Alternative Investment Fund Managers Act (AIMFG; Alternative Investmentfonds Manager-Gesetz[6]) and non-EU-AIFMs pursuant to Article 39 para. 3 AIFMG;
- electronic money institutions pursuant to Article 3 para. 2 E-Geldgesetz 2010[7];
- payment institutions pursuant to Article 10 of the Payment Services Act 2018 (ZaDiG 2018; Zahlungsdienstegesetz 2018[8]);
- the Austrian Post with regard to its money transaction services;
- financial institutions pursuant to points a) to d) of Article 3 (2) of Directive (EU) 2015/849 (4th Anti-Money Laundering Directive) with their place of incorporation in another Member State with business operations conducted through branches or branch establishments located in Austria as well as branches or branch establishments of such financial institutions that are authorised in third countries;
- wind-down units pursuant to Article 84 para. 2 of the Bank Recovery and Resolution Act (BaSAG; Bundesgesetz über die Sanierung und Abwicklung von Banken[9]) as well as Article 3 para. 4 of the Federal Act on the Creation of a Wind-down Unit (GSA; Bundesgesetz zur Schaffung einer Abbaueinheit[10]);
- wind-down entities pursuant to Article 162 para. 1 BaSAG in conjunction with Article 84 para. 2 BaSAG;
- virtual asset service providers pursuant to Article 2 no. 22 FM-GwG (MN 8).

6 A financial institution pursuant to Article 1 para. 2 nos. 1 to 6 BWG is an institution that is not a credit institution as defined in Article 1 para. 1 BWG, and which is authorised to provide one or

[4] Insurance Supervision Act 2016 (VAG 2016; Insurance Supervision Act 2016), published in Federal Law Gazette I No. 34/2015 as amended.
[5] Securities Supervision Act 2018 (WAG 2018; Wertpapieraufsichtsgesetz 2018), published in Federal Law Gazette I No. 107/2017, as amended.
[6] Alternative Investment Fund Managers Act (AIFMG; Alternative Investmentfonds Manager-Gesetz), published in Federal Law Gazette I No. 135/2013 as amended.
[7] Electronic Money Act 2010 (E-Geldgesetz 2010), published in Federal Law Gazette I No. 107/2010 as amended.
[8] Payment Services Act 2018 (ZaDiG 2018; Zahlungsdienstegesetz 2018), published in Federal Law Gazette I no. 17/2018, as amended.
[9] Bank Recovery and Resolution Act (BaSAG; Bundesgesetz über die Sanierung und Abwicklung von Banken), published in Federal Law Gazette I No. 98/2014 as amended.
[10] Federal Act on the Creation of a Wind-Down Entity (GSA; Gesetz zur Schaffung einer Abbaueinheit), published in Federal Law Gazette I No. 51/2014 as amended.

several of the activities listed in Article 1 para. 2 BWG on a commercial basis, provided that the institution conducts such activities as its principle activity. The principal activity as defined for the purposes of qualifying as a financial institution is to be identified based on the overall picture arising in the specific case in hand, i.e. taking into consideration all relevant factors of both qualitative and quantitative natures as well as criteria with regard to a flexible system. In any case, a principal activity shall be assumed to exist, in the case that the activity contributes 50 % to the entity's performance.[11] In addition, the existence of a principal activity is not only to be assessed purely based on the contribution of the activity to the entity's performance - i.e. a purely quantitative feature. Instead, whether an activity of an undertaking is a principal activity or whether this activity "*due to its close relationship to the principal activity and due to its subordinate significance in comparison to the principal activity in accordance with public opinion appears to be comparable*"[12] is the case, based on an overall picture of the case in hand based on qualitative features. As part of a flexible system, the business plan and business strategy, the deployment of resources, returns, acquisitions, marketing etc. must be considered in doing so. [13] It should focus on whether a specific activity *"by way of its nature has an autonomous character or is purely of an ancillary nature to the undertaking's other […] activities"*.[14] It should be noted in this context that the definition is based on the commercial law interpretation of the principal activity and that an undertaking may not necessarily only have one principal activity.[15]

7 For the provision of safe deposit services pursuant to Article 1 para. 2 no. 6 BWG, joint control by the entity is not a compulsory condition, provided certain security obligations - especially including access control - are observed.[16]

8 A virtual asset service provider is any natural or physical person resident/domiciled in Austria or providing a service on a commercial basis for third parties in Austria pursuant to Article 2 no. 22 FM-GwG in relation to virtual currencies pursuant to Article 2 no. 21 FM-GwG. It also covers virtual asset service providers domiciled in another EU Member State or in a third country that actively offers or provides a service pursuant to Article 2 no. 22 FM-GwG in Austria.

9 Where designations used refer to natural persons, the formulation used applies to both genders.

[11] Supreme Administrative Court (VwGH) 10.11.2017, Ro 2017/02/0023 citing further literature.
[12] Federal Administrative Court (BVwG) 02.08.2017, W230 2150836-1 citing further literature; VwGH 24.10.2018, Ro 2017/02/0025.
[13] The corporate identity, company name and the activity advertised on the undertaking's website may be taken into consideration in the assessment. Furthermore, it must also be taken into account, whether *"other items, other assets, another organisation and measures are necessary"* for the performance of the activity in questions (BVwG 02.08.2017, W230 2150836-1).
[14] Federal Administrative Court (BVwG) 02.08.2017, W230 2150836-1 citing further literature.
[15] In this case also Federal Administrative Court (BVwG) 02.08.2017, W230 2150836-1.
[16] Supreme Administrative Court (VwGH) 10.11.2017, Ro 2017/02/0023.

2 FROM BECOMING AWARE OF THE ANOMALY THROUGH TO REPORTING IT

2.1 Anomalies

10 Various constellations are listed in MN 12 et seq. as guidance in relation to businesses, transactions and business relationships, which are to be considered as being "anomalous" by obliged entities, and which trigger a reporting obligation where their plausibility is unable to be checked.

11 Corresponding constellations are generally recognised by the obliged entities. They regularly come to light either directly in relation to customer contact, such as in the process of establishing the business relationship or when updating Know Your Customer (KYC) information or as part of the ongoing monitoring of the business relationship[17] using automated monitoring systems and/or manual checks.

12 An anomaly in particular exists when the actual customer and/or transactional conduct deviates from the expected conduct based on the submitted information, data and documents. Anomalies may for example arise from monitoring actions conducted manually or by automated means.

13 In light of this there is a necessity for obliged entities to internally determine and to train accordingly about, for example

- what is considered as "anomalous",
- what steps employees have to take, in the case that they observe anomalies,
- when and/or how the Anti-Money-Laundering Officer is to be involved, or
- how the anomaly is to be documented.

14 Examples of anomalies with regard to business relationships, businesses and/or transactions include:

- exerting time pressure in the conclusion of the transaction;
- legal constructions with particular complexity, the ownership or control relationships of which are difficult to explain or comprehend;
- refusal to provide typical information without stating any reasons;
- discrepancies between the person acting and the business, e.g. where the intended transaction does not match the customer's profile with regard to their age or knowledge;

[17] See the FMA Circular on "Due diligence obligations for the Prevention of Money Laundering and Terrorist Financing", published February 2022, MN 225ff.

