Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Money Laundering Reporting Office Switzerland (MROS)

Typology Report

Volume I / II

September 2025

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Money Laundering Reporting Office Switzerland (MROS)

Typology Report

Volume I / II

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Polizei fedpol
Meldestelle für Geldwäscherei (MROS)
3003 Bern

Telefon: (+41) 58 463 40 40
E-Mail: meldestelle-geldwaescherei@fedpol.admin.ch

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

Table of contents

1 Introduction

This typology report published by the Money Laundering Reporting Office (MROS) aims to provide financial intermediaries with practical examples of suspicious circumstances relating to money laundering and terrorist financing, thereby raising awareness of these facts.

Based on practical cases, MROS has compiled examples to provide financial intermediaries with illustrations of indicators, potential risks, and methods used to combat money laundering and terrorist financing.

The target audience are employees of the compliance departments and those in direct customer contact, as well as members of senior management responsible for due diligence.

This typology report is published on the MROS website. The collection is constantly being expanded.

2 Typology report Vol. I

2.1 Case 1: Criminal mismanagement – il nostro account

Preliminary remarks

This case illustrates a client's attempt to transfer funds not via his personal account but via a bank nostro account. The point 4.4 of the Appendix to the AMLO-FINMA[1] states that a client who wishes certain payments not to be made directly from his or her own account, but via a financial intermediary's nostro account[2] is a qualified indication of money laundering.

Facts

A financial intermediary's client is active in the textile industry. In particular, he was a shareholder and CEO of a company specialised in the wholesale of various industrial supplies and equipment. His wealth came from his professional activity.

The client expressed the wish to deposit several hundred thousand Swiss francs in cash into a nostro account at the financial intermediary, which he would then transfer to his personal account. In this way, the accounting entries would not have shown the client's name on his account statements. In view of this, the financial intermediary asked for explanations and then refused to execute the transaction, which is why no payments were made to or credited to the nostro account. The client did not insist on the transaction either. The financial intermediary reported the case to MROS on the basis on Art. 305ter para. 2 SCC[3].

Based on the legal principles MROS transmitted the information via its partner FIU to the competent international authority. This information was used to provide mutual legal assistance within the criminal proceedings conducted abroad which under Swiss law would constitute serious criminal mismanagement according to Art. 158 para. 2 SCC.

Best practice for financial intermediaries

The client's atypical request prompted the financial intermediary to refuse the transaction. It then carried out clarifications in accordance with Art. 6 AMLA[4] on all business relationships linked to this specific client, i. e. those where he was the contracting party, beneficial owner, control holder or where he held power of attorney rights.

Even though the transactional analysis did not reveal any suspicion of a specific predicate offence to money laundering, the discomfort of the situation generated by this qualified indication of money laundering prompted the financial intermediary to make use of its right to report on the basis on Art. 305ter para. 2 SCC.

2.2 Case 2: Fraud – Enabling scams by transit accounts

Preliminary remarks

This case illustrates the importance of financial intermediaries reporting transit accounts.

The use of a transit account constitutes a general indication of money laundering, respectively a specific indication of money laundering according to point 2.1.2 and 3.2.14 of the Appendix to the AMLO-FINMA[5]. When a financial intermediary reports a transit account to MROS, the difficulty lies in identifying the predicate offence. Even if the use of a transit account is an indication of an obstructionist act, MROS still needs to determine a predicate offence to money-laundering.

Facts

A Swiss financial intermediary noticed that the activities of several client companies were not in line with the original aims indicated when the business relationship was opened.

1 Ordinance of the Swiss Financial Market Supervisory Authority on the Prevention of Money Laundering and the Financing of Terrorism (FINMA Anti-Money Laundering Ordinance, AMLO-FINMA), SR 955.033.0.

2 Term for the account of a credit institution, which is held at a domestic or nowadays mostly foreign correspondent bank for the credit institution, in the credit institution's own accountancy.

3 Swiss Criminal Code, SR 311.0.

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

5 Ordinance of the Swiss Financial Market Supervisory Authority on the Prevention of Money Laundering and the Financing of Terrorism (FINMA Anti-Money Laundering Ordinance, AMLO-FINMA), SR 955.033.0.

Following clarifications with the client and the submission of contracts and invoices by the client, the financial intermediary came to the conclusion that these documents were unclear, contained a large number of spelling errors and often lacked meaning. The financial intermediary was unable to verify the plausibility of the companies' activities and did not understand the economic background of the transactions. Moreover, the scale of the account movements and balances suggested that these were transit accounts. The fact that the business relationship involved a large number of counterparties, often unknown and with no accessible information, led the financial intermediary to conduct in-depth clarifications with the client and to attempt to verify the plausibility of the transactions and their purpose. Since the client was unable to provide the necessary information for plausibility verification, the financial intermediary reported the case to MROS in accordance with Art. 9 AMLA[6]. Due to the numerous, mostly unknown counterparties, the financial intermediary did not identify any predicate offense. However, he could not rule out money laundering activities.

MROS analysed the case and was able to link these transit accounts to other reports and to a large-scale fraud case in a neighbouring country. MROS transmitted the information to the responsible prosecution authority.

Best practice for financial intermediaries

The financial intermediary acknowledged the discrepancy between announced and current activities on the accounts and he carried out clarifications in accordance with Art. 6 AMLA. Furthermore, he identified counterparties, both senders and receivers of funds and considered several accounts as transit accounts. Even if MROS does not forward the information to the competent law enforcement authority within 40 days, it can subsequently identify a predicate offense on the basis of relevant information received from other partner authorities and, if necessary, report the case to the competent law enforcement authority. Therefore, it is important that financial intermediaries report such transit accounts.

2.3 Case 3: Fraud – Accounts in the name of foreign financial intermediaries

Preliminary remarks

This case illustrates the extraordinary due diligence duties of a Swiss financial intermediary if the contracting party is a foreign financial intermediary.

When a foreign financial intermediary opens an account in Switzerland, the Swiss financial intermediary's due diligence duties are reduced provided that the foreign financial intermediary is subject to equivalent supervision and regulation in its country with regard to combating money laundering and terrorist financing (in particular Art. 58 let. e AMLO-FINMA[7] and Art. 65 para. 1 let. d AMLO-FINMA). In accordance with Art. 65 para. 2 let. a AMLO-FINMA, the Swiss financial intermediary will request a declaration of beneficial ownership from the contracting party if there are indications of money laundering or terrorist financing.

Facts

A foreign financial intermediary, specialised primarily in offering cryptocurrency payment solutions, opened an account with a Swiss financial intermediary. The foreign financial intermediary provided its customers access to a multi-currency payment solution, enabling them to access liquidity at any time. The foreign financial intermediary also maintained relationships with other financial intermediaries who hold sub-accounts with the Swiss financial intermediary. Foreign customers could buy cryptocurrencies on a platform operated by one of the foreign financial intermediaries holding a sub-account.

The Swiss financial intermediary received unforeseen the notification of an aggrieved party's complaint. The financial intermediary realized that a foreign client of the foreign financial intermediary invested several thousand euros in a cryptocurrency on the cryptocurrency platform. This amount was credited to the cryptocurrency company's Swiss sub-account. After the notification of the Swiss financial intermediary, it turned out that this was probably a scam. But the funds were no longer available in Switzerland. The Swiss financial inter-

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

[7] Ordinance of the Swiss Financial Market Supervisory Authority on the Prevention of Money Laundering and the Financing of Terrorism (FINMA Anti-Money Laundering Ordinance, AMLO-FINMA), SR 955.033.0.

mediary submitted a Suspicious Activity Report (SAR) to MROS. As a predicate offence the financial intermediary admitted fraud.

Based on the legal principles MROS transmitted the information to a partner FIU.

Best practice for financial intermediaries
After receiving a copy of the aggrieved party's complaint, the Swiss financial intermediary immediately identified the holder of the sub-account to which the potentially incriminating funds were credited. It also identified the holder's business model. Having carried out these clarifications in accordance with Art. 6 AMLA[8], the Swiss financial intermediary reported its suspicions to MROS.

2.4 Case 4: Criminal Organisation – An exemplary currency exchange office

Preliminary remarks
This case shows the importance of submitting a Suspicious Activity Report (SAR) to MROS according to Art. 9 para. 1 let. b AMLA[9] in case of terminating negotiations.

The AMLA imposes a duty to file a report if the financial intermediary terminates the negotiations to establish a business relationship, in particular if it knows or has reasonable grounds to suspect that the assets involved are subject to the power of disposal of a criminal organisation (Art. 9 para. 1 let. b in conjunction with Art. 9 para. 1 let. a no. 3 AMLA).

Facts
A Swiss currency exchange office received a phone call from the manager and control holder (of a company based in Northern Italy), which provided consulting services to companies. The manager intended to regularly cross the Italian-Swiss border with cash amounting between EUR 30 000 and EUR 70,000 and intended to exchange the money at the Swiss currency exchange office. The manager wished to remain discreet about the reasons for these transactions.

The currency exchange office refused the transaction and reported the case to MROS on the basis of Art. 9 para. 1 let. b AMLA. In particular, it could not rule out a link to an Italian criminal organisation. Indeed, opensource research associated the prospect with a case of aggravated extortion and tax fraud on behalf of an Italian criminal organisation.

