Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP
Federal Office of Police fedpol

Practice of the Money Laudering Reporting Office Switzerland MROS

Negative typologies in reporting

August 2025

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP
Federal Office of Police fedpol

Practice of the Money Laudering Reporting Office Switzerland MROS

Negative typologies in reporting

Federal Department of Justice and Police FDJP
Federal Office of Police fedpol
Money laundering Reporting Office Switzerland (MROS)
3003 Bern

Tel: +41 (0)58 463 40 40
Emaill: meldestelle-geldwaescherei@fedpol.admin.ch

Website: http://www.fedpol.admin.ch

Table of contents

1 Background and objective of negative typologies

The Swiss anti-money laundering system relies on financial intermediaries to conduct basic first enquiries into potentially illegal assets or transactions. The Parliament has clearly opted for a system of qualitative reporting. The Swiss law has so far refrained from "threshold-based" reporting that requires a certain transaction amount or other quantitative trigger. The due diligence duties of the Anti-Money Laundering Act (AMLA) are structured in a cascading and a repetitive manner. Articles 3 to 5 AMLA[1] form the starting point which require financial intermediaries to verify the identity of the customer, to establish the identity of the beneficial owner and to repeat this identification process periodically. Article 6 AMLA establishes special duties of due diligence. It requires financial intermediaries to investigate any indications or suspicions and clarify them thoroughly. Only if these investigations are unsuccessful, or if suspicions cannot be dispelled and a reasonable suspicion arises they must submit a suspicious activity report (SAR) to the Money Laundering Reporting Office Switzerland (MROS) within the meaning of Article 9 AMLA. A SAR is therefore the result of a qualified assessment, not merely a risk-based assumption.

In practice, MROS repeatedly finds differences in the quality of incoming SARs. Partially, the facts of the case have barely been clarified or it is unclear whether the mandatory duties of due diligence have been carried out in accordance with Article 6 AMLA.

The evaluations of MROS clearly show a current trend towards defensive reporting. Specifically, this means that:

- SARs are not primarily submitted based on a clarified suspicion of money laundering, but rather to protect the financial intermediary from criminal or regulatory risks;
- financial intermediaries deliberately set the reporting threshold well below the level required by law and appropriate from the perspective of crime prevention;
- the information contained in the SAR is of little value or is even irrelevant and the SAR is therefore of no added value in any criminal investigation.

SARs like these do not help to combat financial crime. MROS can only process SARs effectively if they are based on an adequate initial suspicion and contain a substantiated, well-structured and well-documented presentation of the facts. Only then can the data be analysed, prioritised and forwarded to the law enforcement authorities if necessary.

The negative typologies in reporting set out here are intended to provide financial intermediaries with examples in which MROS repeatedly identified insufficiently clarified or entirely unclarified facts in a suspicious activity report ("negative typologies"). They are intended to raise awareness among financial intermediaries, improve the quality of incoming SARs and contribute to their efficient processing by MROS.

[1] Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), SR 955.0.

2 Negative typologies – Case-by-case review

The following typologies are based on the practical experience of the MROS. These typically involve case constellations in which MROS receives insufficiently clarified facts and there are no adequate indications of money laundering, its predicate offences, organized crime or terrorist financing within the meaning of Article 9 AMLA.

It is the sole responsibility of the financial intermediary to decide always on a case-by-case basis whether a set of circumstances leads to a duty to report according to Article 9 AMLA.

If a financial intermediary decides to submit a SAR, it must document the elements that gave rise to a reasonable suspicion based on the findings of its enquiries under Article 6 AMLA and present them to MROS in a comprehensible manner.

3 Negative typologies - Individual constellations

3.1 Typology 1 – Failed attempt to open an account

MROS is receiving an increasing number of SARs concerning attempts to open an account online that are aborted before a business relationship is established or any money flows (Art. 9 para. 1 let. b AMLA). What is striking about these cases is that the reporting financial intermediary has often had no contact with the customer, has not carried out full client identification and has no information on the beneficial owner of the assets. In addition, there is no indication of a predicate offence as required by Article 305bis or Article 260ter of the Swiss Criminal Code (SCC)[2] .

Often, such SARs are not based on any verifiable evidence of money laundering or terrorist financing within the meaning of the Anti-Money Laundering Act. A technical interruption during the process of opening of an account online, for example while uploading an identity document or during video identification or document transmission, does not constitute sufficient grounds for a SAR. Where a potential client terminates the process because they have changed their mind or are experiencing technical difficulties, this does not meet the criteria for submitting a SAR, unless there are some other money laundering-related irregularities. In these cases, there are no objective or plausible grounds for a reasonable suspicion within the meaning of Article 9 paragraph 1 letter b AMLA. The technologically complex process of opening an account online, in particular using mobile apps or web portals, is often aborted before a business relationship is established. When this occurs, there are no objectively verifiable grounds to suspect a predicate offence within the meaning of Article 305bis SCC or a connection with a criminal or terrorist organisation (Article 260ter paragraph 1 SCC).