- ostentatious behaviour by the customer e.g. change of lifestyle, unexpected and unsuitable changes of business;
- customers that make false or misleading statements;
- incorrect or implausible statements about trust transactions;
- customers obviously avoiding direct contact to the obliged entity, or ostentatiously seeking contact to specific staff members;
- business dealings and transactions, which do not pursue any apparent financial purpose;
- business dealings that do not appear plausible due to the considerable geographic distance between the obliged entity and the place of residence or headquarters of the customer;
- business deals involving countries that provide constructions under company law that make it difficult to determine and verify the origin of funds and in which, accordingly to credible sources, there is an increased risk of money laundering and terrorist financing;
- transfers from virtual currencies, for which the origin of funds is unable to be checked (e.g. decentralised "unhosted software wallets or hardware wallets", using "mixing services", using "privacy coins", etc.);
- business deals with legal persons or constructions that have the purpose of wealth management, in which additional potential risk factors exist e.g. international interdependencies or a large degree of anonymity of the beneficial owner;
- transfers of virtual currencies from and to wallets that have a link to decentralised "peer-to-peer networks" (e.g. decentralised trading or exchange platforms); without a plausible explanation e.g. a connection to a business activity;
- customers undertaking exchange services on decentralised exchange platforms (peer-to-peer);
- transfers from and to "hot wallets" where the domain cannot be unambiguously allocated to the owner of the wallet or the wallet's custodian (e.g. using a "proxy server", or a VPN);
- making use of complex ("off-shore") company constructions that prevent the beneficial owner from being clearly identified;
- repeated transactions or contracts being concluded for amounts that are just under the threshold for identification requirements ("smurfing");
- a lack of or incomplete details about the payer of payment orders;
- a lack of or incomplete details about the payers of payment orders and the recipient in the case of transfers involving virtual currencies;
- large amounts of collateral in cash or early high repayments in the case of loans without any plausible explanation about the origin of such assets;
- unusual cash transactions;

- unusual cash transactions in relation to virtual currencies (e.g. unusual intervals and volumes when exchanging fiat money in cash at ATMs);
- frequent and unexplained transfers from accounts to different obliged entities or switching to new contracts;
- increased transfer/exchanging of virtual currencies from and to or using various virtual asset service providers (VASPs), especially ones incorporated in a non-equivalent (third) country;
- transfers from fiat money into virtual currencies and vice versa, which are associated with a loss of value or higher charges as applicable without any plausible explanation;
- movements of funds that are incongruous to the customer's financial background;
- deviations in actual customer behaviour from the expected customer behaviour, e.g. in relation to transactions and types of transaction actually conducted;
- frequent and unexplained movements of funds between obliged entities in different locations;
- exchanging large amounts of low-denomination banknotes into high denomination banknotes (or vice versa);
- exchanging virtual currencies into different types of virtual currencies, especially into anonymous virtual currencies;
- making use of "mixing services" and anonymous virtual currencies within the scope of a business relationship or single transactions;
- virtual currency transfers being made to an "unhosted wallet" without the wallet owner's knowledge;
- receiving and transferring virtual currencies from and to wallets for which there are apparent anomalies (e.g. connection to incriminating acts, online marketplaces and trading venues, incriminated persons etc.);
- using anonymous prepaid cards for exchanging fiat money into virtual currencies and direct transfers to various exchange platforms or to "unhosted wallets" without plausible explanation;
- large projects both in Austria as well as abroad, for which the majority of the funding has been secured from unnamed investors, or for which high levels of equity capital are offered, where its origin is not explained in a plausible manner;
- large-scale trading business, which for example are only settled financially in Austria by means of opaque international company networks, and for which the flow of goods cannot be traced or checked from Austria.

- export and import financing of high-risk goods[18] or exports to countries upon which sanctions, embargoes or similar measures by international organisations have been enforced in the area of prevention of money laundering and terrorist financing;
- transactions, in which securities are purchased for a high price and are sold at a considerable loss;
- buying and selling unlisted securities with a large difference in price within a short timeframe;
- activation of dormant accounts without any plausible reason;
- opening and subsequently closing "hosted wallets" and "unhosted wallets" shortly thereafter without any plausible reason;
- an expensive restructuring of transactions without any discernible reason for doing so;
- insurance contracts with customers, whose principle place of residence is not in the country in which the business relationship is based, and are unable to provide a plausible financial link;
- high one-off premiums on life insurance policies (especially in conjunction with early redemptions);
- insurance contracts with legal persons or constructions with the purpose of wealth management, where additional potential risk factors e.g. international interdependencies occur;
- unusually high transactions not being conducted from the account;
- high premium payments compared to the customer's other financial circumstances;
- a lack of sensitivity to costs arising from the redemption of life insurance contracts;
- payments that exceed the agreed premium;
- little interest in the yield of the transaction;

15 Furthermore, anomalies may also become apparent from external information sources (e.g. from media reports, warnings through the goAML application (see MN 71), feeds or similar items).

2.2 Plausibility assessment of the anomaly

16 Where anomalies are observed by an obliged entity, then they must be analysed accordingly. A suspicious activity report must be submitted without delay, where suspicion or a justified reason to assume pursuant to Article 16 para. 1 FM-GwG already exists on the basis of this analysis.

17 Where the circumstances are not resolved adequately, then further investigative steps or actions are necessary to check the plausibility of the anomaly. Furthermore, the measures prescribed by the law must be taken where applicable (e.g. classification in a higher risk class and as a follow-

[18] For example the goods that are covered in Article 1 point 44 lit. b) sublit. ii) of Directive (EU) 2015/849 as amended by Directive (EU) 2018/843 (including among others: oil, arms, luxury goods etc.)

up enhanced ongoing monitoring of the business relationship). All actions from the detection of the anomaly, through to the potential checking of its plausibility, or the submission of a suspicious activity report, must be documented in a transparent manner as well as to an extent that is proportionate to the circumstances of the case-in-hand. The obliged entity is responsible for the nature and manner of the documentation.

18 During such auditing steps or activities, the obliged entity must check to what extent the plausibility of an anomaly may be checked against the background of the specific KYC information held about the customer or other specific information that has been supplied. Where necessary, further information and documentation should be obtained to allow a plausibility check to be conducted. For example, the (conclusive) representation of the customer regarding the origin of funds must be checked using appropriate documentation with regard to the origin of funds, such as in the case that the customer wishes to invest an unusually high amount with the obliged entity and states that the money originates from an inheritance or from savings.

19 Regarding the documentation to be gathered, particular attention must be paid that the documentation fulfils appropriate quality criteria. This means that there must be no doubts about its authenticity, while simultaneously also being suitable both in terms of its content as well as its context in terms of timing to support the customer's version of the facts.

20 Furthermore, the gathering of such documentation or any follow-up to do so must occur promptly, in a manner that is appropriate for the case in hand, and the specific steps taken by the obliged entity must be documented in a comprehensible manner. A timeframe for example of several months, in which the obliged entity follows up at regular intervals, but where however the customer is not reachable and/or is not willing to cooperate in the checking of the plausibility of the anomaly, shall be considered in any case by the FMA to be inappropriate or too long.