MROS carried out an in-depth analysis regarding this manager. The results confirmed the financial intermediary's suspicion. The manager was known to Swiss and foreign law enforcement authorities. Based on the legal principles MROS transmitted the information to a Swiss police authority and to a partner FIU.

Best practice for financial intermediaries
In practice, it is rare that information reported under Art. 9 para. 1 let. b AMLA leads to a transmission from MROS to the prosecution authorities (Art. 23 para. 4 AMLA). However, as the 'first line of defence' in the fight against money laundering, a financial intermediary who terminates negotiations in such a case enables MROS to provide administrative assistance within the meaning of Art. 29 cont. AMLA. This case underlines the importance of reporting under Art. 9 para. 1 let. b AMLA, both in terms of the conduct of the financial intermediary who, as a 'first line of defence' against money laundering, prevents potentially criminal funds from being laundered in Switzerland, and in terms of the operational analysis of MROS, which was able to inform two partner authorities, both national and international. In this case, the currency exchange office did not receive a transmission notification from MROS, which does not mean that MROS remained passive. It used two channels other than the transmission according to Art. 23 para. 4 AMLA.

2.5 Case 5: Art work – Paintings from a Caribbean art gallery

Preliminary remarks
This case illustrates the diligence with which a financial intermediary clarified transactions linked to the art market.

Studies have shown that the art sector is at risk from money laundering and terrorist financing. The vast majority of market participants do not have

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

a connection to illicit activities, but there are risks associated with these markets, and some jurisdictions do not have sufficient awareness and understanding of them. This results in a lack of investigative resources and expertise, and difficulties with pursuing cross-border investigations.[10] Clarifications in accordance with Art. 6 AMLA[11] enable the financial intermediary to understand the economic background of a transaction linked to the art market, to document it and to detail the suspicious activity report addressed to MROS.

Facts

Due to the transaction monitoring, a Swiss financial intermediary identified thirteen unexpected incoming transfers totalling USD 1,8 Mio. originated from a foreign art gallery at a personal account of one client.

The financial intermediary tried to clarify the background. As per the client's feedback, the payments were related to the sale of two paintings which were part of his divorce settlement and were supposed to be sold to the foreign art gallery. According to a contract with the art gallery, the client sold the two paintings for USD 1,1 Mio. and USD 0,9 Mio., a total value of USD 2 Mio.. An initial payment of USD 200,000 was already made, the remaining USD 1,8 Mio. had to be transferred after the sale. The payments to the client's account were made from an account of the art gallery with a currency exchange office in South America (USD 800,000) and from another account in the Caribbean (USD 1 million). The total USD 1,8 Mio. was split up and paid in thirteen transactions, between USD 25,000 and USD 105,000 each.

Regarding the art gallery's split payments, the client provided the following explanations:

- First, the art gallery's bank in the Caribbean has imposed a daily transfer limit, requiring the payments to be made in instalments.
- Second, the art gallery's funds available in the Caribbean account, were not sufficient to cover the full purchase price. Due to this lack of liquidity the art gallery used two different channels to settle the payment. The remaining balance was paid through foreign exchange agreements in a South American country in compliance with Central Bank regulations.

While external sources that are tracking art auctions showed comparable prices for comparable artworks, the financial intermediary had strong concerns regarding the payments. The contract stipulated the initial payment of USD 200,000 that was already made before signing the contract and the remaining USD 1,8 Mio. that had to be transferred to the client's bank account after the sale. However, the contract did neither stipulate any rationale for the split payments (limitations on daily transfers and lack of liquidity) nor anything about the need for using an offshore account in the Caribbean. OSINT researches found out that the Prosecutor of a South American country accused the art gallery's owner of money laundering in relation to bribery and corruption.

The financial intermediary exercised its right to communicate to MROS in accordance to Art. 305ter para. 2 SCC[12]. The suspected predicate offense was corruption. Based on the legal principles MROS transmitted the information to a foreign partner FIU.

Best practice for financial intermediaries

The financial intermediary immediately clarified the origin of the paintings and the purchasing art gallery. It asked for the contracts and compared the prices with them on the market. The smurfing and payment through two different accounts (in particular one in a Caribbean country) created a feeling of discomfort and the financial intermediary reported the matter to MROS.

2.6 Case 6: Criminal Organisation – 'Ndrangheta's life insurance policy

Preliminary remarks

This case illustrates the diligence of a life insurance institution which carefully checked who was paying the premiums.

---

10 FATF Report Money Laundering and Terrorist Financing in the Art and Antiquities Market, published February 2023.

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

12 Swiss Criminal Code, SR 311.0.

Life insurance institutions are subject to the AMLA[13] by virtue of Art. 2 para. 2 let. c AMLA. The conclusion of life insurance contracts and the payment of high premiums can prove to be an attractive laundering vehicle for potential criminals.

Facts

A couple concluded a life insurance contract with a Swiss insurance institution. Two insurance policies were issued. After a while both policies were assigned to a trust based in Italy. From then on, the trust paid the insurance premiums. Years later, the trust requested the payment of the surrender value of one of the policies into an account in Italy. The amount in question was over CHF 100,000.

The request for payment came from a company whose name differed slightly from that of the trust to which the insurance policies had been assigned. The insurance institution undertook clarifications in accordance with Art. 6 of the AMLA. It came across an article referring to the minority shareholding of the Italian trust by a 'Ndrangheta boss.

Fearing that some of the premiums paid had been contaminated, or that they came from funds under the control of a criminal organisation, the insurance institution reported the matter to MROS in accordance with Art. 9 AMLA. It suspected the participation in a criminal organisation or the support of such an organisation in accordance with Art. 260ter para. 1 SCC[14].

Best practice for financial intermediaries

The Swiss insurance institution identified the (minor) name difference of the trust requesting payment of the surrender value, researched the Italian trust and promptly reported the matter to MROS, indicating the Italian account provided by the trust for payment of the surrender value of the insurance policy.

2.7 Case 7: Commodity Trading – A diligent gold trader

Preliminary remarks

This case illustrates that a financial intermediary also must fulfil its due diligence duties with due care and attention in an ongoing business relationship.

According to Art. 2 para. 3 let. c AMLA[15] and Art. 5 para. 1 let. a AMLO[16], the professional purchase and sale for the account of third parties of banknotes and precious metals falls within the scope of financial intermediation.

Facts

A foreign company (hereinafter 'Company A') is a customer of a Swiss commodity trader (hereinafter 'the Trader'). Company A obtains its precious metals from European individuals and LBMA[17] refiners. Company A sends its scrap of bars, loose jewelry, ingots, coins and industrial scrap to the Swiss based commodity trader for processing. Once the materials received have been processed, the Trader credits company A's weight accounts (depending on the materials). Company A has the liberty to use its weight accounts to acquire materials or to ask the dealer to sell the materials and credit the equivalent value to its bank account. For the Trader, Company A was classified as a 'normal' risk customer. That said, a review of the due diligence file is carried out every five years by the Trader, in accordance with its internal guidelines.

Recently, the trader noticed the following:

- Company A submitted several requests to the trader to modify its bank accounts. These requests were also submitted by an employee of Company A who was not one of the persons authorized to issue such instructions.
- The Trader had difficulties in contacting directly the person authorized to give instructions.
- Company A announced the appointment of a new managing director. The Trader took the usual steps required by its due diligence to validate

13 Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), SR 955.0.
14 Swiss Criminal Code, SR 311.0.
15 Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), RS.955.0.
16 Ordinance on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Ordinance, AMLO), RS 955.01.
17 The London Bullion Market Association (LBMA) coordinates as an independent authority the trade at the London Bullion Market, the most important over-the-counter trading centre for gold and silver in London.

this change, but these were never completed. The trader was subsequently informed that the new director would no longer be its contact.
- The Trader found various errors in the documents sent by Company A.
- The Trader was informed by a third-party of possible legal proceedings involving the controlling shareholder of Company A. This information led the trader to do further research. The Trader found negative press relating to money laundering regarding Company A.

After reading the press article, the Trader decided to immediately freeze Company A's account and to file a suspicious transaction report with MROS in accordance with Art. 9 AMLA, as the information provided by Company A could be linked to the acts of which the controller was accused. The Trader suspected an aggravated tax misdemeanour in accordance with Art. 305bis para. 1bis SCC[18]. The Trader attached Company A's foreign bank accounts, the KYC, the negative press article, the open invoices, Company A's financial accounts and the documents used to open the business relationship.

Based on the legal principles MROS transmitted the information to a foreign partner FIU.

Best practice for financial intermediaries

The Trader carried out clarifications as soon as the request to change bank accounts was received. It carried out opensource research. It documented its suspicious activity report with a clear and precise explanation of its business relationship with Company A. He provided information on Company A's bank accounts.

2.8 Case 8: Fraud – The magic behind a virtual IBAN

Preliminary remarks

This case illustrates how a Swiss financial intermediary was able to identify the end client of a foreign financial intermediary using virtual IBANs.

A virtual IBAN or vIBAN is a pseudo account number that redirects incoming payments directly to an IBAN linked to a conventional 'physical' bank account (master account). The main difference between a regular IBAN and a vIBAN lies in the account matching. A classic IBAN is linked one-to-one to one single physical account. A payment made using the classic IBAN will be credited to the bank account to which the IBAN is linked. By contrast, a vIBAN is not matched to a physical bank account. It is a reference number used to redirect a payment to another IBAN linked to a physical bank account. Its balance is constantly zero. Several vIBANs can be used by one account holder[19].

