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

Annual Report 2022

May 2023

Money Laundering Reporting Office Switzerland MROS

Annual Report 2022

May 2023

Federal Department of Justice and Police FDJP
Federal Office of Police fedpol
Money Laundering Reporting Office Switzerland MROS
3003 Bern

Tel.: (+41) 058 463 40 40
E-mail: meldestelle-geldwaescherei@fedpol.admin.ch

Website: www.fedpol.admin.ch

Table of contents

1. Foreword

As in the previous ten years, a significant increase in Suspicious Activity Reports (SARs) could be observed in the year 2022. The Money Laundering Reporting Office (MROS) of the Federal Office of Police fedpol received a total of 7,639 SARs, which corresponds to an estimated 13,750 business relationships and represents an increase of 28% compared to the previous year. At first glance, one might assume that part of this increase was linked to the sanctions imposed in the wake of Russia's military aggression against Ukraine. However, this is actually not the case. No significant change in the reporting behaviour of financial intermediaries was seen in this regard. Analysis of the SARs received by MROS shows that financial intermediaries understood the differences between the reporting systems (e.g. relating to sanctions, relating to money laundering, etc.) and knew which agency (State Secretariat for Economic Affairs SECO or MROS) was responsible in each case.

There was also an increase in the number of information requests from foreign financial intelligence units (FIUs). This is directly related to the new powers to obtain information (Art. 11*a* para. 2bis AMLA) which MROS has received as of 1 July 2021. Foreign FIUs have adapted to the new situation and are making increasing use of this instrument. The increase in information requests related not just to the number of incoming requests but also to the amount of information requested. In turn, MROS sent more of its own information requests to foreign FIUs and used the information received from them in its own analysis. Money laundering, organised crime and terrorist financing know no national borders, but rather spread globally. The international nature and complexity of the various scenarios have steadily grown in recent years. Accordingly, international cooperation in the fight against crime plays a crucial role. MROS strives to make active use of the international channels at its disposal and further deepened its relations with foreign FIUs during the reporting year.

In 2021, the Swiss Federal Audit Office (SFAO) conducted an audit of MROS activities and published its findings on 28 March 2022. The SFAO report gave a generally positive assessment of MROS and made five recommendations. In 2022, MROS set about implementing these recommendations in an effort to address the issues raised in the report. Fedpol drew up and adopted rules of procedure with criteria enabling a clear delineation of MROS activities. MROS also took a number of steps towards digitalisation and upgrading of its goAML (government office Anti Money Laundering) information system. At the heart of these efforts was the launch of the 'goAML-Futuro' project, which aims to expand the technical possibilities for receiving, processing and forwarding data. Action was also taken to further develop data management and strategic analysis (DSA) capabilities: MROS has so far managed to fully automate certain data processing proce-

dures. Finally, further progress was made on the 'Public-Private-Partnership – PPP' project. Here, MROS, in cooperation with other authorities and the private sector, explored the possibilities of setting up a PPP in Switzerland. MROS drafted a report on this subject, which it submitted to the Federal Council in April 2023.

Bern, May 2023

Federal Department of Justice and Police FDJP
Federal Office of Police fedpol
Money Laundering Reporting Office MROS

2. Main strategic developments

2.1 Public-Private-Partnership (PPP)

On 17 November 2021, the Federal Council instructed fedpol/MROS, to work with other authorities to explore the possibility of introducing a public-private-partnership (PPP) for the exchange of financial information. The aim of the PPP would be to further enhance the ability to tackle money laundering and terrorist financing in Switzerland.

In Switzerland, there is currently no partnership at national level between the public and private sectors to deal with money laundering or terrorist financing. However, the crime-fighting strategy devised by the Federal Department of Justice and Police (FDJP) sees closer cooperation between the public and the private sector as a cornerstone.[1] MROS's own strategy also calls for the creation of a PPP.[2] In its evaluation report dated 20 December 2021, the SFAO recommends that MROS move forward with plans to establish a PPP and expand its cooperation with financial intermediaries. This PPP should not be limited to banks, but should instead include the full range of financial intermediaries. All financial market participants subject to the Anti-Money Laundering Act should be encouraged to submit more SARs, in a timely fashion and improve the overall quality of the information that they provide. The SFAO also stresses that a PPP helps to prevent money laundering and can improve the effectiveness of the Swiss anti-money laundering system.[3] In particular, the SFAO draws attention to the fact that MROS is required by law to ensure that financial intermediaries understand what money laundering entails, are familiar with the various predicate offences, are able to recognise activities relating to organised crime and terrorist financing and thus to actively take preventive measures. The SFAO also highlights the importance of building up MROS's ability to conduct strategic analyses and considers the creation of PPPs and more extensive information sharing as key ways to achieve this objective.

Based on international standards and Swiss legislation, financial intermediaries play a crucial role in the fight against money laundering and terrorist financing. They are the closest to the clients and their money flows, and their assessment of the origin and use of assets is therefore the main starting point for anti-money laundering measures. When assessing business relationships and transactions, financial intermediaries rely on a database that is as comprehensive as possible. Ideally, this database should contain information that goes beyond the succinct details provided by clients. In turn, the authorities – above all MROS in Switzerland – also rely on information being as meaningful

---

1 Federal Department of Justice and Police (FDJP), *FDJP Strategy Paper on Measures to Fight Organised Crime, 2020–23 (in German)*, 22 June 2020.

2 See *2020 MROS Annual Report*, Chapter 2.2.

3 See *MROS Audit Report from the Swiss Federal Audit Office (SFAO-20146) dated 20 December 2021 (in German)*, p. 32 f. (published on 28 March 2022).

as possible. Information should not only be case-related, but also, if possible, provide a bigger picture and be useful for the so-called strategic analysis. By 'strategic analysis' we mean using information and data to recognise money laundering and terrorist financing methods and trends and thus assess the corresponding threats and risks. The term 'strategic analysis' is defined in the relevant international standards[4] aimed at countering money laundering and terrorist financing. The Federal Council Dispatch on the Anti-Money Laundering Act of 1996 is based on these international standards and thus already stresses the importance of strategic analysis. In this dispatch, MROS was given the mandate of implementing this legislation and competently informing financial intermediaries and authorities of the threat situation.[5]
In reent years, globalisation and digitalisation combined with the emergence of new technologies and business models have greatly increased the complexity and speed of transactions. Both financial intermediaries and the competent authorities have seen a sharp rise in the sheer volume of data. This development, which has been observed worldwide, makes it more difficult to limit our analysis to individual cases. This has led to greater emphasis being placed on strategic analysis. Closer cooperation between the authorities and the private sector can considerably improve the data situation and thus boost analytical capabilities on both sides. Such cooperation can also improve the defence mechanisms against money laundering and terrorist financing.
In the past year, MROS has held in-depth discussions with the State Secretariat for International Finance (SIF), the Federal Department of Foreign Affairs (FDFA), the Swiss Financial Market Supervisory Authority (FINMA) and a panel of banking and finance experts on the appropriateness and framework conditions of a PPP. The various authorities and experts involved in these discussions concluded that a PPP can greatly improve anti-crime efforts, particularly in terms of prevention. Previous experiences abroad seem to back this assessment. Today, over 20 of the 30 main financial centres have established at least one such partnership. The form and objectives of these PPPs vary greatly depending on the country and legal system. Moreover, there is no uniform standard for cooperation. The stakeholders involved consider the sharing of aggregated strategic information – i.e. information on trends, risks and methods – to be the best-suited option for a Swiss PPP. This is because the current legal framework only allows for a limited exchange of information. The sharing of case-related 'tactical information' (e.g. personal data, information from criminal proceedings, etc.) within a PPP would require far-reaching legal changes and is therefore not being considered at present. The establishment of a PPP is also supported by the majority of trade associations, indicating that they would like to actively take part in the process of creating such a PPP. There are different opinions and approaches on the question of how a PPP should be formed and what information should be shared. The sharing of strategic information is also considered as the 'least common denominator' by the industry associations – even if the benefits of having access to tactical information is considered greater in some cases.
MROS drafted a report[6] detailing the key outcomes of discussions with authorities and experts and pointing the way forward. This report was submitted to the Federal Council for consideration in April 2023. At the same time, MROS began discussing and working with the private sector to design a PPP that would operate under the current legal framework. The aim

---

4 *FATF-Recommendations 2012 – Updated February 2023*: Interpretive Note to R. 29 – Analysis (b), p. 104.

5 *BBl 1996 III 1101*: In the Federal Council dispatch on implementation of the 2012 revised FATF recommendations of 13 December 2013 (*BBl 2014 605*), the Federal Council writes the following: 'The new FATF recommendations stipulate that FIUs must conduct strategic analyses, which means using available or obtainable information, including information provided by other competent authorities, to analyse trends and patterns for the purpose of ascertaining whether money laundering or terrorist financing has occurred. So far, MROS has never carried out this type of analyses but will be expected to do so in the future.'

6 *Public-Private-Partnership (PPP) on the exchange of information in the fight against money laundering and terrorist financing*, March 2023.

is to establish a sustainable PPP as quickly as possible, which can take up its function. While the 'least common denominator' (i.e. the creation of a PPP where only strategic information is shared) is the current option moving forward, the sharing of operational/tactical information through the newly created PPP at some point in the distant future has not been ruled out. On the contrary, the involvement of all stakeholders lays the necessary foundation and support for the expansion of information sharing capabilities if the given situation warrants this.

2.2 Sanctions, their impact and limitations

Following Russia's military aggression against Ukraine, the Federal Council decided on 28 February 2022 to adopt the sanctions imposed by the European Union (EU)[7] against Russia. Based on the EmbA[8], the Ordinance of 27 August 2014 on Measures Relating to the Situation in Ukraine (hereinafter referred to as the 'Ukraine Ordinance') was fully revised on 4 March 2022.[9] This led to several other adjustments. Article 16 of the Ukraine Ordinance states that persons and institutions that hold or manage funds or have knowledge of economic resources, which are likely to be frozen under the provisions of the Ukraine Ordinance, have a duty to report to the State Secretariat for Economic Affairs (SECO). Banks – or authorised persons under Art. 1*b* BankA[10] – are also required to provide SECO with a list of deposits exceeding CHF 100,000 held by Russian nationals, natural persons residing in the Russian Federation, or held by banks, companies and organisations established in the Russian Federation.[11] The duty to report assets and economic resources to be frozen not only applies to financial intermediaries, but also to all persons or institutions that have knowledge of economic resources to be frozen. SECO has sole responsibility for monitoring compliance with the reporting obligation and the sanctions regime.

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 obligations under the AMLA[12] 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 investigations (Art. 6 AMLA). Depending on the outcome of these investigations, a SAR may be submitted to MROS.[13] In all cases, a SAR may only be submitted if there are reasonable grounds to suspect that the assets involved in a business relationship are: being used to support a criminal or terrorist organisation; are being used for money laundering purposes; constitute proceeds from a felony or a qualified tax offence; are at the disposal of a criminal or terrorist organisation or are being used for terrorist financing purposes. According to Art. 10 para. 2 SCC, felonies are defined as offences that carry a custodial sentence of more than three years. A violation or evasion of sanctions as such only qualifies as a felony in serious cases – a simple violation of sanctions therefore does not constitute a predicate offence within the meaning of anti-money laundering legislation.[14] Suspicion of a simple

---

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

8 Federal Act of 22 March 2002 on the Implementation of International Sanctions (Embargo Act, EmbA), SR 946.231.

9 *Ordinance of 4 March 2022 on Measures Relating to the Situation in Ukraine, SR 946.231.176.72.*

10 *Federal Act of 8 November 1934 on Banks and Savings Banks* (Banking Act, BankA), SR 952.0. Authorised persons under Art. 1*b* BankA are persons who mainly work in the financial sector and who accept deposits on a professional basis from private individuals of up to CHF 100,000,000 or crypto-based assets designated by the Federal Council. Authorised persons may also include individuals who publicly promote their services and who neither invest nor earn interest on these public deposits or assets.