21 It is necessary to differentiate between the obligation to submit a suspicious activity report "without delay" and the amount of time an obliged entity is given to check the plausibility of an anomaly. From the instant where knowledge, suspicion or justified reason to assume pursuant to Article 16 para. 1 FM-GwG exists, the suspicious activity report shall in any case be submitted "without unnecessary delay" or "without undue delay". In practice, this means that suspicious activity report must be made as soon as possible, ideally on the same day, but within a few working days in any case (e.g. taking into consideration the specific organisational structure) from the time at which knowledge of, suspicion of, or the justified reason to assume have manifested themselves.

22 Where a plausibility check cannot be conducted, at least a justified reason to assume as defined in Article 16 para. 1 FM-GwG shall be assumed and a suspicious activity report made (cf. MN 29 ff).

23 Otherwise, please refer to Article 7 para. 7 FM-GwG, which stipulates that obliged entities

- shall not perform any transaction using a bank account,
- shall not establish any business relationship, and

- shall not conduct any transactions, or
- must terminate already existing business relationships,

where they fail to observe or are unable to observe their due diligence obligations in relation to the identification of the customer, the beneficial owner and the trustor/trustee as well the gathering of KYC information including information relating to the origin of funds (cf. Article 6 para. 1 nos. 1 to 5 FM-GwG).

Accordingly, with regard to life insurance contracts, insurance undertakings shall not be allowed to establish a business relationship and to conduct any transaction if they fail or are unable to observe their due diligence obligations towards a customer or a beneficiary, while occupational severance funds shall not be allowed to conduct any transaction if they fail or are unable to observe their due diligence obligations towards a customer.

Pursuant to Article 6 para. 1 no. 6 FM-GwG (ongoing monitoring of the business relationship including the checking of transactions conducted during the course of the business relationship) a transaction may be delayed until the necessary investigative steps have been concluded (cf. FMA Circular on the due diligence obligations for the prevention of money laundering and terrorist financing, version from February 2022, MN 225ff).

In the cases listed in Article 7 para. 7 FM-GwG, the obliged entities shall consider submitting a suspicious transaction report in relation to the customer in accordance with Article 16 FM-GwG to the Financial Intelligence Unit (Geldwäschemeldestelle). In such cases, where obliged entities are unable to conduct plausibility checks, a suspicious activity report must be submitted where there are justified reasons for assumption as defined in Article 16 para. 1 FM-GwG (cf. also MN 29 et seq.)

3 REPORTING OBLIGATIONS

3.1 Triggering of the reporting obligation

24 Pursuant to Article 16 para. 1 FM-GwG obliged entities shall submit a suspicious activity report without delay of their own accord, in the case that they "know, suspect or have reasonable grounds to suspect" that

- (no. 1) an attempted, upcoming, ongoing or previously conducted transaction is related to assets originating from one of the criminal activities listed in Article 165 StGB (including assets which stem directly from a criminal act on the part of the perpetrator) (MN 36 et seq.);
- (no. 2) an asset originates from one of the criminal activities listed in Article 165 StGB (including assets which stem directly from a criminal act on the part of the perpetrator; MN 45 et seq.)
- (no. 3) a customer has violated the obligation to disclose trust relationships pursuant to Article 6 para. 3 (MN 47 et seq.); or
- (no. 4) the attempted, upcoming, ongoing or previously conducted transaction or the assets are connected to a criminal organisation pursuant to Article 278a StGB, a terrorist organisation pursuant to Article 278b StGB, a terrorist crime pursuant to Article 278c StGB or terrorist financing pursuant to Article 278d StGB (MN 49 et seq.)

25 Apart from the cases listed in Article 16 para. 1 FM-GwG (cf. MN 24) reporting obligations also arise pursuant to Article 16 para. 3 FM-GwG in relation to all applications for having savings deposits paid out where the identity of the customer has not been determined for the savings deposit and the pay-out is intended to occur for a savings deposit, that has a credit balance of at least EUR 15 000 (or equivalent) (cf. MN 57 et seq);

26 Furthermore, pursuant to Articles 9 and 13 of Regulation (EU) 2015/847, when assessing whether a transfer of funds or a related transaction is suspicious and whether it is required to be reported to the Financial Intelligence Unit (Geldwäschemeldestelle) it is necessary to consider whether the information about the payer or payee are missing or incomplete (cf. MN 66);

27 Where it is not possible to observe the due diligence obligations regarding the identification of the customer, the beneficial owner or the trustor/trustee and the gathering of KYC information as well as information about the origin of funds, the obliged entities shall consider pursuant to Article 7 para. 7 in conjunction with Article 6 para. 1 nos. 1 to 5 FM-GwG the submission of a suspicious activity report pursuant to Article 16 FM-GwG to the Financial Intelligence Unit (Geldwäschemeldestelle) (cf. MN 69).

28 It should be noted that the risk-based approach pursuant to Article 6 para. 5 FM-GwG – only applies to the scope of the due diligence obligations to be applied by the obliged entities pursuant to Article 6 paras. 1 to 3 FM-GwG, but does not apply to Article 16 FM-GwG.

3.2 Suspicion vs reasonable grounds to assume

29 Article 16 para. 1 FM-GwG stipulated three different possibilities:

- knowledge of a circumstance subject to a reporting requirement,
- the suspicion that a circumstance subject to a reporting requirement exists and
- Reasonable grounds to assume that a circumstance exists that is subject to a reporting requirement,

30 Already from the wording of Article 16 para. 1 FM-GwG (*"[…] know […] suspect […] or have reasonable grounds to suspect […]"*) it is possible to see that there are three alternative "reporting thresholds". It therefore follows that the formulations "suspect" and "have reasonable grounds to suspect" are not to be understood as being synonymous with one another.

The lowest of these thresholds for an obligation to submit a suspicious activity report ("reporting threshold" is having "reasonable grounds to suspect". An obligation for the obliged entities to make a report is triggered as soon as this threshold is reached. Practical experience has shown that this is the most frequent case of application for obliged entities or that most issued are connected to such constellations.

31 This – lowest – threshold is already reached when the obliged entities become aware of anomalous circumstances existing, and where it is not possible to conduct a plausibility check (cf. MN 22). Depending on the situation in the specific case in hand, a factual situation (that is either anomalous or which does not allow plausibility to be checked) or a combination of multiple such factual circumstances may constitute such "reasonable grounds to assume".

32 Consequently, "reasonable grounds to assume" may also exist as defined in Article 16 para. 1 FM-GwG, where an anomaly is unable to be clarified in an understandable way, or is not clarified in an understandable way.

33 In such a case, an obliged entity shall estimate, based on its experience and the objective circumstances, the extent to which the plausibility of an anomaly may be resolved by other explanations given by the customer or proved as being plausible based on the documents submitted. It is not necessary for the obliged entity to conduct a (conclusive) appraisal in terms of criminal law of the factual circumstances.