Facts

A Swiss financial intermediary opened a business relationship with a foreign bank. This foreign bank offered its clients the possibility of issuing vIBANs which were linked to the client's wallets. Payments made to the foreign bank's clients via these vIBANs were pooled in the foreign bank's account at the Swiss financial intermediary and then transferred to the client in form of e-money into a wallet.

A client of a Swiss third-party bank transferred several thousand Swiss francs to an account with an IBAN beginning with CH. The IBAN was verified by using a traditional IBAN verification tool ('IBAN-Calculator'). It referred to the account opened with the Swiss financial intermediary. The client of the Swiss third-party bank complained of potential fraud.

In fact, the Swiss financial intermediary had no direct business relationship with the client of the foreign bank. The foreign bank's client had no sub-accounts with the Swiss financial intermediary. The foreign bank was itself the beneficial owner of the funds transferred via the vIBANs. Thus, the foreign bank's client who received payments via the vIBANs had a claim against the foreign bank. They were entitled to have these amounts booked as e-money in the wallet managed by the foreign bank. The vIBAN served only to redirect the amounts transferred to the foreign bank's end clients.

However, the Swiss financial intermediary was able to identify the end client of the vIBAN by analysing the comments of the fraudulent transactions. The name of the final beneficiary was mentioned in the payment reference. The Swiss financial intermedi-

[18] Swiss Criminal Code, SR 311.0.
[19] European Banking Authority (EBA), Report on virtual IBANs, May 2024.

ary asked the foreign bank about the exact personal details of the end client and reported the case with these details to MROS in accordance with Art. 9 AMLA[20]. The suspected predicate offence was fraud.

Based on the legal principles MROS transmitted the information to a foreign partner FIU.

Best practices for financial intermediaries

As a financial intermediary providing services to a foreign financial intermediary, the Swiss financial intermediary reacted immediately to a complaint from a client of a third-party Swiss bank. It identified the end client of vIBAN by analysing the comments of the fraudulent transactions. It immediately reported the case to MROS. The Swiss financial intermediary and the foreign financial intermediary have agreed that the latter will provide details of its clients using vIBANs. In the event of transmission to a criminal prosecution authority, the Swiss financial intermediary cannot block the account of the foreign financial intermediary. In this case, it would reserve an amount equal to the potentially criminal proceeds.

2.9 Case 9: Art work – An art collection enhanced by a convicted curator

Preliminary remarks

This case illustrates the diligence with which a financial intermediary clarified transactions linked to the art market.

Studies have shown that the art sector is at risk from money laundering and terrorist financing. The vast majority of market participants do not have a connection to illicit activities, but there are risks associated with these markets and some jurisdictions do not have sufficient awareness and understanding of them. This results in a lack of investigative resources and expertise, and difficulties with pursuing cross-border investigations.[21] The clarifications in accordance with Art. 6 AMLA[22] enable the financial intermediary to understand the economic background of a transaction linked to the art market, to document it and to detail the suspicions addressed to MROS.

Facts

A Swiss financial intermediary had a business relationship with a client. In the KYC the client declared that the account was used for the purposes of asset management. The client intended to use this account to manage funds from third parties.

At a certain point the financial intermediary was informed in-house regarding a planned transaction of several millions of euros on the client's account. The internal documentation mentioned that the amount would be the proceeds from the sale of a part of the client's private art collection. This new activity on the client's account was not in line with the client's KYC profile. Therefore, the financial intermediary preventively blocked the account.

Requesting clarification, the client declared to own an art collection and the expected incoming payments on his account were from the sale of art work from his private art collection. The financial intermediary insisted in more information. To this end, the financial intermediary requested an official valuation of the art work in order to determine whether the expected amount on the client's account was in line with the market prices of the art work. In the documentation then provided by the client, the collection was valued by a curator who, after verification by the financial intermediary, had been convicted in Italy of a series of financial crimes committed by a group.

The financial intermediary refused the transaction and reported its suspicions to MROS in accordance with Art. 305ter para. 2 SCC[23], attaching the foreign accounts from which the assets should have come. The suspected predicate offence was fraud in accordance with Art. 146 SCC.

Best practice for financial intermediaries

The financial intermediary blocked the transaction when it noticed the discrepancy between the KYC and the amount that was going to be credited. The

[20] Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), SR 955.0.
[21] FATF, Report Money Laundering and Terrorist Financing in the Art and Antiquities Market, February 2023.
[22] Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), SR 955.0.
[23] Swiss Criminal Code, SR 311.0.

financial intermediary immediately began clarifications. It investigated not only the client but also all the persons involved in the suspicious transaction. The financial intermediary carried out clarifications in accordance with Art. 6 AMLA and found corresponding indications that suggest that a suspicion based on reasonable grounds has been confirmed. The financial intermediary also clarified the background of curator, who had written the expert opinion on the art objects. The financial intermediary reported its suspicions to MROS, indicating the foreign account from which the funds might have come.

2.10 Case 10: Virtual Assets – The diligent crypto-currency broker

Preliminary remarks

This case illustrates the responsiveness of a crypto-currency broker who was able to block crypto-fiat transactions and quickly report the case to MROS.

Financial intermediaries are also persons who on a professional basis accept or hold on deposit assets belonging to others or who assist in the investment or transfer of such assets; they include in particular persons who trade for their own account or for the account of others in banknotes and coins, money market instruments, foreign exchange, precious metals, commodities and securities (stocks and shares and value rights) as well as their derivatives (Art. 2 para. 3 let. c AMLA[24]).

Thus, a crypto-currency broker qualifies in general as a financial intermediary (Virtual Asset Service Provider [VASP]).

Facts

A Swiss crypto-currency broker, offering exchange services (fiat to crypto and crypto to fiat), allowed its clients to use its services via a widget on its website or by downloading a self-custodial wallet. The Swiss crypto-currency broker operated via a Swiss financial intermediary and a foreign payment service provider.

A client started a business relationship with this Swiss crypto-currency broker and provided in this context a copy of his passport, a proof of address and a live selfie. The client wanted to carry out transactions via a self-custodial portfolio. Explicitly, he wanted to transfer the crypto currency Ethereum (ETH) from one wallet to another.

During the onboarding process, the crypto-currency broker carried out a costumer due diligence check on the client and his background. Therefore, he checked the sanctions lists, media reports and OSINT (Open-Source Intelligence). According to press reports and other OSINT researches, the client appeared as a drug baron from a European country based in South America. He was said to run an international money-laundering network for drug cartels. He had been arrested and was facing extradition to a North American country.

Following this information, the crypto-currency broker blocked the profile preventing any transactions. The crypto-currency broker had nevertheless observed attempts from the client to change ETH into EUR by transferring them to an account in a European country. These transactions were automatically refused and returned by the crypto-currency broker's system due to the profile being blocked.

The crypto-currency broker filed a report to MROS in accordance with Art. 9 AMLA. It suspected serious offence to Narcotics Act[25] in accordance with Art. 19 para. 2 NarcA.

Based on the legal principles MROS transmitted the information to a partner FIU.

Best practice for financial intermediaries

The crypto-currency broker did researches regarding its client in OSINT and not only on sanctions lists. Based on the negative information, it immediately blocked the client's profile to prevent any transactions. Furthermore, it monitored the client's activity and noticed attempts to change crypto-currencies into fiat currencies. In his communication to MROS, he provided details of the account held in a European country.

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

[25] Federal Act on Narcotics and Psychotropic Substances (Narcotics Act, NarcA), SR 812.121.

2.11 Case 11: Enabler – The lawyer and a luxury car in the free port

Preliminary remarks

This case illustrates the difficulty presented by lawyer accounts used for atypical purposes under the guise of form R.

According to Art. 36 CDB 20[26] and based on the protection of professional confidentiality (see Art. 321 SCC[27]), depending on the circumstances, a lawyer may not provide precise information about the beneficial owners of assets he holds on behalf of clients. The lawyer as the contracting partner must therefore confirm that he is subject to professional confidentiality within the meaning of Art. 321 SCC and that the account/custody account is used exclusively for the purposes of his activity as a lawyer. On the other hand, as subject to professional confidentiality, he is not required to specify for which activities the account/custody account is used. In accordance with the material scope of Art. 321 SCC, form R must be signed by the lawyer who is bound by professional confidentiality. The financial intermediary is not obliged to carry out any checks in this respect.

Facts

A Swiss financial Intermediary maintained a business relationship with a lawyer. The account served for the lawyer's typical business activities. A formular R has been signed.

One day, the financial intermediary observed an inflow of several million Euro from a car dealer on the lawyer's account. According to the lawyer he acted as an escrow agent between the car dealer and a foreign company. The inflowing amount was connected to the sale of a luxury car. The luxury car would be stored in a free port in Switzerland. The beneficial owner of the company was unknown to the financial Intermediary.

The financial intermediary tried to clarify the situation and to verify the transaction. The client refused to provide any further information invoking the transaction was subject to professional confidentiality.