11 Art. 21 Ukraine Ordinance.

12 Federal Act of 10 October 1997 on Combating Money Laundering and the Financing of Terrorism (Anti-Money Laundering Act, AMLA), SR 955.0.

13 Right to report (Art. 305ter para. 2 Swiss Criminal Code [SCC], SR 311.0) or duty to report (Art. 9 AMLA).

14 Art. 32 para. 1 Ukraine Ordinance in conjunction with Art. 9 para. 1 and 2 EmbA.

violation or evasion of sanctions does not in itself trigger a SAR to MROS.
MROS continuously monitored and analysed the situation in connection with the above-mentioned sanctions regime – whenever this was relevant from a money laundering and terrorist financing perspective. Overall, it can be said that the sanctions ordered in March 2022 did not have a significant impact on MROS in terms of SAR processing. There was no significant change in the reporting behaviour of financial intermediaries. Although some SARs pertained to violations and evasion of sanctions, most of these were also related to suspicions of money laundering, organised crime or terrorist financing. Based on experiences so far, MROS can confirm that financial intermediaries have a very clear understanding of the difference between reporting systems (sanctions versus money laundering) and also fully understand the different areas of authority (SECO or MROS) and have therefore been submitting their SARs in a differentiated manner. 'False reports' or 'pre-emptive reports' were only found in a few isolated cases. It can therefore be said that the recent increase in SARs for 2022 is not due to the sanctions regime (see Chapter 4).
It should be noted that in the context of international cooperation with partner authorities, information on sanctions violations and evasion was provided to MROS on a number of occasions. In cases where the legal requirements were met, MROS then forwarded this information to the competent authorities in Switzerland. At the same time, foreign partners also showed a growing general interest in Switzerland's anti-money laundering legislation. In 2022, MROS received several enquiries regarding whether or not specific economic branches or parts thereof were subject to anti-money laundering legislation. Specifically, our partners wanted to know about legislative provisions concerning the real estate market, trade in fine art and luxury goods and how legislation applied to lawyers and consultants.

2.3 Implementation of recommendations from the Swiss Federal Audit Office (SFAO)

MROS was the subject of an audit by the Swiss Federal Audit Office (SFAO) in 2021. Their findings were presented in a corresponding audit report dated 28 March 2022.[15] This audit yielded many positive findings. The SFAO found MROS's strategy to be convincing and felt that MROS was effective in achieving goals. The SFAO also gave a positive rating to MROS's current structure and judged its processes to be adequate. It further noted that cooperation with national and international authorities was constructive. Finally, the SFAO made five recommendations in its audit report. In 2022, MROS took steps to implement these recommendations and pushed for further progress to be made on the relevant issues raised.

2.3.1 Recommendation 1: Issue rules of procedure to regulate interactions between fedpol and MROS

In its report dated 20 December 2021, the SFAO concludes: '*MROS is adequately integrated into fedpol's structures and processes. The SFAO did not identify any situation where fedpol undermined the required operational independence of MROS. However, the issue of independence does not need to be interpreted in an overly absolute manner. Ultimately, it makes sense for MROS and the other divisions of fedpol to work closely together in the fight against money laundering. This was also the view of lawmakers when they assigned MROS to the Federal Office of Police (then FOP, now fedpol). However, due to the special position and growing importance of MROS, it would be advisable to have rules of procedure similar to those used for internal audits of federal departments and offices: These rules of procedure should help clarify what is and is not included in fedpol's 'management' of MROS under Art. 23 para. 1 AMLA. The FDJP's General Secretariat*

[15] See Swiss Federal Audit Office (SFAO), *Audit no. 20146: 'Fulfilment of tasks by the Money Laundering Reporting Office Switzerland – Federal Office of Police' (in German)*, March 2022 as well as a brief summary of the audit findings in the *2021 MROS Annual Report*, Chap. 2.1 (p. 8).

(GS) and/or FDJP's Financial Inspectorate (FISP) could also play a role in the drafting or monitoring of these rules of procedure. The SFAO therefore recommends that fedpol work with the FDJP GS to draft rules of procedure for MROS. The FISP could also periodically check to verify MROS's operational independence and compliance with the rules of procedure.'[16]

Fedpol manages MROS.[17] The issue of the subordination and operational independence of MROS is therefore relevant. Both the Financial Action Task Force (FATF)[18] and the Egmont Group[19] have established rules on the operational independence and autonomy of financial intelligence units (FIUs)[20] and regularly check compliance with them. Basically, all FIUs must remain independent in terms of their core operational processes. When analysing cases, they must be free to decide for themselves whether and what to forward to a prosecution authority. Likewise, the confidentiality of sources of SARs must be guaranteed at all times. FATF Recommendation 29 provides that each country should establish an FIU to act as a national centre for the receipt of suspicious transaction reports and other information relevant to money laundering, associated predicate offences and terrorist financing.[21] According to this recommendation, each FIU is also responsible for analysing these reports and information and for disseminating the results of that analysis. An FIU should be able to obtain additional information from reporting entities, and should have timely access to information from financial intermediaries, administrative and prosecution authorities in order to perform its functions properly.

In its 2016 assessment of Switzerland, the FATF did not criticise the fact that MROS is a part of fedpol. Generally speaking, both the Interpretive Note to FATF Recommendation 29 and the Egmont Guidelines[22] (which refer to FATF Recommendation 29) state that an FIU may be established as part of an existing authority as long as the FIU's core functions remain distinct from those of the other authority. The FATF confirmed that fedpol's influence on MROS was organisational and not operational in nature. The core tasks of MROS are described in Art. 23 AMLA and differ from those of fedpol.

Fedpol/MROS followed up on the SFAO's recommendation in 2022 and issued corresponding rules of procedure. The challenge was to describe the division of tasks between fedpol and MROS as clearly as possible in order to satisfy FATF and Egmont Group requirements as best as possible. However, the general administrative structure of MROS and its organisational and hierarchical integration within fedpol are clearly anchored in legislation and cannot be negated by rules of procedure. In other words: rules of procedure/regulations must fit into the corset of the general government structure. The resulting rules of procedure, which came into force on 1 November 2022, are based on four main pillars:

– No 1 – Organisational aspects: MROS is managed by fedpol by virtue of Art. 23 para. 1 AMLA. From an organisational and hierarchical standpoint, MROS is part of the Directorate of Crime Prevention & Legal Affairs (CPL). As part of fedpol, MROS is subject to all organisational, personnel and administrative regulations and directives issued by the Federal Administration as a whole, as well as by the FDJP and fedpol.
– No 2 – Operational tasks: MROS's operational tasks are largely derived from the AMLA and

16 See Swiss Federal Audit Office (SFAO), *Fulfilment of tasks by the Money Laundering Reporting Office*, March 2022, p. 19 f., see Chap. 2.1.

17 Art. 23 para. 1 AMLA.

18 *Homepage Financial Action Task Force (FATF)*.

19 *Homepage Egmont Group of Financial Intelligence Units*.

20 MROS is Switzerland's financial intelligence unit (FIU) and has been a member of the Egmont Group since 1998, which brings together over 165 FIUs worldwide. This organisation enables information to be shared globally in a secure, rapid and legally permissible manner, thus sustaining efforts to combat money laundering and terrorist financing.

21 *The FATF-Recommendations 2012 – Updated February 2023: R.29* – Financial Intelligence Units, p. 24 and 102.

22 *See Egmont Group of Financial Intelligence Units Operational Guidance for FIU Activities and the Exchange of Information* 2013 – Updated 2017.

the MROSO[23] and are based on MROS's and the FDJP's respective crime-fighting strategies. The main task is the reporting system (receiving SARs, analysing and forwarding of information to the competent prosecution authorities). In addition, MROS is a member of the Egmont Group, exercises the rights and duties associated with this status and maintains diplomatic ties with partner FIUs abroad. MROS also acts as a specialised agency in the fight against money laundering and terrorist financing and is involved in a number of preventive tasks (raising awareness among financial intermediaries, working in expert groups, conducting training courses, etc.).

– No 3 – Operational independence of MROS: MROS is free to decide how to carry out and prioritise its tasks. It is important to note that fedpol provides the financial and human resources needed by MROS to carry out its remit, while complying with the organisational and budgetary guidelines of the Federal Administration. Other points in these regulations concern the employment of staff, data protection and travel.
– No 4 – Verification of operational independence: Finally, the rules of procedure contain rules on verification and escalation. Accordingly, the FDJP's Financial Inspectorate (FISP)[24] is responsible for periodically verifying the operational independence of MROS. It then drafts a brief report summarising its findings and, if necessary, makes recommendations. The FISP is also the authority in charge of assessing ambiguities when it comes to matters of independence.

These rules of procedure provide MROS and fedpol with criteria enabling a clear delineation of MROS activities. The adoption of these rules of procedure was assessed as positive in an audit by the Egmont Group, which took place in 2022.

2.3.2 Recommendation 2: goAML optimisation project

In its report, the SFAO states the following on the subject of digitalisation: '*With the introduction of goAML, MROS has achieved noticeable efficiency gains thanks to digitalisation. However, the average processing time can be reduced even further. In order to achieve this, automated database queries and a (partially) automated triage (especially for smaller cases) are needed. Thus, MROS will be able to handle further increases in SARs through greater automation instead of additional human resources. This should allow financial analysts to perform more in-depth analyses instead of diverting their attention to time-consuming database queries. Improving the quality of the data provided by financial intermediaries via the 'goAML' information system is crucial. Progress is also needed in the area of strategic analyses, which would require a good statistical tool, a business intelligence module and a business warehouse. Additional tools will be needed to optimise standard goAML software for this purpose. Other FIUs are already further ahead in this area than MROS. The SFAO recommends that fedpol prioritise the goAML optimisation project and set a date for implementation, especially with regards to the automation of database queries.*'

In 2022, MROS took several measures relating to digitalisation and further development of goAML, the most important of which was the launch of the 'goAML-Futuro' project. It aims to provide greater technical support and automation for certain processes in the receipt of SARs, the processing and analysis of data, and the communication with the various stakeholders (financial intermediaries and authorities). Specifically, action will be taken to eliminate the following persistent weaknesses:

– Lack of interoperability (automatic database connection): MROS still lacks an automat-

[23] Ordinance of 25 August 2004 on the Money Laundering Reporting Office Switzerland (MROSO), SR 955.23.

[24] The Financial Inspectorate (FISP) of the Federal Department of Justice and Police (FDJP) is described as an internal auditing body of the FDJP and its subordinate organisational units within the meaning of Article 11 of the Swiss Federal Audit Office Act (FAOA), SR 614.0.

ed connection to existing databases, even though this was already planned back in 2016.
– Lack of connection with the Swiss Federal Archives: So far, no IT solution has yet been found to ensure the legally required transfer of data to the Swiss Federal Archives.
– Potential of goAML has not yet been fully exploited: goAML's current configuration in MROS operations does not enable the full range of technical tools that goAML offers to be used. 'Templates' are the most notable example: MROS analysts have to manually 'copy' any data that they wish to transmit to prosecution authorities from the database and send this data in separate Word templates. They have to do this even though goAML offers very good templates that could be used to automate this process 'with a click of a button'.