34 When estimating whether circumstances exist, for which there are reporting obligations, the focus should not be on an obliged entity's subjective feeling, but instead how an obliged entity acting in accordance with the law would assess such circumstances in accordance with the FM-GwG. In the case that an obliged entity acting in accordance with the law ought under objective criteria to have had reasonable grounds to assume as defined in Article 16 para. 1 FM-GwG, but nevertheless fails to submit a report, then it commits the legal offence of a breach of reporting obligations.[19]

[19] In this case also UVS-06/FM/46/15241/2012.

3.3 Reporting obligations pursuant to Article 16 FM-GwG

35 The reporting obligations pursuant to Article 16 para. 1 nos. 1 to 4 and para. 3 FM-GwG are addressed individually as well as aspects to be taken into consideration in this regard:

3.3.1 Transactions involving assets originating from punishable offences under Article 165 StGB

36 Where obliged entities know, or where a suspicion or justified grounds exist to assume, that an attempted, upcoming, ongoing or previously conducted transaction involves assets originating from one of the criminal activities listed in Article 165 StGB (including assets resulting directly from a criminal act on the part of the perpetrator) then a suspicious activity report pursuant to Article 16 para. 1 no. 1 FM-GwG must be made.

37 Article 165 of the Austrian Criminal Code (StGB; Strafgesetzbuch)[20] defines the criminal offence of money laundering. It differentiates primarily between predicate offences (cf. para. 1 no. 1 and 2 para. 2 leg cit.) and organisational money laundering (para. 3 leg. cit.).

38 Under Article 165 para. 1 nos. 1 and 2 or para. 2 StGB, anyone who,

- converts or transfers assets derived from criminal activity to another person with the intent of concealing or disguising their illegal origin, or to assist another person involved in such criminal activity, so that they escape the legal consequences of their action (para. 1 no. 1), or
- conceals or disguises the true nature, origin, location, disposition or movement of property derived from criminal activity (para. 1 no. 2);
- acquires, otherwise takes possession of, possesses, converts, transfers to another person or otherwise uses assets, in the case that at the time of acquisition they know that they originate from a criminal activity of another person (para. 2);

shall be criminally liable.

39 Article 165 para. 5 defines three categories of predicate offences as criminal activities in the cited money laundering provision ("predicate offences"), thereby basically adopting the predicate offence catalogue of the predecessor provision:

- an offence that carries a custodial penalty of more than one year's imprisonment ("general threshold for predicate offences"),
- specific offences in accordance with the StGB, namely those pursuant to Articles 223, 229, 289, 293 and 295 StGB [counterfeiting of legal documents, suppression of legal documents,

[20] Published in Federal Law Gazette 1974/60 as amended by Federal Act in Federal Law Gazette I 2021/159; Amended version of the money laundering provision transposing Directive (EU) 2018/1673 on combating money laundering by criminal law (ML Criminal Law Directive) OJ L 284, 12.11.2018; entry into force 01.09.2021.

false testimony to an administrative authority, counterfeiting of evidence, suppression of evidence], or

- specific offences in accordance with the Narcotic Substances Act (SMG; Suchtmittelgesetz) specifically pursuant to Articles 27 and 30 SMG [illegal handling of narcotics and illegal handling of psychotropic substances],

where they:

- are subject to Austrian criminal laws, and were committed unlawfully (no. 1 leg. cit.), or
- were committed abroad, without being subject to Austrian criminal laws, but fulfil the elements of an act punishable by a court under both Austrian criminal laws and - unless they are certain offences[21] described in greater detail in the cited provision - under the laws of the place where the offence was committed, and were committed unlawfully. It is neither necessary that the offender is able to be convicted of the criminal activity, nor that all elements of the factual elements or all circumstances in connection with this activity, such as the identity of the perpetrator, are established (no. 2 leg. cit.).

40 As a result, all criminal offences are still considered predicate offences of money laundering, provided that they are punishable - either by the StGB itself or the corresponding penal provisions in other laws - with a custodial sentence of more than one year. Consequently, all financial crimes that fall within the competence of the courts in any case constitute a predicate offence, since they either bear the primary or abstract threat, in addition to fines, of a custodial sentence of longer than one year. By explicitly citing Articles 27 and 30 SMG in Article 165 para. 5 StGB, not only are such constellations captured that would already have been covered by the general threshold for predicate offences, but also for example those listed in Article 27 paras. 1, 2 and 5 SMG, even though they have lower penalties.[22]

41 Assets constitute the object of the offence in Article 165 StGB. Under para. 6 leg. cit., this covers assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible), and legal documents or instruments in any form, including electronic or digital, evidencing title to, or an interest in, such assets; units of virtual currencies and their appreciation or rights attached to them, but not mere savings, such as unrealised losses, forgiven debts or saved expenses and charges.

42 Under para. 7 leg. cit., an asset is considered to have been the proceeds of a criminal activity where the perpetrator of the criminal activity received it through the offence or in order to

[21] Article 165 para. 5 no. 2 StGB contains the following insertion: "*… provides that they are not actions in accordance with Article 2 no. 1 lits. a to e and h of Directive (EU) 2018/1673 on combating money laundering by criminal law, OJ L 284, 12.11.2018, p. 22, and applicable Union law …*" The predicate offences listed in the law from the catalogue listed in Article 2 no. 1 of the Directive on combatting money laundering by criminal law are offences in the area of participation in an organised criminal group and racketeering, terrorism, traffic in human beings and smuggling, sexual exploitation, as well as illicit trafficking of drugs and corruption, where such offences are listed under EU law. See also explanatory remarks to the government bill (ErlRV) no. 849 in the supplements to the stenographic protocols of the National Council (BlgNR) for the 27th legislative period, p. 10 et seq.

[22] Cf. explanatory remarks to the government bill (ErlRV) no. 1621 in the supplements to the stenographic protocols of the National Council (BlgNR) for the 25th legislative period, which relates to the predecessor provision, but which remains meaningful in terms of content.

commit the offence, or if the asset represents the value of the originally obtained or received asset.

43 For the sake of completeness, we refer to the fact that money laundering is only subject to a predicate offence in the cases listed in Article 165 para. 1 nos. 1 and 2 or para. 2. In addition to money laundering in relation to a predicate offence, based on the general reference contained in Article 16 para. 1 FM-GwG to Article 165 StGB, organisational money laundering (cf. MN 36) is also relevant:

Pursuant to Article 165 para. 3 StGB, anyone who acquires assets subject to the power of disposition by a criminal organisation (Article 278a StGB) or a terrorist organisation (Article 278b StGB) on its behalf or in its interest, or which otherwise takes possession of, possesses, converts, transfers to another or otherwise uses the asset, is liable to prosecution if they know of this power of disposition at the time of obtaining the asset.

44 The object of the offence in para. 3 leg. cit. is therefore an asset (cf. MN 41), that is subject to the power of disposal of a criminal organisation or a terrorist organisation. Assets are covered, for example, which the organisation may dispose of through its members, through nominees, dummy companies, or legal undertakings that it controls. In addition to proceeds from criminal activity, the assets may also include assets obtained by legal means.[23]

3.3.2 Assets from a criminal activity listed in Article 165 StGB

45 Where obliged entities know, or where there is a suspicion or justified grounds to assume that assets originate from a criminal activity listed in Article 165 StGB (including assets originating directly from a criminal act on the part of the perpetrator) then a suspicious activity report must be made pursuant to Article 16 para. 1 no. 2 FM-GwG.