A few months later, almost the entire amount credited to the car dealer was transferred to a bank account owned by a non-EU e-money institution in Eastern Europe. The account in Eastern Europe was opened by the non-EU e-money institution to have access to SEPA[28] transfers. The lawyer controlled the non-EU e-money institution. According to further information obtained from the lawyer, the funds were then transferred to an account at a bank administrated and controlled by the lawyer in a Caribbean country. However, he refused to give the bank any information about the identity of the seller of the luxury car.

The bank reported the case to MROS in accordance with Art. 305ter para. 2 SCC. The suspected predicate offence is fraud in accordance with Art. 146 SCC. MROS forwarded the case to the competent Swiss law enforcement authority.

Best practice for financial intermediaries

The financial intermediary was alerted by a transaction which did not fall within the scope of the lawyer's typical activities. The financial intermediary tried to obtain information about the cash inflow. Despite the lawyer's initial denial, the financial intermediary insisted to receive more information when the funds were released. The financial intermediary finally obtained some information, but nothing about the identity of the seller of the luxury car. Unable to fully clarify the economic background to the transaction and because of the use of the account as a transit account, it reported the matter to MROS.

2.12 Case 12: Sanctions Evasion – The fall of the Syrian regime

Preliminary remarks

This case illustrates the importance to not only checking the sanctions lists carefully but also doing clarification in regard to suspicious transactions.

26 Swiss Banking, Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CDB 20), 2020.
27 Swiss Criminal Code, SR 311.0.
28 Single Euro Payments Area; SEPA stands for the standardisation of cashless payments for transactions in euros within Europe.

On 18 May 2011, the Federal Council issued the Ordinance imposing measures against Syria (hereafter the Syria Ordinance)[29]. In doing so, Switzerland aligned itself with the sanctions imposed on Syria by the European Union on 9 May 2011. The Syria Ordinance was revised on 8 June 2012. The sanctions against Syria were imposed because of the violent repression of the civilian population by the Syrian army and security forces. A list of persons subject to different sanctions (in particular financial sanctions) is annexed to the ordinance and frequently updated.

According to the Syria Ordinance financial intermediaries are obliged to block the bank accounts of listed persons and report them to the State Secretariat for Economic Affairs (SECO). While submitting a report to SECO does not necessarily mean that a SAR also needs to be sent to MROS, financial intermediary due diligence and reporting duties under the AMLA still apply. If investigations into a possible violation or evasion of sanctions also provide indications of money laundering, then the financial intermediary must carry out additional clarifications (Art. 6 AMLA[30]). Depending on the outcome of these clarifications, a SAR may be submitted to MROS.

Facts
After the fall of the Syrian regime in December 2024, financial intermediaries paid particular attention to possible clients linked to the deposed regime. In this context, a Swiss financial intermediary has identified a client with a Syrian background. Checking the sanctions lists has shown, that the client was not subject to the EU or Swiss sanctions.

However, the Swiss financial intermediary had further concerns. And in fact, the client had received large donations from a member of his family which was a politically exposed person (PEP). The financial intermediary concluded that the origin of these donations could have been a result from a criminal activity. It reported the case to MROS in accordance with Art. 305ter para. 2 SCC[31]. The suspected predicate offence was bribery of foreign public officials in accordance with Art. 322^{septies} SCC.

The case was forwarded to the competent Swiss law enforcement authority.

Best practice for financial intermediaries
The financial intermediary reacted immediately after the fall of the Syrian regime. It carried out a review of clients who might have links with the deposed regime. Based on new media coverage the financial intermediary identified a client in Switzerland who was not subject to sanctions, but there were indicators that the client has a kinship to a person from the Syrian regime. Therefore, the financial intermediary suspected that the assets involved in the business relationship were being used for money laundering purposes. The financial intermediary had a clear understanding of the difference between the reporting systems (sanctions versus money laundering) and also understand the different areas of authority (SECO or MROS). Therefore, the financial intermediary has been submitting the SAR in a differentiated manner.

2.13 Case 13: Commodity trading – The manufacturer of self-luminous technology

Preliminary remarks
This case illustrates how embargo law can overlap with anti-money laundering provisions in the context of a ban on Russian gold imports.

On 28 February 2022, the Federal Council decided to adopt the sanctions imposed by the European Union (EU)[32] against Russia. Based on the EmbA[33], the Ordinance of 27 August 2014 on Measures Relating to the Situation in Ukraine[34] (hereinafter referred to as the 'Ukraine Ordinance') was fully revised on 4 March 2022. In accordance with Art. 14*d* Ukraine Ordinance, the acquisition of gold with an origin of the Russian Federation, which was export-

[29] Ordinance on Measures against Syria, RS 946.231.172.7.

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

[31] Swiss Criminal Code, SR 311.0.

[32] *Council Regulation (EU) No. 833/2014* of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

[33] Federal Act on the Implementation of International Sanctions (Embargo Act, EmbA); SR 946.231.

[34] Ordinance imposing measures relating to the situation in Ukraine; SR 946.231.176.72

ed after August 4, 2022, from the Russian Federation, as well as the import, transit and transport of this gold in and through Switzerland, is prohibited. A serious violation of Art. 9 EmbA is a felony under Swiss law and may constitute a predicate offence to money laundering.

Facts

On the basis of its regular due diligence, a Swiss financial intermediary found out that a client – besides running its own watch brand – manufactures self-luminous technology as a main business activity. The innovative lighting elements contain tritium, which enables 'lighting without electricity'. This technology is used to create products such as indexes for watch dials or lights in hospitals, but also illuminated parts in sights, which are used as accessories for mainly pistols and rifles, etc.

The following in-depth transaction analysis identified incoming payments from a company in Central Asia. When being asked about the unusual counterparty, the client replied that the payments were in connection with the sale of watches to a customer in Central Asia. Further clarifications detected, that's this client was the subject of negative headlines and was portrayed as one of the top importers of – allegedly – sanctioned Russian gold and jewelry.

The financial intermediary identified all transactions with this counterpart of his client and reported the case to MROS in accordance with Art. 305ter para. 2 SCC[35]. The suspected predicate offence was a serious violation of Art. 9 EmbA.

Best practice for financial intermediaries

The financial intermediary identified that a client was incidentally active in the business of manufacturing self-luminous technology, and he identified a counterparty that was subject of bad publicity in connection with the import of Russian gold. It identified all the transactions between his client and this suspicious counterparty and reported them to MROS, suspecting a potential circumvention of the sanctions or a serious violation of the Swiss Embargo Act.

2.14 Case 14: Real estate – Arabian Gulf estate at Lake Geneva

Preliminary remarks

This case illustrates the importance of classifying the risks of a business relationship, specifically with regard to politically exposed persons (PEP), and the risks that can exist in the Swiss real estate sector.

In accordance with Art. 2*a* para. 1 let. a AMLA[36], politically exposed persons are individuals who are or have been entrusted with prominent public functions by a foreign country, such as heads of state or of government, senior politicians at national level, senior government, judicial, military or political party officials at national level, and senior executives of state-owned corporations of national significance (foreign politically exposed persons). In accordance with Art. 6 para. 3 AMLA, business relationships with foreign politically exposed persons and their family members or close associates in terms of Art. 2*a* para. 2 AMLA are deemed in every case to be business relationships with a higher risk.

Facts

For several years a Swiss financial intermediary had a client who was a former magistrate from an Arabian Gulf country. Due to the PEP status the relationship to this client was classified as 'high risk'. According to later publications in the European media relayed by various private investigative organisations fighting international corruption, the former magistrate was the subject of numerous international complaints for misappropriation in his home country. He was suspected of having embezzled tens of millions of USD.

Due to the negative press reports, the Swiss financial intermediary reported two business relationships to MROS in which the client was the beneficial owner. These business relationships recorded assets worth several million CHF, which were unrelated to the client's salaries according to the notes of the financial intermediary. The suspected predicate offence was bribery of foreign public officials in accordance with Art. 322^{septies} SCC[37].

[35] Swiss Criminal Code, SR 311.0.

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

[37] Swiss Criminal Code, SR 311.0.

One of the two business relationships was opened in the name of a company involved in the purchase and sale of real estate. It has a 'c/o' address with a trust company. MROS identified outflows of more than 10 Mio CHF to an account in the name of a notary's office. These transactions involved the purchase of a property at Lake Geneva. The notary's office account was held by another Swiss financial intermediary. MROS issued this account on the basis of a request pursuant to Art. 11*a* para. 2 AMLA. The account was used by the notary's office for client assets and was opened using Form R. MROS attempted to obtain documents on the clarifications pursuant to Art. 6 AMLA, in particular the contract for the sale of real estate involving the former magistrate. To no avail. In fact, the notary's account records transactions of several million CHF that were not clarified by the bank since they fall under the typical activity of the notary. MROS was unable to identify the seller of the property.

Subsequently, the financial intermediary himself, who received the request according to Art. 11*a* AMLA notified MROS. However, the financial intermediary reported another suspicious real estate transaction that had been subject of a seizure order from a Swiss public prosecutor's office. At the time, the account of the company sending the funds was subject of the order, not the account in the name of the notary's office. Both accounts are held at the same bank, which is how it was able to make the connection.

The case was forwarded to the competent Swiss law enforcement authority.

Best practice for financial intermediaries

Exemplarily, the financial intermediary has categorized the business relationship with the former magistrate of an Arabian gulf country as 'high risk' and carried out permanent media monitoring. At the first negative news, he identified the main cash flows. It highlighted the disproportion between the cash inflows and the client's salaries and reported the matter to MROS.