Expanding reporting to include failed attempts to open an account solely because of errors or technical difficulties would not be in line with the purpose of Article 9 AMLA and would cause unnecessary work for MROS and the law enforcement authorities. In addition, MROS cannot analyse these SARs because they are based on assumptions or general risk assessments, and offer no tangible evidence of money laundering or terrorist financing.

3.2 Typology 2 – Suspicious clients who have no apparent connection to criminal assets

MROS regularly receives SARs in which financial intermediaries describe unusual client behaviour without providing any tangible evidence of any criminal assets or their origin (What triggered the clarifications at what point in time, and which indications or leads could not be dispelled through the clarifications?). These reports often cite vague inconsistencies or subjective risk factors, such as an 'implausible business model' for which there is no clear explanation, frequent changes in beneficial owners, or client companies with overly complex legal structures.

While these factors may indeed be worth considering as part of risk-based client monitoring, they do not in isolation meet the legal threshold for a SAR under Article 9 AMLA. These reports are usually vague and limited to a general assessment by the financial intermediary, without there being any clear link to the type of predicate offence required by Article 305bis SCC (e.g. fraud, embezzlement, corruption, aggravated tax offence).

However, reasonable suspicion within the meaning of the Anti-Money Laundering Act requires more than just a risk-based assessment. It requires objectively verifiable evidence that assets have been obtained through criminal activity.

3.3 Typology 3 – Third-party information

MROS regularly receives SARs based on third-party information, such as media reports or disclosure or seizure orders from domestic or foreign law enforcement authorities. These pieces of information may prompt financial intermediaries to conduct further inquiries. For a SAR pursuant to Article 9 AMLA, it is essential that the financial intermediary establishes a connection between this information and its own business relationships as part of its money laundering-related investigations, rather

[2] Swiss Criminal Code, SR 311.0.

than merely forwarding third-party information. The following typologies are examples of unsubstantiated SARs based on third-party information:

3.3.1 Typology 3.1 – Disclosure order

A disclosure or seizure order issued by a law enforcement authority is not in itself a matter that must be reported. The purpose of this criminal procedural measure, which often relates to a specific business relationship or to particular account activities and transaction histories, is to secure evidence during ongoing investigations or criminal proceedings.

If a financial intermediary receives such an order, it must decide whether it has any information to add to the information contained in the order that would corroborate a reasonable suspicion of money laundering, its predicate offences, organised crime or terrorist financing (Art. 9 para. 1 AMLA in conjunction with Art. 6 AMLA).

3.3.2 Typology 3.2 – TWINT account

Another example of unnecessary SARs involves the TWINT payment app. Financial intermediaries often submit a SAR when they learn that a TWINT account is part of a police investigation, either through information from a law enforcement authority, an official request for information from an individual authority, or an informal tip. In many of these cases, however, the financial intermediary does not mention any specific suspicions, but merely refers to the 'alleged involvement' of the TWINT account without providing any background information, context of the offence or details about the person in question. These broad references do not constitute reasonable grounds for suspicion within the meaning of Article 9 paragraph 1 AMLA. Instead, the financial intermediary should first obtain additional information indicating that the TWINT account is being used for money laundering, its predicate offences, organised crime or terrorist financing.

The general reference to a TWINT account involved in a police inquiry is not sufficient to clear the threshold for 'reasonable suspicion'. In cases involving TWINT accounts, financial intermediaries should carefully examine whether their own observations or internal analyses provide additional information that substantiates suspicions (Art. 6 AMLA), which meet the requirements for the submission of a suspicious activity report pursuant to Article 9 AMLA.

3.3.3 Typology 3.3 – Media reports

Media reports about a financial intermediary's clients or their alleged misconduct are not sufficient to justify a SAR under Article 9 AMLA. The financial intermediary must relate the information contained in media reports to its business relationships or to unusual transactions, and present the findings obtained during its clarifications (Art. 6 AMLA) in the report.

3.4 Typology 4 – Use of cryptocurrency exchanges

MROS is receiving an increasing number of SARs citing the use of cryptocurrencies or cryptocurrency services as the reason for suspicion. These SARs are usually based solely on the fact that clients have changed fiat money (cash) into cryptocurrencies or vice versa, deposited cryptocurrencies in accounts on crypto platforms, or received cryptocurrency payments, for example for salaries, fees or services.

The financial intermediary's description of the facts is often vague and merely mentions a crypto connection, without any detailed information of actual transactions, beneficial ownership, the origin of the funds or a possible criminal connection. However, the use of cryptocurrencies or a connection to a cryptocurrency service provider is not in itself suspicious and therefore does not meet the legally required threshold for reasonable suspicion under Article 9 AMLA.

Similar to foreign bank accounts, cash payments or trust arrangements, the use of cryptocurrencies or cryptocurrency services is a potential risk factor that requires a particular risk assessment. Submitting a SAR to MROS is only justified if a financial intermediary has reasonable grounds for suspicion based on this assessment.

3.5 Typology 5 – 'victim accounts'

From the perspective of MROS, 'victim accounts' represent a special category of suspicious activity

reports. These typically involve situations in which clients possess lawfully acquired funds but, due to fraud or the loss of payment instruments, become unintentionally involved in a criminal context.