The project will also help to improve the overall user-friendliness of goAML. In particular, this means improving the web upload interface for financial intermediaries. Where possible, data gaps detected during analysis should be eliminated, thus simplifying statistics and evaluation. There are also plans to digitalise communication with other authorities and optimise the process of administrative assistance. For MROS, the digitalisation of analysis is also important because it allows to recognise relevant information sooner, more effectively and more quickly, thus reducing operational risks.
The goAML-Futuro project is intended to develop a user-friendly and intuitive system. Over time, this will streamline MROS processes and minimise latent data processing risks. In addition to improving the current situation, the project also addresses the matter of how system support will be provided at MROS in the future. The medium to long-term needs of MROS are thus being evaluated.
The goAML-Futuro project was launched on 1 January 2023 and will be backed by closer cooperation with the UNODC.[25] The latter will actively assist MROS in the further upgrading of goAML, especially on-site. In 2022, in-depth discussions were held between MROS and foreign partner FIUs that also use goAML. In this regard, too, MROS will intensify this dialogue in the future in order to enable mutually beneficial sharing of existing know-how in the areas of digitalisation and automated data processing.

2.3.3 Recommendation 3: Development of the DSA division

In its report dated 20 December 2021, the SFAO states the following with regard to strategic analysis capabilities: *'Strategic analyses and statistics are still not sufficiently developed to provide an overall picture of the effectiveness and efficiency of anti-money laundering efforts in Switzerland as required under FATF Recommendation 33.26 The lack of staff in the division 'Strategic Analysis' makes it hard to gain an overview or data concerning the entire process chain and SAR 'life cycle'. MROS would need to have this information in order to assess the effectiveness of SAR processing. For data analysis, MROS would require specialists and suitable IT tools. Much of MROS's work still has to do with the processing of individual SARs. As such, it is constantly under pressure to handle the large volumes of SARs within a reasonable period of time. There is a risk of losing sight of the bigger picture. Not only should statistical data be collected, but also be interpreted and lead to specific action. The SFAO recommends that fedpol develop the division 'Strategic Analysis' within MROS, as was originally planned under strategic objective 3.1.'*
For MROS, the development of strategic analysis remains a key pillar of its strategy. In order to be able to identify money laundering trends and methods and share information through a public-private-partnership, it first needs to be able to carry out regular consolidated analysis of data, which can then be viewed in light of other available information. The insights gained from strategic analysis can also be used to determine the effectiveness of the reporting system – par-

[25] United Nations Office on Drugs and Crime (UNODC).
[26] *FATF Recommendations 2012 – Updated February 2023: R.33* – Statistics, p. 25.

ticularly in view of the next FATF evaluation – and for implementing the MROS strategy.
In 2022, MROS significantly developed the division 'Data Management and Strategic Analysis (DSA)'. Nowadays, modern FIUs depend on staff who are specialised in database architecture, data structuring and programming. Their knowledge and know-how provide financial analysts with a stable foundation for their work and help to improve the efficiency of both operational and strategic analysis. In 2022, MROS managed to fully automate certain data processing procedures. As a result, MROS is now able to retrieve key statistical data from the system on a daily basis, leading to better overall effectiveness. Improved technical support and the automation of certain steps in the triage process have also shortened MROS's processing times and largely reduced its backlog of pending cases.[27] MROS will continue its DSA development work in 2023. With the initialization of the project 'goAML-Futuro' and the intensified cooperation with the UNODC (see Chapter 3.4), essential prerequisites are created to achieve the ambitious goals of MROS in terms of analytical capability.

2.3.4 Recommendation 4: Create a Public-Private-Partnership

Chapter 2.1 covers aspects relating to implementation of Recommendation 4. The aim is to work with the financial sector to establish a sustainable PPP as quickly as possible, which can take up its function. MROS will press ahead with this project in 2023.

2.3.5 Recommendation 5: Strengthening the cooperation between MROS and FINMA

In its report dated 20 December 2021, the SFAO states the following with regard to the sharing of information at national level: '*The sharing of information at national level (public-public partnership) should be intensified. Swiss anti-money laundering measures are more effective if they are coordinated. To achieve this, the Swiss authorities must remove legal hurdles that make cooperation difficult and improve the interoperability of their systems. MROS and FINMA should work closely together and speak with one voice to financial intermediaries. FINMA – and with it also the supervisory organisation (SO) and self-regulating organisations (SRO)28 – are able to exert greater leverage than MROS due to their ability to conduct on-site inspections of financial intermediaries. They therefore have the authority, but also the duty, to use this leverage in support of MROS activities. Under the Gambling Act (GamblA)29, FINMA, the SO, the SROs, the Swiss Federal Gaming Board (SFGB) and intercantonal supervisory and executive authorities also need to more readily apply their subsidiary duty to report under Art. 16 and Art. 27 para. 4 AMLA. The argument that supervised parties report themselves or are encouraged to do so is only partially true, as in some cases, FIs send their SARs to MROS years late, submit incomplete information or do not submit SARs at all. Similarly, certain supervised sectors hardly ever report to MROS (e.g. lawyers, notaries, commodities and precious metals traders, foreign exchange traders and dealers). The SFAO recommends that fedpol/MROS enhance its cooperation with FINMA and formalise this cooperation by means of a cooperation agreement.'*
As in previous years, MROS and FINMA periodically discussed anti-money laundering measures and specifically the reporting behaviour of financial intermediaries. MROS raised the issue of data quality with FINMA and provided it with relevant information on individual institutions. In its 2022 annual report[30], FINMA states the following: *'In recent years, the number of suspicious transaction reports being submitted by banks to the Money Laundering Reporting Office Switzerland (MROS) has grown significantly. In order that the*

---

27 Only 6% of the SARs that MROS received in 2022 were still pending as of 31 December 2022.

28 With the entry into force of the new Art. 29*b* AMLA on 1 January 2023, information can also be exchanged with supervisory organisations (SOs) and self-regulating organisations (SROs).

29 Since 1 January 2023, the Central Office for Precious Metals Control must also be notified (see Art. 16 para. 1 AMLA).

30 *FINMA Annual Report 2022, p. 38*

MROS can process these reports effectively, and is then in a position to swiftly implement measures based on the findings drawn from those reports, the quality of the reports is also a very important factor. On numerous occasions during 2022, FINMA observed a lack of quality in the suspicious transaction reports submitted to the MROS by financial intermediaries. For example, documents were missing, factual circumstances had not been correctly recorded, or account information had not been provided in sufficient detail. The MROS has confirmed this state of affairs. Systematic shortcomings in data quality may be indicative of organisational defects and deficient processes and control measures among the financial intermediaries.'

MROS regards the current level of information exchange and cooperation with FINMA to be very satisfactory. At present, there is no reason to formalise this cooperation any further.

MROS also shared information with the Central Office for Precious Metals Control and SROs in 2022. From its perspective, MROS sees considerable money laundering risks both in precious metals trading and in the para-banking sector.

3. goAML information system

In January 2020, MROS introduced the goAML information system, which allows SARs to be submitted, received and processed electronically. The goAML system is a key element in the implementation of MROS's strategy for digitalisation and optimisation. After only three years, it has become the standard tool used by financial intermediaries to submit SARs. The system runs smoothly with minimal service disruption. The proportion of SARs submitted to MROS via goAML has been steadily rising, approaching the 100% mark (see Chapter 3.1). Swiss authorities are also increasingly using goAML to submit their requests for administrative assistance electronically. In addition, prosecution authorities use the same system to notify MROS of action taken on those SARs.
As in previous years, the quality of the information submitted by financial intermediaries remains a major challenge for MROS. In 2022, MROS again had to reject a significant number of SARs because the financial intermediaries did not enter the mandatory information correctly in the goAML database (see Chapter 3.3). The planned rollout of goAML 5 in 2023 and the corresponding adaptation of the XML framework[31] will give MROS an opportunity to work with FIs to clarify rules and introduce new technical solutions to simplify FI reporting.

3.1 Proportion of SARs and information submitted electronically

MROS notes that the proportion of SARs and responses to MROS requests under Art. 11*a* AMLA submitted electronically continued to increase in 2022.

Proportion of SARs and (spontaneous) information that were submitted electronically

2022	2021	2020
98%	95%	90%

Proportion of replies to requests for information under Art. 11*a* AMLA that were submitted electronically

2022	2021	2020
92%	85%	68%

MROS can only fully exploit the technical and analytical possibilities of the goAML system when SARs are submitted electronically. Paper SARs, on the other hand, require an above-average amount of time to enter, scan and link with already existing information in the system. MROS is therefore taking active steps to further increase the proportion of SARs and information submitted electronically.

[31] The XML framework mentioned here establishes the structure of the information that financial intermediaries provide to MROS in an XSD format file. More information on the XML framework can be found on the MROS website. See *https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/geldwaescherei/meldung.html*.

3.2 Fully automated transfer using .xml files

Of the SARs received via goAML, an average of 61% (previous year 60%) were sent to MROS by FIs using fully automated transmission. This fully automatic transmission using .xml files also optimises requests under Art. 11*a* AMLA. This is particularly important as the number of MROS enquiries under Art. 11*a* para. 2bis AMLA is expected to increase. With fully automatic transmission of the requested documents, FIs can save considerable time and effort.

3.3 Rejected SARs

When a financial intermediary submits a SAR to MROS, specially trained MROS staff check whether the information submitted meets minimum legal requirements (Art. 3 MROSO) and complies with the goAML guidelines published by MROS.[32] The aim of the latter is to ensure that the information contained in electronically submitted SARs matches the structure of the goAML template. Further analysis of rejected SARs also shows that information uploaded via XML is rejected far less often than manually entered information.[33] Despite clear user instructions[34], MROS regularly had to return SARs and replies to requests for information under Art. 11*a* AMLA to the financial intermediaries, asking them to supplement the missing information and documents or to revise incorrectly entered data. In many cases, account information is missing (accounts not mentioned, missing balance amounts or balance dates) or no mention is made of authorised signatories.
The rejection rate is still high (14%) and MROS has managed to bring this figure down by manually correcting the data in the system in certain cases. In 2023, MROS intends to pay even closer attention to incoming data and consistently reject incorrect data records in order to improve the quality of the SARs submitted by financial intermediaries. A new version of goAML (version 5) will simplify data entry and verification of data quality. This makes it possible to dynamically design input fields and create forms that more accurately reflect the given situation at hand.

3.4 Future of goAML/goAML 5

As the developer of goAML software, the UNODC is fully committed to the product and has announced its intention over the next few years to continuously adapt the application to the latest needs and keep it at the cutting edge of technology and security. To achieve this, UNODC has been working closely with the countries that use goAML. It also works with several organisations and companies that have specific expertise in complex areas such as virtual currencies and trade-based money laundering as well as with companies that offer innovative IT security solutions. These efforts have paid off. During the reporting year, a number of major enhancements were introduced with the latest software release (goAML 5). After intensive testing, MROS decided to adopt goAML 5, which was made available at the end of October 2022. MROS expects that the new version of goAML can be installed and brought online in the second half of 2023. With the new version, various changes to the XML template will be needed. This will have an impact on FIs that use automatic reporting interfaces. Fortunately, goAML 5 will be 'backward compatible': during the transition period, FIs will still have the ability to submit SARs and information using the previously valid template. This will give them enough time to adapt their internal systems. MROS is striving to keep the burden on financial intermediaries as low as possible – however, adjustments will be unavoidable in 2023 and 2024.