2.15 Case 15: Real estate – The unemployed architect in a villa

Preliminary remarks

This case illustrates the persistent behaviour of the financial intermediary following immediate cash withdrawals after unusually large inflows.

According to point 2.1.2 of the Annex to AMLO-FINMA when assets are withdrawn shortly after they are placed in an account (transit account), these activities are considered an indicator of money laundering, unless there is a plausible reason for the immediate withdrawal arising from the customers business activities.[38].

Facts

A Swiss financial intermediary opened a business relationship with a client, who considered himself as an unemployed architect, who was a citizen of an Eastern European country. Over the first year after the account opening there were only few financial inflows. Later, within a short period of time, two companies transferred six major transactions to the client's account.

One of the companies (company A) was owned by the client's wife. The other company (company B) was just recently established in the name of the client. Shortly after the receipt, the client withdrew the assets at the Swiss financial intermediary in cash or transferred them to other accounts with third-party intermediaries.

Consequently, the financial intermediary asked the client for explanations regarding the transactions. and the client stated that these were 'salaries' paid to him in advance respectively 'interest-free loans'. The client explained that one of the companies (company A) owned a building that he purchased with his own savings and the sums transferred were coming from the rental income of this building. In regard to the purpose of the transactions, the client explained that the money would be used to purchase a villa. A mortgage would be negotiated with a third-party intermediary to which the funds were transferred.

[38] Ordinance of the Swiss Financial Market Supervisory Authority on the Prevention of Money Laundering and the Financing of Terrorism (FINMA Anti-Money Laundering Ordinance, AMLO-FINMA), SR 955.033.0.

He also explained that the recently established company B received a large sum from a customer, who commissioned him for building a multi-party house. Being asked for clarification, the client refused to reveal the identity of his customer. Irritated by the financial intermediary's questions, the client denied to provide any documentation on these transactions and transferred most of the balance to an account opened in his name with a small regional bank.

The financial intermediary reported the case to MROS in accordance with Art. 305ter para. 2 SCC[39].

Best practice for financial intermediaries

The sudden inflow of large sums of money and the cash withdrawals alerted the financial intermediary. It tried to clarify the matter with the client and remained persistent in its clarifications. Since the financial intermediary was unable to fully clarify the matter, it filed a suspicious activity report to MROS.

2.16 Case 16: Commodity Trading – From raw material to art work via a trust company

Preliminary remarks

This case illustrates the diligent behaviour of a financial intermediary maintaining a banking relationship with a client active in commodity trading.

Commodity trading is subject to the AMLA only if it is carried out on behalf of third parties. 'Commodity' refers to unprocessed raw materials from the mining, agricultural or energy sectors, such as crude oil, natural gas, metals, ores and coffee[40]. For financial intermediaries, monitoring trading accounts can be challenging due to the large volume of transactions.

Facts

A Swiss financial intermediary has a business relationship with a company (hereafter 'client') trading in commodities.

Over a certain period, hundreds of thousands of Swiss francs entered the client's account and were withdrawn in cash almost immediately by the client's controlling shareholder. The bulk of the cash inflows came from two trust company's accounts (Company B and C) with a third-party financial intermediary.

After the transaction monitoring generated an alert on the client's account, the financial intermediary discovered additional irregularities. For example, the financial intermediary found that the two trust Companies B and C had identical directors, although they were not domiciled at the same address. In addition, the client had its domicile at the trust Company B.

When asked about the purpose of these incoming transactions from the trust Company C by the Swiss financial intermediary, the client explained that he was offering shares in art works to private investors. These investors would become joint owners of the art works. The said investors are supposed to pay their shares into the account of the trust Company C, which would then be transferred to the account of his company, and would then be paid in cash to purchase the art works in question at auctions, at which cash transactions would be common. In support of his explanations, the client presented contracts concluded with investors. However, these contracts were redacted, drafted in an unprofessional manner, and their terms and conditions sometimes differed substantially, even though they were supposed to relate to identical transactions. The financial intermediary also noted that the company's accounts were used by the client for apparently private expenses and that the sums paid by the investors substantially exceeded the price of the art works potentially purchased. The financial intermediary found the client's explanations unconvincing and suspected investor fraud and misappropriation. It reported the business relationship with the trading company to MROS.

The case was forwarded to the competent Swiss law enforcement authority.

Best practices for financial intermediaries

Despite the enormous volume of transactions that can be recorded on a traditional trading account,

[39] Swiss Criminal Code, SR 311.0.

[40] FINMA, Circular 2011/1, Financial intermediary activity within the meaning of the AMLA, Details of the Ordinance on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Ordinance, AMLO), RS 955.01, page 14.

the financial intermediary identified passing transactions and withdrawals in cash that appeared to him to be outside the scope of the traditional activity announced for the said business relationship. The financial intermediary clarified the matter and identified that the account was allegedly being used for activities in the art sector. The financial intermediary critically scrutinized the information provided by the customer and uncovered contradictions between the information provided by the customer and the actual circumstances. He reported the matter to MROS.

2.17 Case 17: Virtual Assets – Fluent communication between a VASP and its Swiss bank

Preliminary remarks

This case illustrates the responsiveness of a crypto-currency broker who was able to block the profile of a client after an alert of a Swiss financial intermediary for any future transactions.

Financial intermediaries are also deemed to be persons who on a professional basis accept or hold on deposit assets belonging to others or who assist in the investment or transfer of such assets; they include in particular persons who trade for their own account or for the account of others in banknotes and coins, money market instruments, foreign exchange, precious metals, commodities and securities (stocks and shares and value rights) as well as their derivatives (Art. 2 para. 3 let. c AMLA).

A crypto-currency broker falls within the scope of financial intermediation as defined in the AMLA (Virtual Asset Service Provider [VASP]).

Facts

A crypto-currency broker offers exchange services (fiat to crypto and crypto to fiat). As a VASP, the crypto-currency broker was affiliated to a self-regulatory organisation. Its potential clients could use the crypto-currency broker's services via a widget on the broker's website or by downloading a self-managed wallet. The crypto-currency broker worked with a Swiss bank (custodian bank) to process its payment services.

The crypto-currency broker correctly carried out the online identification process with the client when opening the account and starting the business relationship. To create the profile, the client provided the crypto-currency broker with a copy of his passport, his phone number and address including proof of address, created a live selfie and answered further identification questions during the video call.

After the client had carried out a transaction via the self-managed wallet, the custodian bank informed the crypto-currency broker that the client was suspected of fraud. In this context, the custodian bank had received a Swift message from a third-party bank and a call from an aggrieved party. This information strengthened the suspicion that the client might be involved in a fraud case. The crypto-currency broker carried out its own clarifications in accordance with Art. 6 AMLA, after receiving the information from the custodian bank. The crypto-currency broker concluded that the suspicion of fraud against the client had been substantiated.

Therefore, the crypto-currency broker submitted a suspicious transaction report to MROS. in accordance with Art. 9 AMLA; giving details of the transaction hash, the wallet address, the sum in traditional currency converted into ETH and its equivalent in ETH. The suspected predicate offence was fraud in accordance with Art. 146 SCC[41]. In addition, the crypto-currency broker blocked the customer's profile, preventing any future transactions.

Based on the legal principles MROS transmitted the information to a partner FIU.

Best practice for financial intermediaries

Following the alert issued by the custodian bank, the crypto-currency broker immediately clarified the situation regarding the customer suspected of fraud. It then promptly reported the case to MROS, attaching documentation relating to the wallet, the transactional hash and the amounts invested in virtual currencies. It also blocked the profile of the customer suspected of fraud for all future transactions for prevention purposes.

[41] Swiss Criminal Code, SR. 311.0.

2.18 Case 18: Fraud – The manipulated ID card

Preliminary remarks

This case illustrates how financial intermediaries deal with third-party alerts in the context of fraud attempts.

When it comes to suspicions of fraud or fraud attempts, the initial alert results from different sources: Often, a potential victim approaches the financial intermediary to report a suspicion. In other cases, the financial intermediary receives a copy of a criminal complaint that indicates possible fraudulent activity. Another possibility is that another financial intermediary sends a request for the repayment of funds, for example by Swift message. Finally, third-party information, such as a list of stolen identities, can also play an important role in raising suspicions of fraud.

Facts

A Swiss financial intermediary had a business relationship with a client of foreign nationality. The Swiss financial intermediary received information from a third party that several perpetrators tried to open bank accounts with Swiss financial intermediaries, using false IDs. This was part of a large-scale fraud attempt against temporary employment agencies in order to receive unlawful salary payments through these accounts.

This alert contained a list of names used to open those accounts in various Swiss financial intermediaries with false IDs from a neighbouring country. After conducting various researches in its databases, the financial intermediary figured out, that one of the identities on the aforementioned list was used at his institution to open an account. The misused ID card was manipulated in terms of identification numbers. The signature on the opening documents did not match that on the ID. And as well, the manipulated ID card used a fake photo.

After the financial intermediary had been informed of this alert and hat carried out its due diligence duties, it blocked the account of the client concerned.

The financial intermediary reported the case to MROS in accordance with Art. 9 AMLA[42]. The suspected predicate offence was fraud in accordance with Art. 146 SCC[43].

Based on the legal principles MROS transmitted the information to a partner FIU.