46 With regard to the general remarks about Article 165 StGB, please see MN 37 et seq.

3.3.3 Disclosure breaches in relation to trusteeships

47 Where obliged entities know or where a suspicion or justified grounds to assume exist that the customer has acted contrary to the disclosure obligations with regard to trust relationships pursuant to Article 6 para. 3 FM-GwG, then a suspicious activity report must be made pursuant to Article 16 para. 1 no. 3 FM-GwG.

48 For example, this is the case when the customer denies the existence of a trust relationship, fails to disclose any change to such an arrangement while the business relationship is being conducted or states the wrong person as trustor (for deals about how obliged entities are required to proceed in conjunction with trust relationships, please see the FMA Circular on Due Diligence

[23] In this respect, where still valid in the author's opinion, Kirchbacher in Höpfel/Ratz, WK² StGB § 165 (as of 1.9.2011, rdb.at), MN 10/2; for further information on the elements of the offences and the offences of the (also partly conceptually) newly formulated Article 165 StGB, see also the explanatory remarks to the government bill (ErlRV) no. 849 in the supplements to the stenographic protocols of the National Council (BlgNR) for the 27th legislative period, p. 10 et seq.

Obligations for the Prevention of Money Laundering and of Terrorist Financing, Version: February 2022, MN 112 et seq.)

3.3.4 Transactions or assets in conjunction with a criminal organisation, a terrorist organisation, a terrorist offence or terrorist financing

49 Where obliged entities know, suspect or have reasonable grounds to assume that the attempted, upcoming, ongoing or previously conducted transaction or the assets are related to a criminal organisation pursuant to Article 278a StGB, a terrorist organisation pursuant to Article 278b StGB, a terrorist crime pursuant to Article 278c StGB, or terrorist financing pursuant to Article 278d StGB, then a suspicious activity report must be submitted pursuant to Article 16 para. 1 no. 4 FM-GwG.

50 This obligation refers both to transactions by a terrorist, who belongs to a terrorist organisation, as well as those by a third party that are intended for a terrorist or a terrorist organisation.

51 Article 278a StGB penalises the establishment of a criminal organisation or the participation as a member of one. A criminal organisation is a longer-term business-like association of a larger number of people, which, even if not exclusively, aims to repeatedly and deliberately commit serious offences, that threaten life, physical integrity, liberty or prosperity, or serious offences in relation to sexual exploitation of persons, human trafficking or trafficking of weapons, nuclear material and radioactive material, hazardous waste, counterfeit money or illicit drugs (no. 1), which seeks to achieve significant financial gain through such activities (no. 2), and which seeks to corrupt or intimidate others, or to shield itself from law enforcement measures in specific ways (no. 3).

52 Article 278b StGB penalises the directing of a (para. 1 leg. cit.) or the participation as a member of a (para. 2 leg. cit.) terrorist organisation. According to para. 3 leg. cit., a terrorist organisation is a longer-term affiliation of more than two persons, where one or more terrorist offences pursuant to Article 278c are committed by one or more members of this terrorist organisation or performs terrorist financing (Article 278d).

53 Article 278c para. 1 StGB punishes the committing of terrorist offences. These consist of the offences listed in Article 278c para. 1 (including specific offences against life and limb, e.g. murder or offences relating to physical injury, serious damage to property and damage to data, and where by doing so the life of another person or property of others is threatened to a large extent, deliberate crimes against public safety etc.), where such offences are capable of disrupting public life severely or for a longer period of time, or lead to severe disruption to economic activity and are committed with the intent of severely intimidating the population, public bodies, or an international organisation to coerce them to commit, tolerate or refrain from an act or to severely shake or destroy the political, constitutional, economic or social foundations of a State or an international organisation.

54 Article 278d para. 1 StGB punishes the provision or collection of funds with the intention of using them, even only partially, to conduct terrorist offences listed in Article 278d StGB (e.g. hijacking an aeroplane, or deliberately endangering aviation safety, kidnapping for ransom or threatening

to do so). According to Article 278d para. 1a StGB similar penalties also apply to anyone providing or collecting funds for another person they know to commit the acts listed in para. 1, or a member of a terrorist organisation, about which they know that the organisation has been established to commit acts in accordance with para. 1.

55 Financial means for the financing of terrorism may also originate from legal sources.

3.3.5 Further obligations in conjunction with terrorist financing

56 The group of persons connected with terrorist activities or preparatory activities will be announced by means of a publication. Obliged entities should in particular take notice of four sources:

- EU Regulations: EU Regulations are updated on an ongoing basis and prohibit the settlement of transactions with specific persons and groups in conjunction with the implementation of the UN Security Council's Resolutions on the prevention of terrorism and terrorist financing.
- Announcements by the OeNB in relation to the Foreign Exchange Act (DevG; Devisengesetz); these may be accessed (in German only) through the following link: https://www.oenb.at/Ueber-Uns/Rechtliche-Grundlagen/Verordnungen-nach-DevG.html
- OeNB Regulations in relation to the Sanctions Act (SanktG; Sanktionsgesetz); these may be accessed (in German only) through the following link: https://www.oenb.at/Ueber-Uns/Rechtliche-Grundlagen/Verordnungen-nach-SanktG.html
- OeNB Guidance on the freezing of assets; this may be accessed through the following link: https://www.oenb.at/Ueber-Uns/Rechtliche-Grundlagen/Finanzsanktionen/Terrorismusfinanzierung.html

In this context, we would advise persons who are not explicitly listed in the aforementioned publications. Irrespective of any publication being made, a reporting obligation is always triggered, where the justified reason to assume exists as defined in Article 16 para. 1 FM-GwG (cf. especially MNs 45 or 49 et seq.)

3.3.6 Savings deposits

57 Credit institutions are required to inform the Financial Intelligence Unit (Geldwäschemeldestelle) pursuant to Article 16 para. 3 FM-GwG without delay about all requests for paying out of savings deposits, where

- the customer's identity has not yet been determined for the savings deposit, and
- the pay-out is intended to be made from a savings deposit with a credit balance of at least EUR 15,000 or euro equivalent value.

58 This obligation to make a report shall exist irrespective of there being a suspicion or justification reason to assume. Pay-outs from such savings deposits shall only be made upon expiry of a period of seven calendar days following the request for the pay-out, unless the Financial Intelligence

Unit (Geldwäschemeldestelle) orders a longer period institution shall assign pursuant to Article 17 para. 4 FM-GwG.

59 When conducting a simple identification process in relation to a savings deposit that has the aforementioned characteristics, without a request for pay-out having been made, it should be checked on the basis of the circumstances of the specific case in hand, whether a suspicious activity report is required to be made. Identification following the acquisition of savings certificates following a death occurring may therefore, although not necessarily, automatically lead to a suspicious activity report being submitted. However, such a report must be submitted where anomalies exist regarding the origin of funds, the amount concerned, links to foreign countries etc.

60 Where the impression exists that a reporting obligation is intended to be deliberately bypassed due to the separation in time of the identification and the request for a pay-out, by initially only conducting the identification check, and with the request for a pay-out only occurring following considerable delay, the submission of a suspicious activity report must then be considered.