3.5 Newsletter

MROS sent four newsletters to goAML-registered FIs in 2022. In these newsletters, MROS covered general topics relating to the use of the goAML system. It also provided information regarding possible changes in practice and discussed vari-

[32] In particular, on the *MROS homepage* (handbooks, FAQs, factsheets).

[33] 75% of the rejected information was previously entered manually by FIs in the goAML system.

[34] Handbooks, FAQs, factsheets are provided by MROS.

ous legal issues. The fourth newsletter published at the end of November dealt exclusively with the changes to the AMLA that came into force on 1 January 2023, based on proposals made by the State Secretariat for International Finance (SIF). MROS described how these legislative changes will be implemented in the goAML system.[35]

3.6 Contact MROS/goAML Hotline

In 2022, MROS installed a new call centre application for the goAML hotline to enable improved assessment of hotline usage. The number of callers remained constant in the reporting year compared to the previous year.

[35] goAML newsletters are now available and can be found in a corresponding folder in the goAML system.

4. Annual MROS statistics

Since goAML was introduced on 1 January 2020, MROS has changed the way it counts SARs: it now counts the number of SARs and not the number of reported business relationships, as was the case up to 2019. Since a SAR can contain several business relationships, it is difficult to make a precise comparison with the figures prior to 2020. Nonetheless, in order to enable a comparison with the statistics of previous years, we have decided to publish percentage figures where possible.

4.1 Overview of MROS statistics for 2022

- *In 2022, MROS received a total of 7,639 SARs, i.e. an average of 30 SARs per working day. This is an increase of 28% over 2021 (5,964 SARs). It is more than double the increase in 2021 (+12%) and the largest since 2018 (+31%).*
- *The overwhelming majority of SARs once again came from the banking sector (92%).*
- *MROS sent 1,232 notifications to the prosecution authorities in 2022, 17% fewer than in 2021 (1,486 notifications). This illustrates the importance of MROS as a filter, how it focuses on the priorities of the prosecution authorities and the FDJP's crime strategy, and how it makes optimal use of the available resources.*
- *The number of requests MROS made to financial intermediaries under Art. 11a para. 2 and 2bis AMLA[36] rose in 2022 by around 38%. The increase is primarily due to the introduction of Art. 11a para. 2bis AMLA in 2021. It is also a result of implementing the MROS strategy adopted in 2020, which provides for the optimal support of the prosecution authorities and requires the in-depth analysis of certain SARs. Consequently, MROS is now also obtaining information from financial intermediaries not directly involved in the reporting process, i.e. third-party intermediaries.*
- *MROS received 667 requests for information from other Swiss authorities in 2022, which represents an increase of 19% compared with 2021. The exchange of information between MROS and other Swiss authorities is steadily increasing.*

[36] Art. 11*a* para. 2 and para. 2bis AMLA provide the legal basis for MROS to request information from third-party financial intermediaries, i.e. those who have not submitted a SAR (see Chapter 4.9).

Table 1

Summary of 2022 reporting year (1 January – 31 December 2022)

Reporting volume	2022 Absolute	2022 Relative
Total number of SARs received	**7639**	**100,0 %**
Analysed SARs	7175	93,9 %
SARs still under analysis	464	6,1 %
Type of financial intermediary		
Bank	6999	91,63 %
Other financial intermediary	163	2,13 %
Payment service provider	150	1,96 %
Credit card company	125	1,64 %
Casino	52	0,68 %
Asset manager/investment advisor	45	0,59 %
Commodity and precious metal trader	24	0,31 %
Loan, leasing, and factoring business	22	0,29 %
Insurance company	21	0,27 %
Currency exchange	20	0,26 %
Fiduciary	8	0,10 %
Securities trader	8	0,10 %
Attorney	2	0,03 %
Trustee	0	0 %
Self-regulatory organisation (SRO)/ FINMA/SFGB/Gespa	0	0 %

The table above provides an overview of the SARs received by MROS in 2022, but not of all SARs processed in that year. At the end of 2021, 1,080 SARs were still pending: although they were processed during 2022, they do not appear in the table above (see Chapter 4.10). In addition, 464 SARs received in 2022 – and therefore counted in the table above – were still under analysis on 31.12.2022.[37]

Table 2

Notifications	1,232	100,0 %
To the Office of the Attorney General of Switzerland	79	6,4 %
To the cantonal prosecution authorities	1,153	93,6 %

Table 2 shows the number of notifications MROS made to the prosecution authorities in 2022 based on Art. 23 para. 4 AMLA. These notifications include an analysis report drawn up by MROS on the basis of the information at its disposal. This can include information from authorities in Switzerland and from abroad as well as from SARs not necessarily submitted to MROS in the same year (see Chapter 4.10).

4.2 Suspicious Activity Reports (SARs)

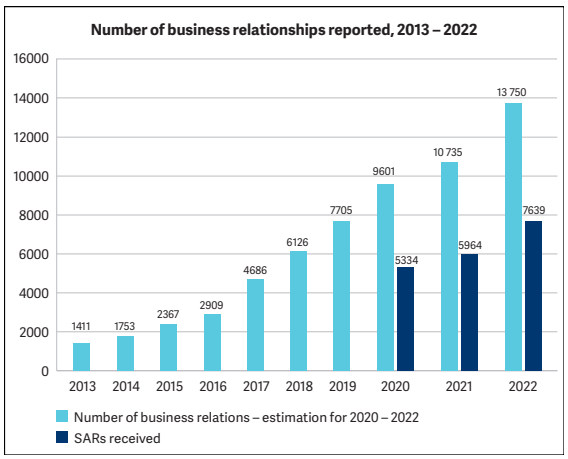
In 2022, MROS received 7,639 SARs, i.e. an average of around 30 SARs per working day. This is an increase of 1,675 SARs (+28%) over the previous year. The relative increase is more than double that of 2021 (+12%) and the largest since 2018 (+31%).

The steady increase in the number of incoming SARs over the past ten years thus continued in 2022 (see Diagram 1). In 2014, 1,411 suspicious business relationships were reported to MROS, whereas in the current reporting year an estimated 13,750 business relationships were reported.[38] Hence, the number of business relationships reported each year increased nearly tenfold between 2014 and 2022. There are several reasons for this increase, the most important ones being the increased awareness of financial intermediaries to the issue of money laundering, legal adjustments particularly in connection with the definition of 'reasonable suspicion', and progress in digitalisation, e.g. better tools for transaction monitoring and internal analysis.

[37] MROS therefore analysed 8,255 SARs in 2022 (7,175 SARs from 2022 in addition to 1,080 SARs that were still under analysis at the end of 2021).

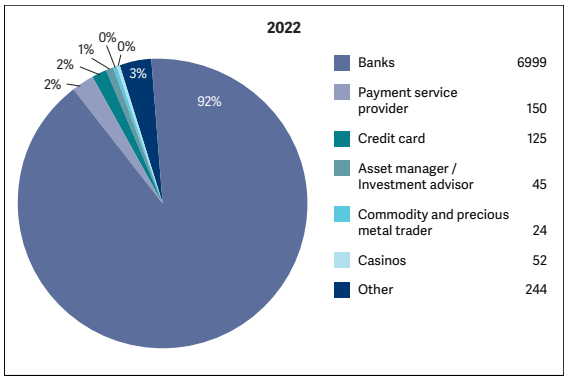
[38] The method of counting SARs changed with the introduction of goAML. In order to be able to compare the figures with previous years, MROS has taken the number of SARs submitted and multiplied this figure by 1.8, i.e. the average number of business relationships per SAR. That means the 7,639 SARs submitted in 2022 are the equivalent of 13,750 business relationships.

Diagram 1



4.3 SARs categorised by financial intermediary sector

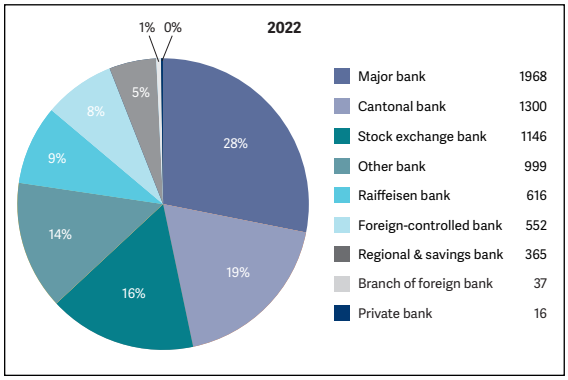
Diagram 2



– Nearly 92% of SARs were submitted by the banking sector (+2% over 2021).
– Compared with the previous year, the relative variation in reporting volume by the different categories of financial intermediary remains stable, whereby the share of reporting volume by the banking sector has risen continually in the last 10 years: in 2012, only 66.2% of reporting volume came from the banking sector.[39]

Diagram 3 shows the number of SARs submitted to MROS by type of bank.[40]

Diagram 3



[39] See *2012 MROS Annual Report*, May 2013, p. 5.

[40] The type of bank corresponds to the Swiss National Bank's classification.

Table 3

For comparison: 2013 to 2022[41]

Branche	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2022 in absolute figures	Average 2013–2022
Bank	79.6%	85.3%	91.3%	86.0%	91.0%	88.8%	89.9%	89.5%	90.0%	91.6%	6,999	88.3%
Other financial intermediary[42]	0.1%	0.2%	0.2%	0.7%	0.4%	2.3%	0.6%	2.3%	2.1%	2.1%	163	1.1%
Payment service provider	5.2%	6.1%	2.4%	4.4%	3.1%	4.4%	4.0%	3.5%	2.5%	2.0%	150	3.8%
Credit card company	1.0%	0.5%	0.5%	0.7%	0.3%	1.2%	1.3%	1.6%	1.7%	1.6%	125	1.0%
Casino	0.6%	0.5%	0.1%	0.5%	0.6%	0.5%	0.7%	0.5%	0.5%	0.7%	52	0.5%
Asset manager	5.2%	2.3%	1.9%	2.2%	1.9%	1.0%	0.9%	0.8%	1.0%	0.6%	45	1.8%
Commodity and precious metal trader	0.7%	0.2%	0.3%	0.1%	0.2%		0.3%	0.2%	0.5%	0.3%	24	0.3%
Loan. leasing and factoring business	0.3%	0.2%	0.3%	0.3%	0.3%	0.3%	0.3%	0.4%	0.3%	0.3%	22	0.3%
Insurance company	1.3%	0.6%	0.5%	3.1%	0.5%	0.6%	0.3%	0.4%	0.3%	0.3%	21	0.8%
Currency exchange								0.1%	0.1%	0.3%	20	0.2%
Fiduciary	4.9%	2.8%	2.0%	1.5%	1.1%	0.7%	0.8%	0.6%	0.5%	0.1%	8	1.5%
Securities trader	0.1%	0.6%	0.1%	0.1%	0.3%	0.1%	0.3%	0.0%	0.2%	0.1%	8	0.2%
Attorney	0.6%	0.6%	0.3%	0.2%	0.1%	0.1%	0.1%	0.1%	0.1%	0.0%	2	0.2%
Foreign exchange trader	0.4%			0.1%			0.3%	0.0%			0	0.2%
SRO		0.1%					0.1%	0.0%			0	0.1%
Supervisory authority (FINMA/ESBK/GESPA)		0.1%							0.1%		0	0.1%
Distributor of investment funds					0.1%						0	0.1%
Trustees								0.1%	0.1%		0	0.1%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**7,639**	**100%**

[41] The absolute figures for 2013–21 are published in the respective *MROS annual reports*.