3.5.1 Typology 5.1 – When the client becomes a victim

MROS regularly receives suspicious activity reports in which there is no doubt about the origin of the funds, and the holders of the funds have become victims of fraudulent activities. Often referred to as 'victim accounts', these are accounts through which trustworthy clients have transferred money to fraudsters, who are usually operating from abroad, in the context of romance scams or investment fraud.

The duty to report under Article 9 AMLA aims to prevent money laundering involving criminally obtained assets. However, in the case of victim accounts, this connection usually does not exist because the assets are legitimate and only become criminally relevant when transferred from the victim's account to criminal actors. While the transfer of these assets may part of a criminal offence, criminal proceedings primarily target the recipient of the funds, not the aggrieved individual who has lawfully generated their assets and can provide supporting documentation thereof.

3.5.2 Typology 5.2 – Stolen debit/credit card

MROS regularly receives SARs concerning lost or stolen credit or debit cards. These reports are often submitted immediately after the financial intermediary's client reports the loss, before any criminal transactions take place. They are a classic example of SARs involving 'victim accounts', i.e. cases in which an asset – in this case a payment card – is lost or stolen through no fault of its owner.

However, MROS cannot analyse SARs based solely on the loss of a payment card unless there is follow-up action by, or contextual information from the financial intermediary. MROS cannot process these SARs because neither the card nor the way it has been used has any connection with a crime. The mere loss of a payment card is not sufficient to justify a reasonable suspicion of money laundering, its predicate offences or organised crime. Only when the financial intermediary obtains further information relevant to money laundering as a result of performing its special duties of due diligence under Article 6 AMLA can an initial suspicion arise. As long as the payment card is not used or no misuse is detected, there is no reason to suspect that assets are being used for criminal purposes and therefore no justification for submitting a SAR under Article 9 AMLA.

3.6 Typology 6 – When a financial intermediary becomes a victim of fraud

MROS regularly receives SARs from financial intermediaries that have fallen victim to fraud, often as a result of cyberattacks, social engineering (e.g. CEO fraud) or the misappropriation of funds through manipulated transaction payments.

In such cases, the financial intermediary's own assets are transferred from the institution's accounts to the fraudsters, who often operate from abroad. The financial intermediary suffers direct financial loss as a result. However, these assets are of legitimate origin and have no connection to predicate offences by third parties or to money laundering-related activities.

The duty to report under Article 9 AMLA requires the financial intermediary to have a reasonable suspicion that assets have been obtained by means of criminal activity. However, if the reporting financial intermediary or institution falls victim to fraud and mistakenly transfers its own funds to the perpetrators, there are generally no grounds to suspect that a predicate offence to money laundering has been committed. Such cases are therefore not subject to mandatory reporting under Article 9 AMLA.

3.7 Typology 7 – Slush funds

MROS regularly receives SARs related to possible slush funds, i.e. assets that the reporting financial intermediary believes could potentially be used for bribes. These SARs are often submitted in the context of an international business relationship with a company operating in a sector with an increased risk of corruption, for example commodity trading, construction or energy supply, or in cross-border government contracts.

However, mere conjecture that funds could be used in the future to exercise undue influence is not sufficient to meet the legal requirements for a SAR under Article 9 paragraph 1 AMLA. As long as the assets in question originate from a legitimate source – such as ordinary business operations – then they are not of criminal origin as required by the Anti-Money Laundering Act, even if they are intended for use for criminal purposes. Under Article 305bis SCC, the offence of money laundering requires a predicate offence (e.g. bribery, criminal mismanagement or fraud) that has led to the acquisition of criminal assets. Only when the act of bribery has taken place – in particular when a payment is made into the account of the recipient of the bribe – has a predicate offence been committed. Only then can the financial intermediary holding the account reasonably suspect that criminal assets are involved, leading to a duty to submit a SAR.

3.8 Typology 8 – Stock exchange offence without shares listed in Switzerland

MROS regularly receives SARs relating to suspected stock exchange offences under Article 142 (Exploitation of insider information) and Article 143 (Market manipulation) of the Financial Market Infrastructure Act (FinMIA[3]). Both types of offences can be predicate offences to money laundering (Article 305bis SCC) under certain conditions.

Under Article 154 paragraph 2 and Article 155 paragraph 2 FinMIA, insider trading and market manipulation only qualify as felonies under the SCC if the criminal act results in financial gain exceeding one million Swiss francs. Only then has a predicate offence to money laundering been committed, and if there are reasonable grounds to suspect that this is the case, then a SAR under Article 9 AMLA must be submitted.

Regarding the duty to report, it should be noted that the unlawful activities in Articles 142 and 143 FinMIA only become criminal offences if they relate to securities admitted to trading on a trading venue or DLT trading facility which has its registered office in Switzerland. If these conditions are not met, in particular if there is no indication that the assets are of criminal origin, there is no reason to submit a SAR to MROS

[3] Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (Financial Market Infrastructure Act, FinMIA), SR 958.1.