3.3.7 Non-Cooperative Countries or Territories

61 There are particular reporting obligations for obliged entities in relation to non-cooperative countries or territories. Under Article 12 para. 3 FM-GwG, the designation “non-cooperative countries” is used for those countries that fail within their national territory or other locations in their jurisdiction to take the necessary actions in accordance with international standards against money laundering. A violation of international standards shall in particular be assumed pursuant to the second sentence of Article 12 para. 3 FM-GwG in such cases where the Council of the European Union or the Financial Action Task Force on Money Laundering have adopted resolutions to this effect. A list of such States is published by way of a Regulation.

62 At the time of this FMA Circular being drawn up, the corresponding Regulation has not yet been issued. Obliged entities shall be required to ensure that their level of knowledge with regard to non-cooperative countries is up-to-date. In the case that the corresponding Regulation is issued, then this will also be published on the FMA website.

63 In relation to non-cooperative countries where the corresponding Regulation exists as referred to in MN 62 pursuant to Article 12 para. 4 no. 5 FM-GwG, all transactions for an amount of at least Euro 100 000 or its Euro equivalent shall be required to be reported to the Financial Intelligence Unit (Geldwäschemeldestelle), where

- the originator or beneficiary is a person domiciled or resident in a non-cooperative country or territory, or
- transactions are conducted to or from an account held at a foreign credit institution or financial institution incorporated in a non-cooperative country or territory.

64 This reporting obligation applies irrespective of whether the transaction is carried out as a single operation or in multiple obviously connected operations; in cases where the amount is unknown

at the start of a transaction, the report must be submitted as soon as the amount is known and it is established that the total will be at least EUR 100 000 or equivalent value.

3.3.8 Regulation (EU) 2015/847 - "Transfer of Funds Regulation" (ToFR)

65 Regulation (EU) 2015/847 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (The Transfer of Funds Regulation ("ToFR")) obliges payment service providers, to submit certain information about the payer (Article 4 (1) ToFR) and the payee (Article 4 (2) ToFR) when making a transfer of funds. Intermediary payment service providers must ensure that all information that they have received on the payer and payee and which is submitted together with the transfer of funds is retained with the transfer when transmitted onwards (Article 10 ToFR).

66 Article 9 and 13 ToFR respectively stipulate when assessing whether a transfer of funds or a related transaction is suspicious and therefore must be reported to the Financial Intelligence Unit (Geldwäschemeldestelle), that one factor to be taken into account by the payment service provider or the intermediary payment service provider, is whether information is missing or incomplete about the payer or payee.[24]

67 Furthermore, Article 8 (2) and Article 12 (2) ToFR stipulate that there is a reporting obligation by the payee's payment service provider or by the intermediary payment service provider to the FMA, in the event that a payment service provider repeatedly fails to submit the prescribed information about the payer or the payee. In such cases, in addition to reports about such failings, reports must also be made regarding the actions taken in this regard by the party subject to the reporting obligation (e.g. issuing a warning, setting a deadline, rejecting all future transfer orders from this payment service provider, restriction or termination of the business relationship to this payment service provider).[25]

68 The Transfer of Funds Regulation (ToFR) also applies in the same way for the transfer of virtual currencies.

3.3.9 Other

69 Where obliged entities fail or are unable to observe their due diligence obligations pursuant to Article 6 para. 1 nos. 1 to 5 FM-GwG (i.e. In relation to the identification of the customer, the beneficial owner or a trustor/trustee as well as the purpose and nature of the business relationship or the origin of funds) towards a customer, then they are required to "consider" pursuant to Article 7 para. 7 FM-GwG submitting a suspicious activity report pursuant to Article 16 FM-GwG (see MN 23 about the other legal consequences of Article 7 para. 7 FM-GwG).

[24] In this regard, we also refer to the EBA Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849, repealing and replacing the Joint Committee Guidelines JC/2017/37, March 2021 (EBA/GL/2021/02).

[25] A separate reporting form is available on the FMA's Incoming Platform for submitting such a report pursuant to Article 8 (2) and/or Article 12 (2) ToFR to the FMA.

4 SUSPICIOUS ACTIVITY REPORTS

4.1 Competent authority

70 Suspicious activity reports pursuant to Article 16 para. 1 FM-GwG are to be submitted to the Financial Intelligence Unit (Geldwäschemeldestelle). The current contact information of the Financial Intelligence Unit (Geldwäschemeldestelle) can be found on its website at https://bundeskriminalamt.at/308/start.aspx.

71 The Financial Intelligence Unit (Geldwäschemeldestelle) housed at the Criminal Intelligence Service Austria, also known internationally as the Austrian Financial Intelligence Unit (A-FIU), is the central point of contact in Austria for suspicious activity reports and enquiries in relation to money laundering, terrorist financing and disclosure breaches in relation to trusteeships. The Financial Intelligence Unit (Geldwäschemeldestelle)'s principle task is to receive suspicious activity reports as well as other information in the regard, to analyse the information and conduct initial enquiries and to inform the competent authorities in detail. Suspicious activity reports in this regard are to be submitted exclusively to the Financial Intelligence Unit (Geldwäschemeldestelle) and not to other authorities, e.g. the FMA. When submitting suspicious activity reports, it must be borne in mind that they (may) subsequently become part of an investigatory and/or sanctioning procedure, and therefore also subject to the inspection of files pursuant to the corresponding applicable regulations under procedural law. In this context, Article 19 para. 2 FM-GWG orders that the obliged entities are required, among other things, to ensure that their employees and representatives that report a suspicion of money laundering or terrorist financing to the Financial Intelligence Unit (Geldwäschemeldestelle) are protected against threats or reprisals. It is therefore recommended to anonymise suspicious activity reports to the extent that individual employees of obliged entities are not named.[26] Despite such anonymization, it must however be ensured that the Financial Intelligence Unit (Geldwäschemeldestelle) is able to reach informed staff members of the obliged entity both with the required degree of urgency and with a minimum of effort, in the event that it is necessary to communicate with them. For this purpose, the contact information of the obliged entity (name of the institution, e-mail address and telephone number) must in particular be entered through the goAML reporting platform and kept up-to-date. Especially in the case that the obliged entity has an AML division with a large number of staff members, it is also recommended, in addition, to provide the direct extension of the respective employee, or a corresponding abbreviation that may be referred to when establishing contact, in order to permit contact to be established quickly.

72 Even if suspicious activity reports relate to terrorist financing, they should nevertheless be submitted by the obliged entities to the Financial Intelligence Unit (Geldwäschemeldestelle).

[26] Against this background, when submitting a suspicious activity report or related documentation, it is also necessary to refrain from naming relevant FMA employees by name or from forwarding personal data about FMA employees.

Once the latter has concluded its analysis, it shall in turn forward the report to the Federal Agency for State Protection and Counter Terrorism (BVT; Bundesamt für Verfassungsschutz und Terrorismusbekämpfung).