[42] The category 'Other financial intermediary' includes, in particular, financial intermediaries with a FinTech licence from FINMA as well as Virtual Asset Service Providers (VASP). VASPs are crypto exchanges, wallet providers and other financial service providers related to the issuance, offer and sale of virtual assets and other business models.

Table 4

For comparison: 2013 to 2022[43]

Type of bank	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2022 in absolute figures	Average 2013–2022
Major bank	28.9%	31.7%	35.3%	31.1%	26.3%	26.7%	28.2%	34.1%	29.5%	28.1%	1,968	30.0%
Cantonal bank	6.4%	5.0%	5.8%	7.6%	5.2%	5.5%	5.3%	14.0%	14.5%	18.6%	1,300	8.8%
Stock exchange bank	10.2%	10.6%	14.0%	12.4%	12.7%	20.8%	25.1%	10.7%	16.8%	16.4%	1,146	15.0%
Other type of bank	20.5%	14.3%	9.9%	12.9%	9.6%	9.5%	8.6%	16.3%	17.1%	14.3%	999	13.3%
Raiffeisen bank	7.0%	9.0%	5.8%	6.2%	3.9%	3.2%	3.1%	7.2%	7.3%	8.8%	616	6.2%
Foreign-controlled bank	21.4%	25.6%	26.6%	26.3%	39.8%	31.0%	26.9%	12.5%	8.3%	7.9%	552	22.6%
Regional and savings bank	0.5%	0.9%	0.5%	1.2%	0.6%	1.1%	1.3%	3.5%	5.8%	5.2%	365	2.1%
Branch of foreign bank	0.4%	0.2%	0.3%	0.1%	0.1%	0.3%	0.2%	1.6%	0.7%	0.5%	37	0.4%
Private bank	4.6%	2.6%	1.8%	2.3%	1.7%	1.9%	1.3%	0.2%	0.1%	0.2%	16	1.7%
Bank with special business clientele	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0	0.0%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**6,999**	**100.0%**

4.4 The legal basis of SARs

Of the 7,639 SARs received in 2022, 4,794 (62.8%) were submitted under Art. 9 para. 1 let. a AMLA[44] (duty to report) and 2,497 (32.7%) under Art. 305ter para. 2 SCC[45] (right to report). A further 348 SARs (4.6%) were submitted under Art. 9 para. 1 let. b AMLA.[46]

With the exception of 2021, SARs submitted under Art. 9 para. 1 let. a AMLA have increased steadily since 2016. As the vast majority of SARs received by MROS are submitted by banks, the trend is mainly an indicator of the behaviour of this sector. Nevertheless, there is a considerable difference between Swiss banks in terms of the number of SARs they submit under Art. 9 para. 1 let. a AMLA or Art. 305ter para. 2 SCC. This is illustrated in the table below.

43 The absolute figures for 2013–21 are published in the respective *MROS annual reports*.

44 Art. 9 para. 1 let. a AMLA: A financial intermediary must report immediately to MROS pursuant to Article 23 if it knows or has reasonable grounds to suspect that the assets involved in the business relationship are: 1) connected to a criminal offence (Art. 260ter or Art. 305bis SCC); 2) derived from a crime or from an aggravated tax offence (Art. 305bis no 1bis SCC); 3) subject to the power of disposal of a criminal or terrorist organisation, or; 4) being used to finance terrorism (Art. 260^{quinquies} para. 1 SCC).

45 Art. 305ter para. 2 SCC: The persons covered by paragraph 1 have a right to report to MROS any observations that suggest that assets originate from a criminal offence or an aggravated tax offence pursuant to Art. 305bis No 1bis SCC.

46 Art. 9 para. 1 let. b AMLA: A financial intermediary must report immediately to MROS if it breaks off negotiations to enter into a business relationship because of a well-founded suspicion under Art. 9 para. 1 let. a AMLA.

Diagram 4

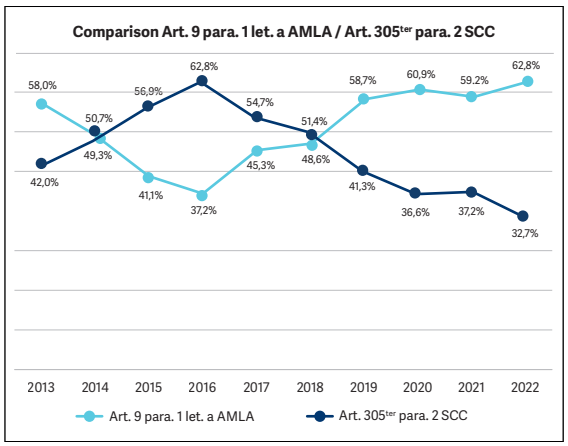


Diagram 5

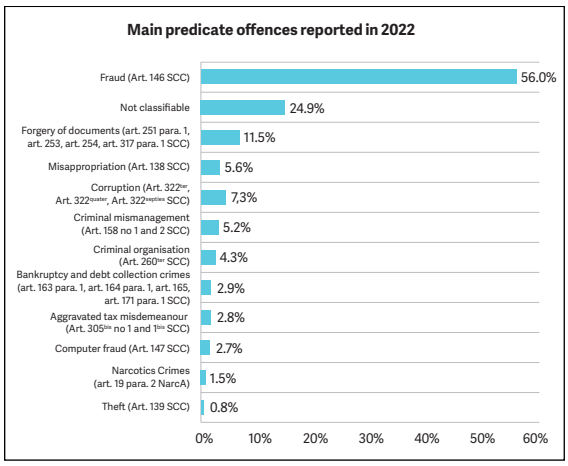


Table 5

Type of bank	Art. 9 para. 1 let. a AMLA	in %	Art. 305ter para. 2 SCC	in %	Other	in %	Total
Major bank	746	37.9 %	1,199	60.9 %	23	1.2 %	1,968
Other type of bank	791	79.2 %	188	18.8 %	20	2.0 %	999
Cantonal bank	1,041	80.1 %	238	18.3 %	21	1.6 %	1,300
Foreign-conrolled bank	311	56.3 %	212	38.4 %	29	5.3 %	552
Stock exchange bank	706	61.6 %	237	20.7 %	203	17.7 %	1,146
Raiffeisen bank	582	94.5 %	25	4.1 %	9	1.5 %	616
Regional and savings bank	220	60.3 %	140	38.4 %	5	1.4 %	365
Branch of foreign bank	6	16.2 %	30	81.1 %	1	2.7 %	37
Private bank	6	37.5 %	9	56.3 %	1	6.3 %	16
Total	**4,409**	**63.0 %**	**2,278**	**32.5 %**	**312**	**4.5 %**	**6,999**

4.5 Predicate offences

The chart below shows the predicate offences that were suspected in the SARs submitted in 2022.[47]

– The above chart shows little variation from 2021. The three most frequently suspected predicate offences (including 'not classifiable') remain the same, although there are slight differences over 2021 in absolute figures. The seven most frequently mentioned predicate offences also remain the same: although they appear in a slightly different order, their absolute figures have not changed substantially.
– Fraud is the most frequently suspected predicate offence by far; its proportion in 2022 (56%) remains similarly high as in 2021 (55%).
– One must be careful not to draw too precise conclusions about the nature of predicate offences in Switzerland from the chart since it only reflects the predicate offences suspected at the time the financial intermediary submitted the SAR. The data presented here does not take into account the value of assets or the number of business relationships or accounts.

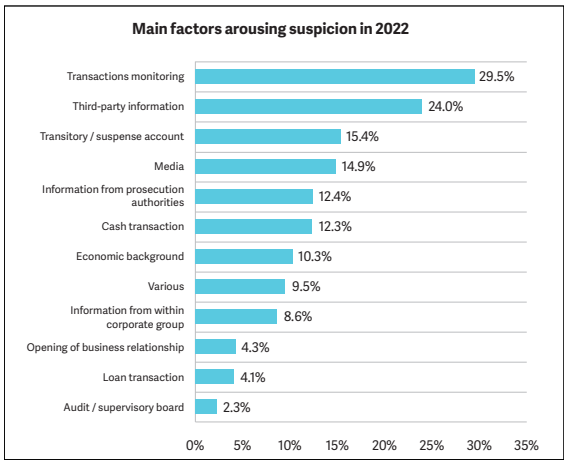
[47] Since 2020, the reporting financial intermediary may indicate several possible predicate offences in each SAR. Consequently, although it is possible to determine the relative frequency of individual suspected predicate offences across all SARs, a comparison with the years prior to 2020 is not meaningful.

The analysis carried out by MROS may also trigger suspicion of another predicate offence. A more detailed analysis of predicate offences was carried out by the Interdepartmental Coordinating Group on Combating Money Laundering and the Financing of Terrorism (CGMT) in 2021.[48]

4.6 Factors arousing suspicion

The chart below shows what factors aroused financial intermediaries' suspicions, prompting them to submit a SAR in 2022.[49]

Diagram 6

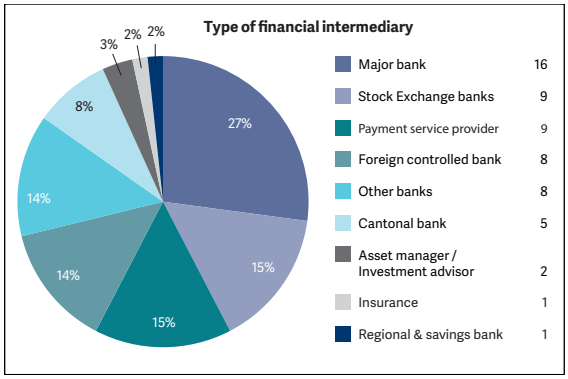


– Once again, transaction monitoring was the category that aroused the most suspicion, in 29.5% of all cases (2021: 32.7%, 2020: 32.6%).

4.7 Terrorism financing

In 2022, 59 SARs were sent to MROS reporting suspicions of terrorism financing and/or the violation of the Federal Act on the Proscription of Al-Qaeda, Islamic State and Associated Organisations.[50] This represents 0.8% of the total number of SARs received. These 59 SARs are also linked to other predicate offences, such as membership in a criminal organisation (18 cases), bribery[51] (6 cases) or fraud (6 cases). Several cases also mention further predicate offences.
The three most frequent sources arousing financial intermediaries' suspicion were media reports (24 cases), transaction monitoring (18 cases) and third-party information (14 cases). Several cases also mention other sources triggering suspicion.
Most of the terrorism-related SARs (47) were submitted by banks, followed by payment service providers (9), asset managers (2) and insurance companies (1).

Diagram 7



Of the 59 terrorism-related SARs in 2022, MROS notified the relevant prosecution authority in five cases.

48 CGMT, *Second national report on the evaluation of the risks of money laundering and terrorist financing in Switzerland*, 29.10.2021, p.17–28.

49 Compared to the years before 2020, financial intermediaries can now indicate several suspicion-triggering elements for their reports in the goAML information system. It is therefore no longer possible to make a meaningful comparison with the figures for the years before 2020.

50 Federal Act on the Proscription of Al-Qaeda, Islamic State and Associated Organisations (SR 122), repealed with effect from 1 December 2022.