Best practice for financial intermediaries

On receiving the list with the names used, the financial intermediary immediately checked whether any accounts had been opened in its books with similar identities. He identified one account and acted immediately: He blocked the account and reported its suspicions to MROS before any funds could be credited.

2.19 Case 19: Dealer – The conscientious pharmacist

Preliminary remarks

This case illustrates indicators where a dealer has to report his suspicions to MROS.

In accordance with art. 2 para. 1 let. b AMLA[44] dealers are also subject to the AMLA when they deal in goods commercially and in doing so accept cash.

In accordance with Art. 8*a* AMLA, dealers are subject to special due diligence requirements if they accept more than CHF 100,000 in cash in the course of a commercial transaction. They must verify the identity of the client and the identity of beneficial owner and they must keep records. They must clarify the economic background and purpose of a transaction if it appears unusual, unless its legality is clear. If there are indications that assets are the proceeds of a felony or an aggravated tax misdemeanor under Art. 305bis number 1bis SCC[45] or are subject to the power of disposal of a criminal or terrorist organisation (Art. 260ter SCC) or serve the financing of terrorism (Art. 260^{quinquies} para. 1 SCC) and, in case of suspicion of money laundering, predicate offence to money laundering, supporting or participating in a criminal or terror organisation or terrorism financing, they must report to the MROS.

[42] Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), SR 955.0.
[43] Swiss Criminal Code, SR. 311.0.
[44] Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), SR 955.0.
[45] Swiss Criminal Code, SR 311.0.

Facts

A client, resident in an Eastern Country and holding the nationality of that foreign country, visited a pharmacy in Switzerland. He purchased medicines for CHF 150,000, which he wanted to pay for in cash via a trustee to whom the invoices should be sent. Surprised by the process and aware of its anti-money laundering duties, the pharmacist had the client sign a declaration form relating to the beneficial owner and asked him for explanation. The pharmacy tried to clarify the economic background and the origin of the funds in accordance with its AMLA due diligence duties. The client remained vague about this large purchase of medicines and the transaction processing. Since the pharmacy did not receive enough information to verify the plausibility of the background of the transaction processing and the origin of the assets, he filed a report with MROS in accordance with Art. 9 AMLA.

Based on the legal principles MROS transmitted the information to a partner FIU.

Best practice for financial intermediaries

The payment of more than CHF 100,000 in cash immediately aroused the pharmacist's suspicions. He had the client sign a declaration relating to the beneficial owner of the funds. He asked the client for an explanation as to the origin of the cash. As his suspicions could not be allayed, he immediately reported the matter to MROS.

2.20 Case 20: Corruption – The unremitting Financial Intermediary

Preliminary remarks

This case illustrates the importance of identifying transactions that are not in line with the client's KYC profile, as the KYC is an instrument that also focuses on the detection of unusual transactions and the clarification of their economic background.

Facts

A client was onboarded by a financial intermediary. His account was intended to be used for wealth management activities. According to the KYC, the client made his wealth through his over 20 years of professional career in the commodities trading industry. During the onboarding process, his role was described as 'dealing with the physical aspects of the commodities trading (meaning: deal with customs, inspection, shipping aspects) and not with contracts'. The client accumulated significant revenues in particular through shares buyback programs.

In the beginning, the account transactions were in line with the indications in the KYC (i. e. inflows from same name account and from his employer for shares buyback, and a few personal expenses). Then, the financial intermediary received an instruction to pay USD 400,000 to a company in the Middle East. An invoice was received to prove the purpose of this payment. According to this invoice, which was sent to the client in his individual capacity, he recently purchased 12 cars from this company in the Middle East.

Based on the KYC, this transaction was not in line with account relationship, which is why the financial intermediary asked for additional clarifications. The initial clarification received from the client was that the entity in the Middle East was his brother's company, in charge of sourcing cars in the Middle East and in order to be re-sold in a state of West Africa at a later stage. The client claimed to have a trading activity there. A few days later, the client explained inconsistently that the entity in the Middle East was his cousin's company, that they are selling cars in a state of West Africa, and that the proceeds from the sale would be credited to his own account in the state of West Africa.

Due to the contradictory explanation received, the financial intermediary asked for additional confirmations, such as shareholding documentation of the company in the Middle East and the exhaustive cars purchase and re-sale contracts. A few hours later, the client cancelled the payment instruction. The financial intermediary searched on public sources and identified a profile presenting an individual named as owner of the said company in the Middle East. He was presumably the CEO of a fuel provider company, who was recently involved in a corruption and money-laundering case related to a state-owned firm.

Pursuant to Art. 9 AMLA[46], the financial intermediary reported the case to MROS for suspicions of money laundering in connection with the corruption of foreign public officials (Art. 322^{septies} SCC[47]).

Based on the legal principles MROS transmitted the information to the partner FIU.

Best practice for financial intermediaries

As the transaction did not correspond to the client's KYC profile, the financial intermediary immediately clarified the economic background of this transaction. Receiving contradictory explanations from the client, the financial intermediary unremittingly asked for further explanations and documents; always checking the information in parallel with OSINT research. The client finally interrupted his transfer order. The financial intermediary reported the case to MROS, who immediately got in touch with the FIU of the country of the company from which the funds were supposed to be transferred.

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

[47] Swiss Criminal Code, SR 311.0

3 Typology report Vol. II – Focus Enabler

3.1 Case 1: Enabler – Use of safe deposit boxes

Preliminary remarks

This typology illustrates, by way of example, the role of an attorney in concealing the origin of assets, particularly through the use of safe deposit boxes.

Facts

An attorney (hereinafter: the client), who maintained two business relationships with a financial intermediary, intended to open an additional account. The financial intermediary was aware that the client acted as a trustee in three other business relationships. As part of the onboarding process for the new account, the financial intermediary conducted an enhanced due diligence review. This review revealed several negative media reports linking the client to alleged money laundering activities (bribery) in South America. Based on these findings, the financial intermediary initiated an internal investigation.

During the course of this investigation, the financial intermediary discovered that one of the affected business relationships was associated with a safe. The intermediary had no knowledge of the content of the safe. The client stated, that the safe was used to store assets belonging to his clients. Furthermore, the financial intermediary found out, that the client had received a transfer of EUR 20 million into an account over which he held a general power of attorney. The amount was transferred in five separate tranches and originated from an Eastern European country. The transferring party was an offshore company based in the Far East. This company was reportedly majority-owned by an individual who was mentioned in the negative media reports and allegedly involved in money laundering activities in South America.

Finally, the financial intermediary identified, that one of the companies for which the client held a signatory authority may have been conducting activities requiring authorization as a financial intermediary, without being affiliated with a self-regulatory organisation (SRO).

Based on Art. 9 para. 1 let. a AMLA[48], the financial intermediary submitted a suspicious activity report to MROS. The suspicion concerned the alleged laundering of assets derived from bribery by foreign public officials in South America. MROS transmitted the case to the competent law enforcement authority.

Best practice for financial intermediaries

In the course of opening the account, the financial intermediary conducted an updated risk assessment and identified new suspicious information regarding the client. An internal investigation was launched, during which both, the use of a safe and the structured transfer (“smurfing”) of significant assets were uncovered. The timely report to MROS enabled swift transmission of the case to the competent public prosecutor’s office.

3.2 Case 2: Enabler – Board member / Trustee and a case of document forgery

Preliminary remarks

This case highlights the importance of regularly verifying the beneficial owner in existing business relationships, particularly when changes in transaction behaviour are observed. Financial intermediaries are reminded of their duty to conduct ongoing due diligence in accordance with AMLA[49].

Form A constitutes a document within the meaning of Art. 110 para. 4 SCC[50] in conjunction with Art. 251 SCC (cf. Federal Supreme Court decision 6B_988/2015 of 08.08.2016, E. 4.2). A board member or trustee who signs Form A without being the actual beneficial owner may be criminally liable for document forgery under Art. 251 SCC.

Facts

In late 2015, a Swiss company (hereinafter: the client) established a business relationship with a Swiss financial intermediary. According to the documentation submitted at the time, the company was intended to acquire and manage a property in

[48] Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), SR 955.0.
[49] Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), SR 955.0.
[50] Swiss Criminal Code, SR 311.0.

a neighbouring country. The client declared a Swiss national residing in another neighbouring state as the beneficial owner in Form A. This individual also served as chairman of the board and acted as a trustee, holding a board position in a law firm, also based in the same neighbouring country .

During the course of the relationship, the client reported a change in the beneficial owner for the account opened in 2015. While the original Form A from December 2015 listed the board member/trustee as the beneficial owner, the updated Form A, signed in 2023, named a European national residing in a European State. The individual was retired and had previously worked in a family-owned construction materials business located in the same town where the property was acquired and managed, as per the original KYC documentation. An official document from October 2022 confirmed his place of residence.

A transaction analysis revealed that, starting in January 2019, the account had processed over 100 incoming payments, totalling approximately CHF 1.5 million and over 110 outgoing payments, amounting to around CHF 900,000. Incoming payments mainly consisted of rental income and internal transfers from a bank in Europe. Outgoing payments included operational costs (e.g. energy, insurance, taxes), substantial cash withdrawals (approx. CHF 500,000), and management fees paid to the law firm, specifically to the declared beneficial owner.