73 The local regulations in relation to the submission of a suspicious activity report must be observed for foreign branches of Austrian obliged entities. The extent, to which a link to Austria exists, as well as whether a suspicious activity report must (also) be submitted to the Financial Intelligence Unit (Geldwäschemeldestelle) in Austria, must be reviewed on a case-by-case basis.

74 Obliged entities and their employees as applicable are required to cooperate fully with the Financial Intelligence Unit (Geldwäschemeldestelle) pursuant to Article 16 para. 2 FM-GwG, by providing the Financial Intelligence Unit (Geldwäschemeldestelle) irrespective of a suspicious activity report pursuant to Article 16 para. 1 FM-GwG being made, directly or indirectly upon request all information it deems necessary for preventing or pursuing money laundering or terrorist financing.

4.2 Format

75 Since 01.04.2021, suspicious activity reports must be exclusively submitted via goAML. Suspicious activity reports submitted through other communications channels without prior approval from the Financial Intelligence Unit (Geldwäschemeldestelle) shall be considered as not having been submitted in an orderly manner. More detailed information about the submission format of suspicious activity reports may be found (in German only) in their currently applicable form on the website of the Criminal Intelligence Service Austria (Bundeskriminalamt) at: https://www.bundeskriminalamt.at/308/start.aspx.

4.3 Contents

76 Irrespective of the format regulations stipulated by the Financial Intelligence Unit (Geldwäschemeldestelle), suspicious activity reports must fulfil substantive minimum requirements, in order to facilitate the reporting procedure, and to ensure it occurs as efficiently as possible. From the statements by the obliged entity in relation to the circumstances triggering the obligation to make a report, it should ultimately be clear for the competent authority

- WHO

- WHAT

- WHEN

- WHERE

- HOW

(it) has happened. The relevant supporting documentation, especially documentation relating to the opening of the account, proof of identity, copies of sample signatures, statements about

accounts, or receipts in relation to account movements/balances, complete proof of transactions in the case of single transactions, including a SWIFT receipt or information including IBAN details about any contra account to which (the) transaction(s) was/were transmitted, are in any case to be provided with the suspicious activity report. In the area of virtual currencies, these in particular include confirmations and screenshots about buying and selling or the trade in question including transaction details and the transaction ID, statements from the wallet including proof of ownership, or the power of disposal over the wallet etc.

77 For the sake of completeness, it should be noted that the formal requirements stipulated by the Financial Intelligence Unit (Geldwäschemeldestelle) must also be observed regarding the submission of accompanying documents as well as account movements. The latter, at the time of this Circular being revised, are for example to be submitted in the format stipulated by goAML, i.e. in a machine-readable tabular form.

78 Furthermore, it must also be stated which activity to be reported is assumed and justified, as well as why the obliged entity assumes a circumstance necessitating a report has occurred (where a link exists to money laundering, then where possible, the (type of) predicate offence(s) assumed to have been committed must be stated), in order for the Financial Intelligence Unit (Geldwäschemeldestelle) is able to understand the obliged entity's considerations.

79 If the obliged entity holds additional information (such as from a meeting with the customer) or documentation (e.g. from their own research) in relation to the matter, then such information or documentation should be submitted as part of the suspicious activity report, with a brief explanation in the report about their background and relevance. Where such information and/or documentation does not exist, then it is expedient to state that a complete submission has been made, and that no further information or documentation exists.

80 Further details, which may prove helpful for the assessment of the case, and which therefore ought to be explicitly mentioned in either the explanation or in the statement of facts in the suspicious activity report, are:

- account numbers or policy numbers or wallet addresses; transaction ID;
- the date on which the account or wallet was opened, or the date on which the application for insurance was signed;
- the date of registration on online platforms for exchanging virtual currencies;
- information about where documentation such as account statements, insurance policies etc. were sent to the customer;
- information about whether and to whom “private keys” were transmitted in the case of transfers of virtual currencies;
- authorised signatories;
- logging data, IP addresses or account access data;
- security camera images from ATMs etc.

81 When submitting a suspicious activity report due to a breach of the obligation to disclose a trusteeship, it should also be attempted, to establish information about the trustor, in order to be able to state it in the suspicious activity report, e.g.

- in the case of natural persons, the full name, date of birth etc. and
- in the case of legal persons the name of the company/designation, legal form, registered address, postal address, forename(s) and surname(s) and date(s) of birth of the management bodies etc.

4.4 Non-execution of transactions and prohibition of disclosure

82 Article 17 FM-GwG defines the non-execution of transactions. According to that provision, the obliged entities shall cease to conduct any further execution of related transactions following submission of a suspicious activity report and shall fulfil any additional specific instructions received from the Financial Intelligence Unit (Geldwäschemeldestelle). Pursuant to Article 17, second sentence FM-GwG, the Financial Intelligence Unit shall take into account whether the risk exists by delaying or ceasing the transactions could hinder or impede the investigation of the circumstances or the pursuit of beneficiaries of the suspicious transaction.

83 Where it is not possible to prevent the execution, or if the non-execution or delaying of execution could impede the pursuit of the beneficiaries then the obliged entities must thereafter immediately submit a suspicious activity report pursuant to Article 17 para. 2 first sentence FM-GwG. Where doubts exist, pursuant to Article 17 para. 2 second sentence FM-GwG, orders involving incoming funds may be executed, while orders involving outgoing funds are not to be executed.

84 The obliged entities are authorised pursuant to Article 17 para. 3 FM-GwG to request a decision from the Financial Intelligence Unit (Geldwäschemeldestelle) about where concerns exists in relation to the execution of a transaction without delay. Where the Financial Intelligence Unit (Geldwäschemeldestelle) does not respond by the end of following bank working day, then the execution of the transaction shall be allowed.

85 It is recommended address enquiries about whether grounds for concern exist that speak against the execution of a transaction without delay, together with the suspicious activity report to the Financial Intelligence Unit (Geldwäschemeldestelle). Such an authorisation to execute the transaction applies exclusively for the transaction, to which the specific enquiry/ the suspicious activity report relates, and does not apply to other additional transactions within the same business relationship. In practice, it has proven sensible to submit such an enquiry promptly on the same bank working day, so that prior to the transaction being authorised, that it is possible to conduct a comprehensive check.

86 All procedures in conjunction with the submission of suspicious activity reports and the non-execution of transactions are required pursuant to Article 20 para. 1 first sentence FM-GwG to be kept confidential by the obliged entities towards customers and third parties. Equally, pursuant to Article 20 para. 1 second sentence FM-GwG, the application of due diligence

obligations towards the customer are to be suspended and instead the Financial Intelligence Unit (Geldwäschemeldestelle) informed directly, where obliged entities obtain knowledge that or have the suspicion of or justified reason to assume the existence of a circumstance that is obliged to be reported pursuant to Article 16 para. 1 FM-GwG, and may reasonably assume that the application of due diligence obligations towards customers might impede the pursuit of the beneficiary of a suspicious transaction.

87 The Financial Intelligence Unit (Geldwäschemeldestelle) is authorised pursuant to Article 17 para. 4 FM-GwG to instruct that:

- a current or forthcoming transaction (that is subject to a reporting obligation pursuant to Article 16 para. 1 FM-GwG) is to be stopped or temporarily suspended, and
- orders by the customer in relation to outgoing payments shall only be allowed to be conducted subject to approval by the Financial Intelligence Unit (Geldwäschemeldestelle).