51 Art. 322ter, Art. 322^{quater} or Art. 322^{septies} SCC

4.8 Organised crime

In 2022, MROS received 328 SARs indicating suspected links to a criminal or terrorist organisation. This represents 4.3% of total reporting volume. The majority of these SARs (87.8%) were submitted by the banking sector.

Diagram 8

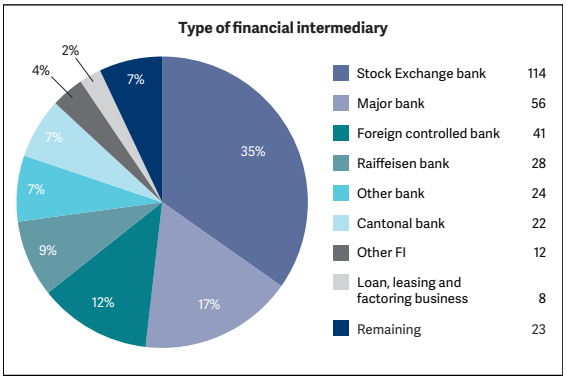


Table 6

Other predicate offences most frequently mentioned in SARs relating to suspicion of membership in a criminal organisation	Number of mentions	in %
Fraud (Art. 146 SCC)	103	31%
Document forgery (Art. 251 no 1, Art. 253, Art. 254, Art. 317 no 1 SCC)	38	12%
Bribery (Art. 322ter, Art. 322^{quater}, Art. 322^{septies} SCC)	30	9%
Narcotics offence (Art. 19 para. 2)	22	7%
Extortion (Art. 156 SCC)	21	6%
Financing of terrorism (Art. 260^{quinquies} SCC)	17	5%
Aggravated tax misdemeanour (Art. 305bis no 1 and 1bis SCC)	16	5%
Criminal mismanagement (Art. 158 no 1 and 2 SCC)	10	3%
Misappropriation (Art. 138 SCC)	10	3%

Table 7

Main factors arousing suspicion of links to a criminal or terrorist organisation	Number of mentions	in %
Media reports	113	34%
Third-party information	79	24%
Transaction monitoring	74	23%
Information from prosecution authorities	53	16%
Opening of business relationship	34	10%
Various	26	8%
Unclear economic background	21	6%
Transitory account	17	5%
Lending business	17	5%

The 328 SARs indicating suspected links to a criminal or terrorist organisation resulted in 43 notifications to the relevant prosecution authorities.

4.9 Requests for information under Art. 11*a* AMLA

The number of requests to financial intermediaries under Art. 11*a* para. 1 AMLA[52] slightly decreased in 2022 compared to the previous year (17%). In contrast, the number of requests under Art. 11*a* para. 2[53] and 2bis AMLA[54] to third-party financial intermediaries who did not submit a SAR rose (+38%). The increase is largely due to the introduction of Art. 11*a* para. 2bis AMLA in 2021. It is also a result of implementing the MROS strategy adopted in 2020, which provides for the optimal support of the prosecution authorities and

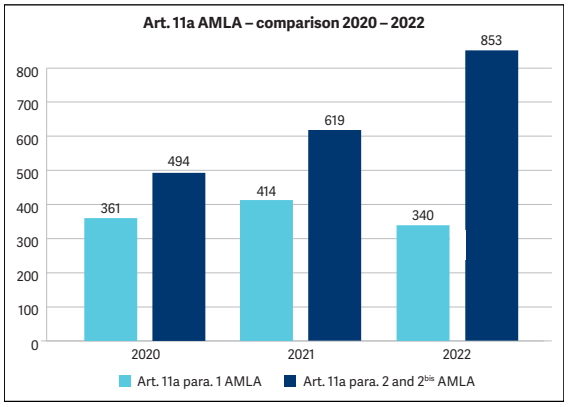
[52] Art. 11*a* para. 1 AMLA: If MROS requires additional information to analyse a SAR it receives under Art. 9 AMLA or Art. 305ter para. 2 SCC, the financial intermediary submitting the SAR must provide MROS with all the relevant information in its possession.

[53] Art. 11*a* para. 2 AMLA: If it becomes apparent from the analysis of a SAR that other financial intermediaries – besides the reporting financial intermediary – are or were involved in a reported transaction or business relationship (third-party financial intermediaries), they must provide MROS with the relevant information on request if it is in their possession.

[54] Art. 11*a* para. 2bis AMLA: If it becomes apparent from information received from a foreign FIU that a financial intermediary subject to AMLA is or was involved in a transaction or business relationship connected with this information, the financial intermediary involved must, upon request, disclose to MROS all related information in its possession.

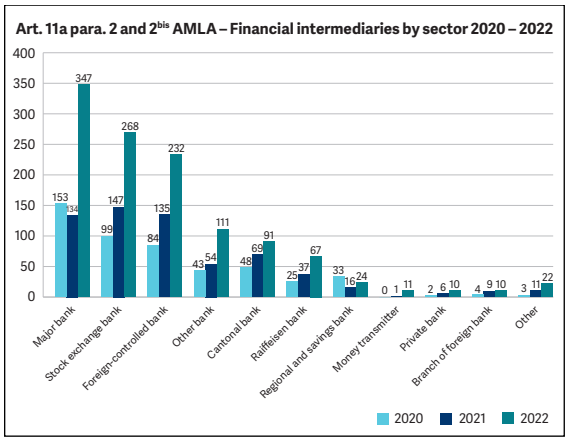
requires the in-depth analysis of certain SARs.[55] Consequently, MROS is now also increasingly obtaining information from financial intermediaries not directly involved in the reporting process, i.e. third-party intermediaries.

Diagram 9



A breakdown of information requests under Art. 11*a* para. 2 and 2[bis] AMLA to financial intermediaries by type of bank shows that the number has increased for all categories. The majority of requests were made to major banks, stock exchange banks and foreign-controlled banks.

Diagram 10



4.10 Notifications to the prosecution authorities

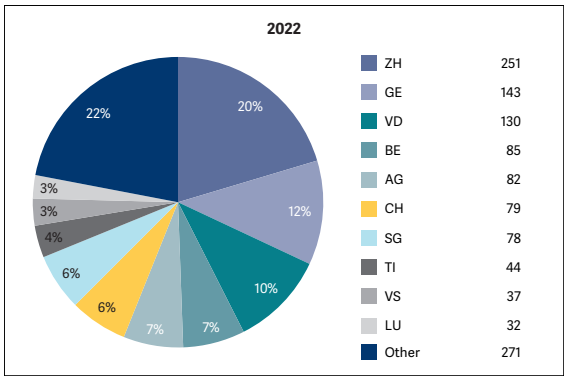
In 2022, MROS submitted 1,232 notifications to the prosecution authorities based on Art. 23 para. 4 AMLA. This is 17% fewer than in 2021 (1,486). The 1,232 notifications contained information from:

- 1,205 SARs received in 2022
- 459 SARs received in 2021
- 14 SARs received in 2020
- 26 business relationships reported in 2019
- 8 business relationships reported in 2018
- 2 business relationships reported in 2017
- 1 business relationship reported in 2016

Diagram 11 shows the prosecution authorities that MROS sent the 1,232 notifications to in 2022.

[55] See Money Laundering Reporting Office Switzerland (MROS), *Annual Report 2020*, Chapter 2.

Diagram 11



– As in 2021, the cantons of Zurich, Geneva and Vaud received the most notifications. The Office of the Attorney General of Switzerland (mentioned as 'CH' in the Diagram) fell from fourth place in the years 2020 and 2021 to sixth place in 2022, after the cantons of Bern and Aargau. The size of the financial sector in the various cantons has a significant influence on this distribution.
– In most cases, the notifications MROS sends to the OAG concern money laundering associated with predicate offences committed abroad. They therefore present a higher degree of complexity and the information they contain is more frequently drawn from different SARs. In contrast, notifications to the cantonal prosecution authorities tend to relate only to a single SAR.
– A comparison with the years prior to 2020 is not relevant: until then, each notification corresponded to one SAR concerning one business relationship. With the introduction of goAML, notifications may now involve several SARs concerning multiple business relationships. The information transmitted in these notifications may also have been drawn from sources other than SARs.

Table 8

For comparison: 2013 to 2022

Authority	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2022 in absolute figures	Average 2013–2022
ZH	18.4%	12.4%	13.5%	12.0%	10.2%	12.8%	14.3%	18.9%	21.1%	20.4%	251	15.4%
VD	2.4%	2.5%	2.6%	3.1%	1.8%	4.3%	5.5%	11.1%	11.6%	10.6%	130	5.5%
GE	15.0%	12.7%	8.4%	14.9%	12.8%	14.1%	15.0%	11.5%	11.3%	11.6%	143	12.7%
CH	34.2%	44.7%	53.4%	38.1%	52.6%	48.4%	39.9%	9.0%	9.1%	6.4%	79	33.6%
BE	1.6%	4.6%	1.8%	3.0%	1.6%	1.8%	3.3%	7.5%	6.7%	6.9%	85	3.9%
AG	1.3%	1.8%	1.5%	2.6%	1.2%	1.6%	1.5%	5.3%	5.2%	6.7%	82	2.9%
TI	12.5%	7.3%	6.5%	6.0%	6.0%	3.3%	3.3%	5.0%	4.8%	3.6%	44	5.8%
SG	1.7%	3.0%	2.0%	2.2%	2.4%	1.3%	1.2%	3.5%	4.0%	6.3%	78	2.8%
FR	0.5%	0.2%	0.6%	0.6%	1.4%	1.6%	1.5%	2.7%	3.1%	2.1%	26	1.4%
LU	1.5%	1.8%	1.0%	1.4%	1.4%	0.8%	1.8%	3.5%	2.9%	2.6%	32	1.9%
ZG	1.2%	1.3%	1.5%	1.2%	0.6%	1.9%	1.9%	2.5%	2.6%	2.2%	27	1.7%
VS	1.1%	1.0%	0.5%	1.0%	1.2%	1.4%	0.8%	2.7%	2.4%	3.0%	37	1.5%
BS	2.2%	1.2%	1.3%	3.3%	2.0%	0.9%	0.9%	2.6%	2.3%	2.3%	28	1.9%
TG	0.7%	1.1%	0.8%	1.5%	0.7%	0.8%	1.3%	3.0%	2.1%	2.6%	32	1.5%
SO	1.1%	0.7%	0.4%	4.2%	0.4%	1.1%	1.2%	1.9%	2.0%	2.1%	26	1.5%
NE	0.7%	0.9%	1.1%	0.9%	1.0%	1.2%	1.4%	2.3%	1.9%	1.7%	21	1.3%
BL	0.8%	0.5%	1.5%	1.5%	1.2%	0.8%	2.9%	2.1%	1.7%	2.3%	28	1.5%
SZ	0.6%	0.2%	0.5%	0.8%	0.5%	0.3%	0.4%	1.0%	1.1%	1.9%	23	0.7%
GR	0.9%	1.0%	0.6%	0.3%	0.5%	0.3%	0.4%	1.5%	1.0%	1.1%	13	0.8%