A second account, opened in September 2023, recorded over 250 incoming payments totalling around EUR 900,000 and more than 80 outgoing payments amounting to approximately EUR 500,000. These transactions also related primarily to rental income and property operating expenses.

Several indicators suggested that the original declaration of the beneficial owner in 2015 may have been knowingly false:

- The location of the property matched the place of business of the newly declared beneficial owner.
- The board member/trustee was a seasoned financial professional.
- The client stated that the change in beneficial ownership was due to the transfer of shares to the European national, which had previously been held in trust.
- An excerpt from the share register dated August 2024 showed the European national as the sole holder of all 150 registered shares of the company.

Based on these findings, the financial intermediary could not rule out that the original declaration of the beneficial owner had been knowingly falsified. It is presumed that the “new” beneficial owner had already been the actual beneficial owner at the outset of the relationship in 2015, and that the trustee acted as a nominee.

In accordance with Art. 9 para. 1 let. a AMLA, the financial intermediary submitted a suspicious activity report to MROS. MROS subsequently transmitted the case to the competent public prosecutor’s office on suspicion of document forgery.

Best practice for financial intermediaries

The notification of a new beneficial owner prompted the financial intermediary to conduct a transaction analysis, which revealed a significant change in transaction patterns. This monitoring led to further investigations and raised questions regarding the actual beneficial owner. Due to the suspicion that the board member/trustee had acted as a nominee for several years, the financial intermediary reported the case to MROS. MROS was able to promptly transmit the case to the competent law enforcement authority.

3.3 Case 3: Enabler – Attorney and Oligarch

Preliminary remarks

This case exemplifies how an attorney may use accounts formally covered by a Form R for investment purposes that fall outside the scope of typical legal activities. Forensic legal services – such as legal advice and representation in court – are protected by professional secrecy under Art. 321 SCC[51]. Atypical legal activities, such as asset management, are on the other hand not covered by this protection.

[51] Swiss Criminal Code, SR 311.0.

Facts

A Swiss financial intermediary maintained several business relationships with an attorney, all of which were covered by Form R and operated as client accounts.

During a periodic review, the financial intermediary's transaction analysis revealed that the accounts in question were not linked to typical legal activities as defined under Art. 321 SCC. Specifically, substantial funds were credited to the attorney's accounts from another Swiss bank and from a bank in a foreign country. The transmitting accounts were held by companies fully owned by an oligarch from an Eastern European country who was suspected of misappropriating public funds.

The incoming funds to the attorney's accounts were declared as dividend income, to which the oligarch was the beneficial owner. These funds were allegedly intended for investments in bonds and real estate. Over a ten-year period, the total incoming funds exceeded CHF 90 million. In light of these findings, the financial intermediary requested the submission of Form A for the relevant transactions. The attorney subsequently declared the oligarch as the beneficial owner.

The financial intermediary exercised its right to report under Art. 305ter para. 2 SCC and submitted a suspicious activity report to MROS. MROS transmitted the case to the competent public prosecutor's office on suspicion of money laundering involving proceeds from criminal mismanagement.

Best practice for financial intermediaries

The financial intermediary identified that the account activity did not align with the client's originally declared professional activities. The transactions no longer reflected typical legal services. The intermediary requested the submission of Form A by the attorney, thereby enabling the identification of the beneficial owner. Based on negative information concerning this individual, the financial intermediary reported the case to MROS, which was able to promptly transmit it to the competent law enforcement authority.

3.4 Case 4: Enabler – Fiduciary active in the precious metals trade

Preliminary remarks

This case highlights the importance of thoroughly assessing the economic activities of clients by financial intermediaries – particularly when dealing with fiduciaries operating across multiple sectors.

Facts

The financial intermediary maintained a business relationship with a company (hereinafter: the client). According to the commercial register, the company's stated purpose was the trade, purchase, sale, and import/export of precious metals. However, the client informed the financial intermediary that its actual business involved the purchase and sale of industrial waste. The authorised signatory for the client was fiduciary X, who also held a minority shareholding. Fiduciary X was additionally the owner of fiduciary company Y, at which the client was domiciled via a c/o address.

Information available to the financial intermediary revealed that fiduciary X held executive roles in numerous other companies, active in sectors ranging from luxury goods to corporate formation and administration. The majority shareholder and beneficial owner of the client was primarily engaged in the precious metals trade and resided in France. He also held executive functions in various companies.

Due to the c/o address and the absence of personnel in Switzerland, the financial intermediary concluded that the client was, contrary to its own representations, a shell company domiciled in Switzerland. During ongoing monitoring of the business relationship, the financial intermediary further observed that companies controlled by the majority shareholder made numerous transfers to the client's account in Switzerland, without any discernible link to the nature of the services allegedly provided. Funds from the client's account were subsequently transferred to companies in which fiduciary X also held interests. These payment flows appeared economically irrational and raised suspicions of concealment.

The financial intermediary submitted a suspicious activity report to MROS pursuant to Art. 9 para. 1 let. a AMLA[52]. Based on additional findings, MROS transmitted the case to the competent public prosecutor's office.

Best practice for financial intermediaries

The financial intermediary conducted inquiries into the role of the minority shareholder, fiduciary X, and examined his business activities across various sectors. As the services allegedly rendered could not be reconciled with the observed financial flows, the financial intermediary submitted a report to MROS. Based on its analysis and information available through its databases, MROS was able to establish substantiated grounds for suspicion and transmit the case to the competent law enforcement authority.

3.5 Case 5: Enabler – Attorney and sanctions against Russia

Preliminary remarks

This case illustrates the risks that may arise when financial intermediaries enter into business relationships with attorneys whose activities extend beyond traditional legal representation.

Facts

A Swiss financial intermediary established a business relationship with an attorney of Russian origin (hereinafter: the client), who had been residing in Switzerland for over ten years. The client was the owner of a company specialising in tax advisory services, primarily targeting Russian-speaking clients. The scope of services offered did not fall within the traditional practice of law, and the attorney was therefore not registered in the Swiss Bar Register. Furthermore, the account held by the client with the financial intermediary was not covered by a Form R.

Characteristic for the business relationship was, that following the entry into force of sanctions against Russia, the client's company began acting as trustee or nominee shareholder for various Russian-speaking clients.

During a periodic review of the business relationship, the financial intermediary came across media reports suggesting that the client's tax advisory firm had been used both for money laundering purposes by Russian business partners and to circumvent sanctions imposed on Russia. Further inquiries revealed, that after the sanctions came into effect, payments from Russian counterparties were received into the client's accounts. These counterparties were suspected of acting as proxies for sanctioned oligarchs. Restructuring activities carried out immediately before or shortly after the sanctions came into force were considered additional indicators of suspicion.

The financial intermediary also began to question the accuracy of the information provided by the client in Forms A, K, and T, particularly in light of the suspected use of straw men.

Based on these findings, the financial intermediary submitted a suspicious activity report to MROS pursuant to Art. 9 para. 1 let. a AMLA. MROS received two additional reports concerning the same factual constellation.

MROS subsequently transmitted a report to the competent public prosecutor's office pursuant to Art. 23 para. 4 AMLA[53], due to reasonable suspicion of document forgery (in connection with "restructuring" and potentially falsified new Forms T and A). At the same time, MROS notified the State Secretariat for Economic Affairs (SECO) via administrative assistance under Art. 29 para. 2bis AMLA.

Best practice for financial intermediaries

Following the publication of press articles, the financial intermediary initiated a review of the business relationship. It identified ongoing restructuring activities involving the client's business partners, in which the client acted in a legal capacity, and established a link between the allegations raised in the media and the facts uncovered during its internal investigations. The financial intermediary subsequently reported the case to MROS, which was able to forward it promptly to the competent public prosecutor's office.

52 Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), SR 955.0.
53 Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), SR 955.0.

3.6 Case 6: Enabler – Life insurance, Offshore entity, and an unresolved homicide

Preliminary remarks

This case illustrates the duties of due diligence of an insurance institution in connection with the payout of a surrender benefit. Insurance institutions subject to the Insurance Supervision Act[54] that deal in direct life insurance qualify as financial intermediaries within the meaning of Art. 2 para. 2 let. c AMLA[55].

Facts

A Swiss insurance company (hereinafter: the financial intermediary) maintained a life insurance policy for a Swiss-based attorney (hereinafter: the client). The client intended to terminate the policy prematurely and claim the surrender benefit. In the course of the associated review, the financial intermediary conducted checks on both the client and a second policyholder, a Russian national residing in Switzerland.

The financial intermediary's investigations revealed that the premiums for both policies – amounting to over one million Swiss francs – had not been paid by the insured individuals themselves, but rather by a company domiciled in the Caribbean. The client explained that both he and the Russian national had provided consulting services to the Caribbean company via a Swiss entity. According to the contractual arrangements, the employer was responsible for covering the insurance premiums of the two consultants and settling them directly with the financial intermediary.

Further inquiries by the reporting financial intermediary uncovered significant grounds for suspicion: the Caribbean company was owned by the wife of a Russian national who had been sentenced to life imprisonment for corruption, membership in a criminal organisation, murder and tax fraud. The unresolved death of this wife further intensified doubts regarding the lawful origin of the assets under review.