88 The customer shall also be informed about such an order pursuant to the third sentence of Article 17 para. 4 FM-GwG by the Financial Intelligence Unit (Geldwäschemeldestelle), although informing the customer may be put off for up to a maximum of five banking days, if doing so could otherwise impede the pursuit of the payee of a suspicious transaction. The obliged entities shall be informed pursuant to the fourth sentence of Article 17 para. 4 FM-GwG about the postponement of informing the customer.

89 Where the customer has been informed about this order, then the obliged entities shall be authorised pursuant to the first sentence of Article 20 para. 2 FM-GwG to refer the customer - albeit only upon enquiry by the customer - to the Financial Intelligence Unit (Geldwäschemeldestelle). Subject to the consent of the Financial Intelligence Unit (Geldwäschemeldestelle), obliged entities are furthermore authorised pursuant to Article 20 para. 2 second sentence FM-GwG to inform the customer about the instruction.

90 Such an instruction

- shall be rescinded by the Financial Intelligence Unit (Geldwäschemeldestelle) as soon as the conditions for its issuance no longer prevail, or the public prosecutor declares that the conditions for confiscation pursuant to Article 109 no. 2 and Article 115 para. 1 no. 3 of the Code on Criminal Procedure (StPO; Strafprozessordnung) do not exist, or
- expires once six months have elapsed since it was issued or as soon as the court has reached a legally final decision in relation to an application for confiscation pursuant to Article 109 no. 2 and Article 115 para. 1 no. 3 StPO.

91 In the case of any further transactions by a customer made in conjunction with a previously filed suspicious activity report, the obliged entities must again check whether an obligation exists (also in this regard) to submit a report. Additional suspicious activity reports shall be submitted where applicable.

92 Where a suspicious activity report has been made regarding a correspondent banking relationship, then obliged entities shall subsequently not only check to what extent an obligation

to make a report exists with regard to other payers/payees or with regard to the correspondent bank itself, but also whether a (further) obligation exists to make a report regarding the same payer or payee.

93 The obliged entity shall determine internally in which cases business relationships must be terminated due to a suspicious activity report having been made. In so doing, the obliged entity must take Article 7 para. 7 FM-GwG into consideration, which stipulates in certain cases of an obliged entity being unable to comply with due diligence obligations that in addition to prohibiting the establishment of a business relationship and executing of transactions, an obligation also exists to terminate a business relationship (see also MN 23 et seq).

4.5 Internal documentation

94 Under Article 23 paras. 1 and 2 FM-GwG, obliged entities are required to establish written policies, controls and procedures regarding the effective mitigation and management of risks of money laundering and terrorist financing, which are to be approved by the management body, to be applied on an ongoing basis and adapted where necessary. According to Article 23 para. 1 nos. 4 and 5 FM-GwG, they must in particular cover suspicious activity reports and the retention of documentation. (For further information cf. FMA Circular on internal organisation for the prevention of money laundering and terrorist financing, publication date: February 2022, MN 58 et seq.)

95 The obliged entity's written instructions about the approach for making suspicious activity reports should in particular define:

- who is responsible for assessing suspicious cases and the submission of suspicious activity reports (usually the AML officer) and who their qualified deputy is in their absence;
- in which cases the AML officer is required to be informed;
- what escalation processes and routes must be observed in the case of anomalies arising e.g. by employees in front office positions or customer advisers through to the AML officer;
- which procedures are to be documented, how, when and by whom, to ensure that procedures that might be relevant in relation to money laundering are recorded in an orderly manner, and to ensure that the adequate documentation of procedures and retention connected to potential suspicious cases duly occurs.

96 Obliged entities are otherwise required pursuant to Article 21 para. 1 FM-GwG to retain the following documentation for a period of ten years following the ending of the business relationship with the customer or following an occasional transaction being conducted:

- copies of the documents and information received necessary for observing customer due diligence obligations (no. 1);
- transaction receipts and records necessary for investigating transactions (no. 2).

97 Pursuant to Article 21 para. 2 first sentence FM-GWG obliged entities shall be required to delete personal data, which they have processed solely for the purposes set out in the FM-GwG upon

expiry of the retention period, unless the regulations set out in other federal acts require or allow a longer retention period. This deadline is subsidiary in nature to longer retention periods set out under law. With regard to data-protection related aspects and the resulting regulations for the obliged entities in relation with the prevention of money laundering and terrorist financing, we refer to Article 21 paras. 4, 5 and 6 FM-GwG.

98 Until the legally final conclusion of pending investigative, main or appeal proceedings in relation to Article 165 (money laundering), Article 278a (criminal organisations), Article 278b (terrorist organisations), Article 278c (terrorist crimes), Article 278d (terrorist financing) or Article 278e (training for terrorist purposes) StGB such information shall not be allowed, pursuant to Article 21 para. 2 second sentence FM-GwG to be expunged. The provision's intention is to permit all available data and information to be able to be used in such proceedings. A condition for an exemption from the obligation to expunge such items is that the obliged entity must have gained knowledge of such proceedings. Obliged entities are not required to investigate proactively whether such proceedings exist.

4.6 Exchange of information

99 Otherwise, Article 22 para. 1 FM-GwG stipulates that obliged entities shall have systems in place to enable them to respond to enquiries from the Financial Intelligence Unit (Geldwäschemeldestelle) or the FMA in a full and expedient manner through secure channels in a manner that ensures full confidentiality of the enquiries, that appear necessary to the aforementioned bodies for the purposes of the prevention or pursuit of money laundering or terrorist financing, regarding whether they maintain or have maintained a business relationship with specified persons in the five-year period prior to the enquiry, and about the nature of such a relationship. At the time of this circular being drawn up, encrypted e-mails are included among the suitably secure communications channels.

100 In addition, Article 22 para. 2 FM-GwG[27] stipulates that obliged entities shall be allowed to exchange information in cases referring to the same customer or transaction in which two or more obliged entities are involved, where doing so is appropriate and necessary for preventing money laundering and terrorist financing (for further information of about the scope of validity see also nos. 1 and 2 of that provision). The information exchanged is to be used ex lege exclusively for the purposes of the prevention of money laundering and terrorist financing.

[27] Published in Federal Law Gazette I 118/2016 in the version amended by Federal Act in Federal Law Gazette I 25/2021; Entry into force 01.03.2021; see also 1191/A 27th legislative period, p. 20.

5 ANNEX

5.1 Literature

- Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC ("4th Anti-Money Laundering Directive").
- Directive (EU) 2018/843 of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU ("5th Anti-Money Laundering Directive").
- Joint Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information, JC/GL/2017/16 (Version: 16.01.2018).
- FATF Report Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing (Version: September 2020)
- FMA Circular on Due Diligence Obligations for the Prevention of Money Laundering and Terrorist Financing (Version: February 2022)
- FMA Circular on internal organisation for the prevention of money laundering and terrorist financing (Version: February 2022)

Note: where Internet links are given in this circular, this is done solely for information purposes. The links are guaranteed as being correct at the time of the decision regarding the publication of this Circular being passed.