Author-ity	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2022 in absolute figures	Average 2013–2022
JU	0.2%	0.6%	0.0%	0.3%	0.1%	0.1%	0.1%	0.3%	1.0%	0.2%	3	0.3%
AR	0.2%	0.2%	0.1%	0.3%	0.2%	0.2%	0.3%	0.6%	0.8%	1.3%	16	0.4%
SH	0.6%	0.3%	0.1%	0.5%	0.3%	0.1%	0.3%	0.5%	0.5%	0.6%	7	0.4%
NW	0.4%	0.1%	0.1%	0.0%	0.0%	0.7%	0.2%	0.3%	0.4%	0.6%	8	0.3%
GL	0.1%	0.0%	0.0%	0.1%	0.1%	0.2%	0.0%	0.2%	0.1%	0.4%	5	0.1%
OW	0.0%	0.0%	0.1%	0.0%	0.0%	0.0%	0.3%	0.2%	0.1%	0.2%	2	0.1%
UR	0.0%	0.1%	0.0%	0.2%	0.0%	0.0%	0.0%	0.3%	0.1%	0.2%	3	0.1%
AI	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.1%	0.2%	3	0.0%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**1,232**	**100.0%**

Legend

AG	Aargau	**NW**	Nidwalden
AI	Appenzel Inner Rhodes	**OW**	Obwalden
AR	Appenzel Outer Rhodes	**SG**	St. Gallen
BE	Bern	**SH**	Schaffhausen
BL	Basel-Landschaft	**SO**	Solothurn
BS	Basel-Stadt	**SZ**	Schwyz
CH OAG	Office of the Attorney General of Switzerland	**TG**	Thurgau
FR	Fribourg	**TI**	Ticino
GE	Geneva	**UR**	Uri
GL	Glarus	**VD**	Vaud
GR	Graubunden	**VS**	Valais
JU	Jura	**ZG**	Zug
LU	Lucerne	**ZH**	Zurich
NE	Neuchatel		

4.11 Sharing information with foreign FIUs

MROS and its foreign counterparts, i.e. other FIUs, may share information through international administrative assistance channels for the purpose of investigating suspected cases of terrorism financing, money laundering and its related predicate offences, and organised crime. When MROS receives SARs involving foreign natural persons or legal entities, it is authorised to request information from its counterparts in the countries concerned. The information MROS obtains is important for its analyses, as most of the SARs it receives have an international dimension. In 2022, MROS sent 262 information requests to 66 foreign FIUs.

In turn, it received 851 requests from 89 countries. This is an increase of 8% over the previous year (2021: 784 requests from 87 countries). The expanded powers of MROS introduced in 2021 for requesting information from financial intermediaries based on information from a foreign FIU (Art. 11*a* para. 2bis AMLA) are the main reason for this increase in requests.

Of the 851 requests for information it received in 2022, MROS processed 521 (61.2%). It also responded to 149 requests it had received in 2021. Hence, in 2022 MROS processed 670 requests for information. Although it is not apparent from the figures presented here, the substance of these responses is now more often supplemented with relevant financial information due to MROS's greater powers. This means that processing information requests is now more complex and time-consuming than it was prior to 2021.

Spontaneous information reports contain information from a foreign FIU to MROS about a case with a link to Switzerland that was not preceded by a request, or information from MROS to a foreign counterpart about a case with a link to that country. In 2022, MROS received 709 spontaneous information reports from 50 countries (2021: 527 reports from 42 countries). In turn, it sent 178 spontaneous reports to 56 foreign FIUs (2021: 399 reports to 69 FIUs).

4.12 Sharing information with national authorities

MROS shares information not only with its foreign counterparts, but also with other Swiss authorities such as supervisory authorities or other authorities active in the fight against money laundering, predicate offences to money laundering, organised crime or terrorist financ-

ing. MROS is authorised to share information with these authorities under Art. 29 AMLA. Since 2020, both the content and volume of information has increased to the point where it has had an impact on workload.
In 2022, MROS received 667 requests from 31 Swiss authorities for information on bank accounts, individuals or companies in the context of investigations into money laundering, organised crime or terrorist financing. In approximately 82% of the cases, these requests came from the cantonal police and the Federal Criminal Police. This is an increase in volume of 19% compared with the previous year (2021: 561 requests).
MROS also received 109 spontaneous information reports from Swiss authorities in 2022.
In turn, MROS forwarded 177 spontaneous information reports to other Swiss authorities or supervisory authorities involved in combating money laundering, its predicate offences, organised crime and terrorism financing.
MROS may also request information from other federal, cantonal or communal authorities; these requests are not listed in the figures above.

5. Typologies

The system for combating money laundering and terrorist financing is complex and multi-layered. MROS plays a pivotal role in this system. By virtue of its function, MROS can make a substantial contribution to providing a holistic view in situations where information is only fragmentarily available. The effectiveness of its work depends crucially on the interactions between all the actors involved, in particular the financial intermediaries, the traders, the supervisory authorities, the law enforcement authorities and the foreign partner FIUs. The aim of this chapter is to illustrate with concrete examples the added value of such an overall picture, which represents more than the sum of the limited individual views of the various actors.

5.1 'On behalf of' requests

5.1.1 Information sharing principles

Based on Art. 30 f. AMLA, MROS can exchange information with its foreign counterparts, the FIUs. This international administrative assistance is based on the principles of the Egmont Group[56]. In principle, the exchange of information between FIUs is a tool that MROS uses when analysing SARs. However, prosecution authorities can also make use of this tool through MROS (e.g. for use in requests for mutual legal assistance). This procedure is called an 'on behalf of' request and is possible even if criminal proceedings have already been opened in Switzerland.

5.1.2 Illustrative case

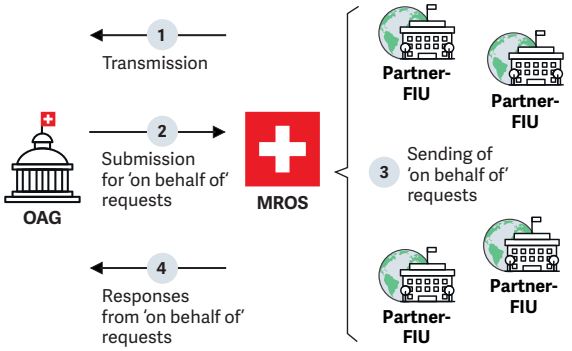
The 'on behalf of' procedure is illustrated below using two specific examples from the year 2022. Both 'on behalf of' requests were made for ongoing criminal proceedings conducted by the OAG. The overall goal was to obtain information that would help the OAG better define any next steps in the respective proceedings.
The first criminal proceedings were based on a transmission by MROS of reported information under Art. 23 para. 4 AMLA to the OAG, although the transmission of reported information is not a mandatory requirement for an 'on behalf of' request. MROS opted in favour of transmitting the reported information because it was presumed to concern an international money laundering case. The analyses showed that various payments were made to and from abroad. In order to be able to assess whether an international request for mutual legal assistance to the countries concerned would be expedient, MROS offered the OAG its 'on behalf of' request service. Subsequently, 'on behalf of' requests were sent to four foreign partner FIUs. MROS returned the responses received to the OAG.
At the same time that these 'on behalf of' inquiries were sent, a Eurojust[57] project on the same corruption case was initiated. Switzerland is a

[56] Principles for information exchange between FIUs, July 2013 (revised in May 2022), available *here*.

[57] *European Union Agency for Criminal Justice Cooperation*, a hub based in The Hague, Netherlands, where national judicial authorities work closely together to fight serious organised cross-border crime.

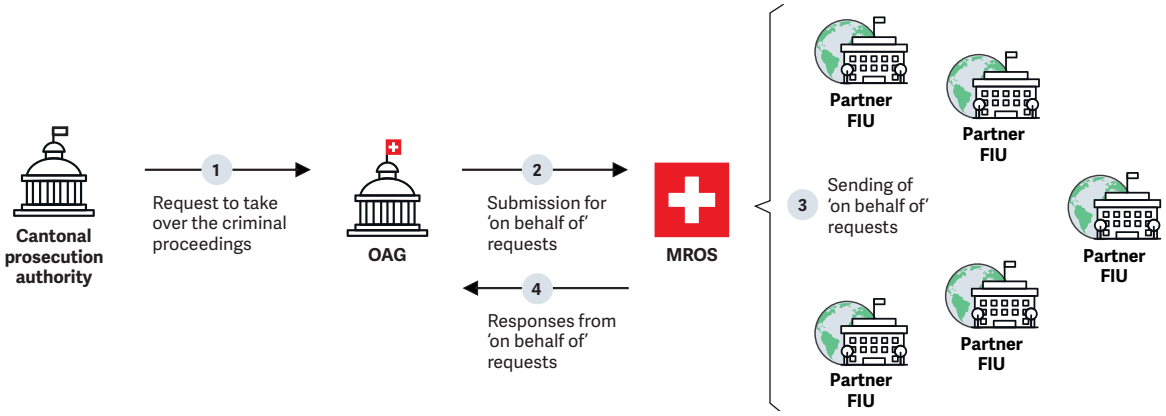
participating member of this project along with other countries, which are not the same countries having been sent 'on behalf of' requests. Based on the responses from the 'on behalf of' requests, it was possible to define which countries could potentially be integrated into the Eurojust project in a second step and where an international request for mutual legal assistance would make sense.

Figure 1: 'On behalf of' request in the context of a corruption case



In the second case, a large number of people residing in Europe (including Switzerland) were allegedly 'cold-called' by fictitious 'brokerage firm representatives' from Southeast Asia in recent years. 'Cold-calls' are proactive calls made by company representatives to private individuals. In this case, the unknown perpetrators were suspected of using various means of deception to persuade those they targeted to transfer money abroad for what the perpetrators alleged were promising investments in Asian companies. The investments were presumably fictitious. Since the victims were located in various cantons and many transactions took place abroad, the OAG decided that this case should be dealt with by the federal prosecution authorities.
In order to be able to assess in which cases an international mutual legal assistance request would be useful, the OAG asked MROS to send five 'on behalf of' requests. Based on the feedback from these requests, the OAG went on to draft international requests for mutual legal assistance.

Figure 2: 'On behalf of' request in the context of a fraud case



5.1.3 Role of MROS

The use of 'on behalf of' requests can help the Swiss prosecution authorities to assess whether an international request for mutual legal assistance is appropriate. Another advantage of these requests is that the response time tends to be shorter than for international mutual legal assistance requests, although MROS cannot influence the response time and quality of its FIU partners. The execution of these 'on behalf of' requests hinges on the fulfilment of legal requirements: Firstly, the requested FIU must be a member of the Egmont Group[58]; secondly, the 'on behalf of' request must not replace or circumvent international mutual legal assistance in criminal matters; thirdly, the requesting authority may only use the information for intelligence purposes or for the initiation of criminal proceedings for money laundering and its predicate offences, organised crime or terrorist financing, or to substantiate a request for mutual legal assistance in criminal proceedings[59]; fourthly, the use of information as evidence in administrative or court proceedings is prohibited[60]; and fifthly, MROS is obliged to disclose information obtained through an 'on behalf of' request only in report form (no disclosure of original documents) and under the conditions set by the foreign FIU.[61]

5.2 Overview of national money laundering proceedings

5.2.1 Information sharing principles

As the central authority in the Swiss system for combating money laundering and terrorist financing, and through its close contacts with the cantonal public prosecutors' offices and the OAG, MROS often has a good overview of ongoing proceedings. MROS's coordinating role repeatedly benefits the authorities.