Since the conclusion of the insurance contracts, premium payments had been processed via accounts held by the Caribbean company at a Swiss bank and its Asian branch. The origin of the funds appeared particularly suspicious, as they stemmed from the assets of the convicted individual, whose wealth management activities were apparently continued by the client – even after the assets had formally been transferred to the deceased wife.

Based on these findings, the financial intermediary submitted a suspicious activity report to MROS pursuant to Art. 9 para. 1 let. a AMLA, on suspicion of bribery of foreign public officials under Art. 322^{septies} SCC[56] and serious tax offences under Art. 305bis para. 1bis SCC.

Best practice for financial intermediaries

The request for the surrender benefit prompted the financial intermediary to re-examine both life insurance policies and their underlying circumstances. Particular attention was paid to the premium payments made by an offshore entity. The financial intermediary subsequently requested further information from both policyholders – the client and the Russian national – and conducted parallel open-source research on the paying entity. In light of the findings, the financial intermediary submitted a suspicious activity report to MROS.

3.7 Case 7: Enabler – The attorney and his pass through account

Preliminary remarks

This case illustrates the enhanced due diligence obligations of financial intermediaries in connection with third-party information relating to an investment fraud. In the context of fraudulent schemes, various circumstances may trigger special duties of due diligence under Art. 6 AMLA[57]. These include, for example, claims for restitution of previously transferred assets, indications from alleged victims, and official orders or decisions issued by competent law enforcement authorities.

54 SR 961.01.
55 Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), SR 955.0.
56 Swiss Criminal Code, SR 311.0.
57 Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), SR 955.0.

Facts

A Swiss financial intermediary maintained a business relationship with a licensed attorney domiciled in Switzerland (hereinafter: the client). The associated client account was opened with the submission of a Form R.

During the business relationship, the financial intermediary received a letter from a legal representative acting on behalf of alleged victims of fraud. These individuals believed they had purchased shares in a company X registered in a Southeast Asian jurisdiction and had transferred substantial amounts to the account held by the intermediary's client for that purpose.

In the course of its analysis, the financial intermediary identified systematic transaction patterns, notably closely timed incoming and outgoing payments. It observed repeated incoming payments from various counterparties, which the client subsequently transferred to accounts held at a bank in a Gulf state, where the investor relations officer allegedly responsible for distributing the shares of company X was believed to reside. The individual transaction amounts ranged from several thousand to over one hundred thousand Swiss francs, with total transfers exceeding one million francs.

In light of these findings, the financial intermediary requested a written explanation from the client. The client stated that he was acting under a mandate relating to the sale of a portion of the shares of company X. His assignment included verifying compliance with anti-money laundering regulations, particularly through the identification of purchasers and the actual execution of the share transactions.

The financial intermediary further discovered that company X was listed on several consumer protection websites as suspicious. Moreover, it had been mentioned by a supervisory authority in a neighbouring country of Switzerland in connection with an investment fraud. Publicly available sources also revealed that the managing director of the company X had previously been convicted in a European country for similar offences.

Based on these findings and the information concerning potential victims of fraud, the financial intermediary suspected that the business relationship with the Swiss attorney was being used as a pass through account in a fraudulent investment scheme. It therefore submitted a suspicious activity report to MROS pursuant to Art. 9 para. 1 lit. a AMLA, on suspicion of money laundering involving proceeds derived from fraud as defined in Art. 146 SCC[58].

MROS subsequently transmitted the case to the competent law enforcement authority pursuant to Art. 23 para. 4 AMLA.

Best practice for financial intermediaries

Immediately upon receipt of the letter from the victims' legal representative, the financial intermediary initiated internal investigations. It conducted a transaction analysis of the account opened with Form R and identified typical characteristics of a pass through account – particularly closely timed incoming and outgoing payments. The financial intermediary promptly reported the case to MROS and submitted the results of its analysis, enabling MROS to transmit the case swiftly to the competent law enforcement authority.

3.8 Case 8: Enabler – Proceeds from medical tests

Preliminary remarks

This case illustrates the abusive use of a client account as a vehicle for money laundering in connection with a suspected fraud scheme.

Facts

A Swiss financial intermediary maintained a business relationship with a company domiciled in Switzerland (hereinafter: the client). The account was operated under a factoring model to claim reimbursements from health insurers for medical tests conducted, thereby ensuring remuneration for the test centres and the responsible physicians.

In the course of this business relationship, the financial intermediary became aware of potential

58 Swiss Criminal Code, SR 311.0.

irregularities involving the client following critical media reports. According to these reports, the laboratories responsible for the testing lacked their own billing infrastructure. Furthermore, there were allegations that a significant portion of the tests for which reimbursements had been claimed and paid, had, in fact, never been conducted.

Against this backdrop, the financial intermediary subjected the client relationship to enhanced due diligence. It was found that the client had received payments totalling more than CHF 10 million, primarily from third-party companies. A substantial portion of these funds was transferred shortly after receipt to an attorney's account held with another financial intermediary.

Based on these findings, the financial intermediary submitted a suspicious activity report to MROS pursuant to Art. 9 para. 1 let. a AMLA[59], on suspicion of money laundering in connection with fraud as defined in Art. 146 SCC[60].

Following receipt of the report, MROS, acting under Art. 11*a* para. 2 AMLA, requested the relevant documentation from the third-party financial intermediary where the attorney's account was held and into which the client's proceeds had been deposited. MROS's analysis revealed that the account had been used to redistribute funds – presumably originating from fictitious tests – to various individuals who used the money for private purposes (e.g. the purchase of luxury watches, travel expenses, etc.). The main beneficiary of these transactions was also the subject of criminal proceedings in Switzerland for misappropriation. He was listed as wanted in Switzerland and was residing abroad.

MROS further established that one of the credit cards linked to the attorney's account was formally issued to a third party. However, an analysis of the credit card statements revealed that this individual had purchased airline tickets for the fugitive main beneficiary. The attorney's account at the third-party intermediary was used to obscure the identity of the ultimate beneficiary of this mechanism.

MROS subsequently submitted the case to the competent law enforcement authority.

Best practice for financial intermediaries

Upon receipt of substantial incoming funds, the reporting financial intermediary conducted a transaction analysis. The rapid transfer of funds to an attorney's account raised red flags. The use of the account as a pass-through vehicle prompted the intermediary to file a suspicious activity report with MROS. Acting pursuant to Art. 11*a* para. 2 AMLA, MROS promptly submitted an inquiry to the third-party financial intermediary where the attorney's account was held.

3.9 Case 9: Enabler – An escrow agreement and a straw man

Preliminary remarks

This case illustrates the role of legal professionals in the establishment and administration of complex structures. Such arrangements foster opacity and hinder the economic traceability of transactions.

An escrow agreement is a contractually regulated arrangement between the various parties to a transaction, whereby an independent third party acts as a trusted intermediary to receive and disburse funds or documents on behalf of the involved parties. The opening of such accounts by attorneys is, in principle, not protected by professional confidentiality within the meaning of Article 321 of the Swiss Criminal Code (SCC)[61].

Facts

A Swiss financial intermediary maintained a business relationship with a law firm (hereinafter: the client), for which it operated several escrow accounts. One of these accounts was used to process repayments of a loan granted by a client of the law firm to a foreign company. According to the client, this company was active in the oil and real estate sectors and, through a complex network of participations, ultimately owned by a businessman of Far Eastern nationality residing in Switzerland.

[59] Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA), SR 955.0.
[60] Swiss Criminal Code, SR 311.0.
[61] Swiss Criminal Code (SCC), SR 311.0.

The ownership structure was highly intricate, involving four Swiss companies located in different cantons, each managed by different attorneys, and supplemented by a Liechtenstein foundation. Notably, one of the involved attorneys was also a partner of the client. The reporting financial intermediary suspected that the businessman residing in Switzerland was acting as a straw man for politically exposed persons (PEPs), whose names had appeared in the media as shareholders of the company repaying the loan.

Following its internal clarifications, the financial intermediary concluded that the escrow accounts may have been used to facilitate transactions in favour of PEPs who had been linked to allegations of corruption in international media reports. The suspicion was reinforced by the excessive complexity of the structures and the lack of economic rationale behind the transactions, which appeared to occur between entities controlled by the same beneficial owner.

Based on the right to report under Art. 305ter paragraph 2 SCC, the financial intermediary submitted a suspicious activity report to MROS. The suspicion concerned money laundering in connection with the bribery of foreign public officials pursuant to Art. 322^{septies} SCC.

In another escrow account held by the same client, the financial intermediary identified further irregularities. This account showed high-volume pass-through transactions in favour of a domiciliary company. Upon inquiry, the client stated that the beneficial owner was a British trustee residing in a Gulf state. The financial intermediary considered this information not credible, as the same company had previously been flagged in another case involving fiduciary structures.

Approximately two weeks after the initial report, the financial intermediary submitted a second suspicious activity report to MROS, again based on Art. 305ter paragraph 2 SCC. In this case as well, there was a suspicion that the accounts were ultimately used for transactions benefiting PEPs. MROS transmitted the case to the competent law enforcement authority.

Best practice for financial intermediaries

The financial intermediary monitored the transactions on the escrow account and verified the origin of incoming funds. In doing so, it identified counterparties that had been negatively reported in publicly accessible sources. It also recognised complex corporate structures through which funds were transfered to the attorney's account. The intermediary promptly submitted a report to MROS, which was then able to transmit the case to the competent law enforcement authority.