5.2.2 Illustrative case

In the early 2010s, company A, active in the oil sector and owned by a Central Asian businessman, paid several tens of millions of US dollars into a Swiss account in the name of an offshore company, B, ultimately owned by a former senior official of the Central Asian country in question. The accounts held in the name of company A were brought to the attention of MROS in December 2019 following a SAR from a financial intermediary.
MROS forwarded the case to the OAG, which opened an investigation against unknown persons for bribery of foreign public officials.
Since February 2022, in coordination with the OAG, MROS has been exchanging information with its counterpart in the Central Asian country in question (see points 1 and 4 in Figure 3). The latter has also recently been analysing the above-mentioned case, and criminal proceedings were reportedly underway in said Central Asian country.
As a result of a request by the foreign country in question, MROS was able to collect information on a Swiss account that was not previously reported to MROS. MROS made use of Art. 11*a* para. 2[bis] AMLA, which it has been authorised to do since 1 July 2021 (points 1 and 2 of Figure 3). The information could be passed on to the OAG (point 3 of Figure 3).

---

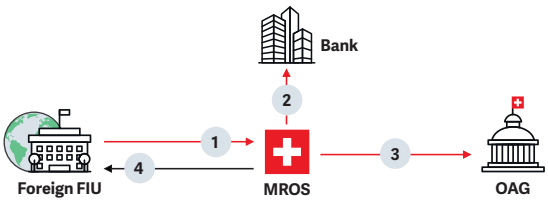
58 *Members by Region – Egmont Group.*

59 'intelligence use only', Art. 30 para. 1 let. a and Art. 30 para. 4 let. a No 1 and 2 AMLA.

60 Art. 30 para. 4 let. c AMLA and Art. 25 para. 2 MROSO

61 Art. 30 para. 3 AMLA

Figure 3: Exchange of information in the context of national procedure

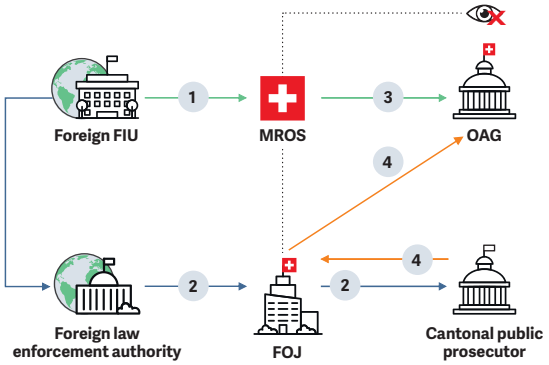


MROS supported the criminal proceedings conducted by the OAG by submitting an 'on behalf of' request to its counterpart in the course of 2022. The purpose of the MROS request was to clarify the status of possible pending criminal proceedings abroad and to encourage the foreign authorities to request international mutual legal assistance in criminal matters from Switzerland (points 1 and 2 of Figure 4).

Figure 4: 'On behalf of' request in the context of a national procedure

MROS received a reply from its counterpart (point 1 of Figure 5) indicating that an international request for mutual legal assistance had been sent by the authorities of the foreign country in question to the Federal Office of Justice (FOJ). The latter had already delegated the execution of the said request for mutual legal assistance to a cantonal public prosecutor's office without knowledge of the criminal investigation initiated by the OAG, since it had been opened against unknown persons (point 2 of Figure 5). As MROS had an overview of the ongoing proceedings, it was able to inform the OAG of the FOJ's decision as soon as it received the answer from the foreign FIU (point 3 of Figure 5). The OAG subsequently asked that the request for mutual legal assistance be delegated to the OAG itself before the cantonal public prosecutor's office had taken any measures (point 4 of Figure 5), thus making use of the knowledge it had already acquired in this case.

Figure 5: Role of the MROS in the context of the exchange of information



The second example also illustrates this role of MROS.
In 2019, MROS received a series of SARs from various financial intermediaries concerning the same facts. The financial intermediaries suspected that the proceeds of acts amounting to breach of trust and embezzlement had been laundered through Swiss accounts. The predicate offence had apparently taken place in a Far Eastern country.
MROS transmitted the case to the cantonal prosecutor's office already in charge of executing a request for mutual legal assistance from the Far Eastern country in question. Two years later, when the request had been executed and the offence was already being prosecuted by the authorities of the relevant foreign country, the cantonal prosecutor's office issued a no-proceedings order.
Almost three years later, the potentially injured company filed a complaint with the OAG. The OAG was not aware of the reports from Swiss financial intermediaries, let alone of the cases referred to the cantonal prosecutor's office in charge of executing the request for mutual legal assistance at the time.
The OAG made use of the mutual assistance in administrative matters provided for in Art. 29 ff. AMLA to ask MROS if it had any information concerning this case. MROS was quickly able to put the OAG in touch with the cantonal prosecutor's office.

5.2.3 Role of MROS

These examples show that MROS has a comprehensive view of the various money laundering proceedings and predicate offences, including those against unknown persons. Cooperation with MROS may therefore be appropriate before delegating the execution of a request for mutual legal assistance in criminal matters. These examples also illustrate that MROS has an overall view of the various cantonal and federal proceedings. This makes it possible for MROS to streamline cooperation between the prosecution authorities and, if necessary, allow one prosecution authority to benefit from the information gathered by the other.

5.3 Facilitating cooperation between national and foreign authorities

5.3.1 Information sharing principles

This typology shows the interaction between MROS and foreign FIUs, national authorities and financial intermediaries. In addition to requests for mutual assistance in administrative matters from a foreign FIU under Art. 30 ff. AMLA, this case study also addresses cooperation with national authorities (spontaneous and upon request) in accordance with Art. 29 para. 2bis AMLA as well as the release of information in accordance with Art. 11*a* AMLA. In this case study, the effective use of the instruments available under the law and the associated exchange of information provided an overall view of the case and created concrete added value in the fight against money laundering, its predicate offences, and terrorist financing.

5.3.2 Illustrative case

MROS received an urgent request from a foreign FIU (point 1 of Figure 6), stating that the police in its country were investigating a possible large-scale investment scam. According to the description of the facts provided by the foreign FIU, unknown persons working for a company had contacted a couple domiciled in the FIU's country and convinced them to invest in bitcoins. The couple, who were probably victims of a scam, allegedly invested more than CHF 2 million by transferring funds to accounts in various European countries, including Switzerland. In its request, the foreign FIU provided MROS with four Swiss accounts to which the assets had been transferred, as well as data on some suspicious transactions. The foreign FIU wanted to obtain the identity of the control holder or beneficial owner of these Swiss accounts, as well as the current balance.

MROS's research revealed that three of the four accounts mentioned in the request had already been the subject of SARs received from Swiss financial intermediaries, who suspected that the assets that had transited via the accounts in question were part of a scam. The reports were based on information that the financial intermediaries had received from potential victims. MROS was soon able to establish that this information all related to the same case and had been forwarded to the same cantonal public prosecutor's office, which had opened criminal proceedings on suspicion of money laundering (serious case). Regarding the fourth account, MROS found that it had not been reported by a financial intermediary. However, the account was registered in its database following a recent request from the cantonal police of another canton, which was made while an investigation into fraud was underway (point 2 of Figure 6).

The prosecutor in charge of the criminal proceedings in Switzerland confirmed to MROS that he was unaware of the fourth account mentioned by the foreign FIU and that he was interested in obtaining further information on other potential funds involved in this large-scale case. On the basis of Art. 11*a* para. 2bis AMLA, MROS was able to contact the Swiss financial intermediary in question and request information on the fourth account referred to by the foreign FIU (see points 3 and 4 of Figure 6), even though there had been no SAR.

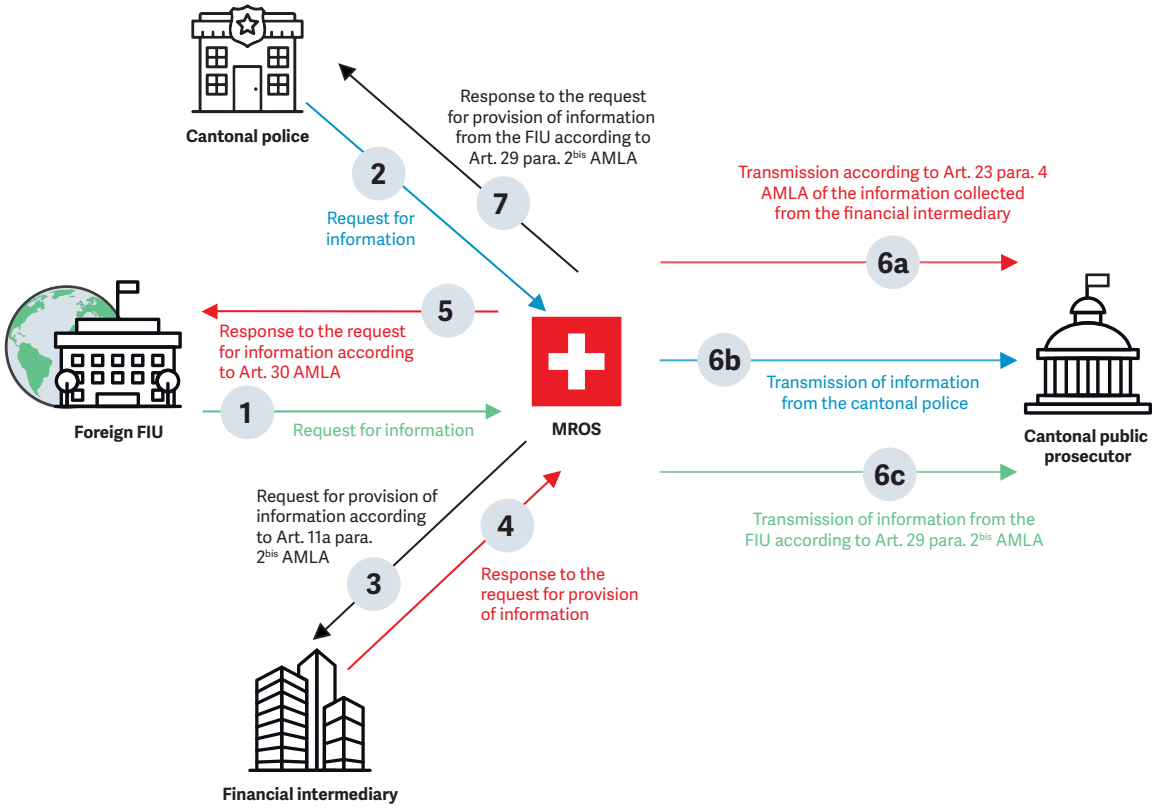
This information was delivered to the foreign FIU (point 5 of Figure 6). The ultimate aim of this exchange was to facilitate international requests for mutual legal assistance in criminal matters. With the information provided by MROS, the prosecution authorities of the country in ques-

tion were able to quickly execute a precise and detailed request for mutual legal assistance in the knowledge that the assets were still in the accounts.
In addition, MROS informed the cantonal public prosecutor's office of the existence of a criminal investigation abroad on the basis of Art. 29 para. 2bis AMLA and provided the name of the foreign authority conducting the investigation abroad and the number of the criminal file. Furthermore, the information collected through the request for information under Art. 11*a* para. 2bis AMLA was also forwarded to the cantonal public prosecutor's office on the basis of Art. 23 para. 4 AMLA. In its report, MROS pointed out that the account in question was also the subject of a criminal complaint filed with the police in another canton. The cantonal prosecution authority thus received new information relevant to the ongoing proceedings (see point 6 of Figure 6). MROS also responded to the cantonal police's request for information (point 7 of Figure 6).

5.3.3 Role of MROS

This case demonstrates the coordinating role that MROS plays between national and foreign authorities and the added value for its analyses of combining the various instruments available in addition to SARs, such as requests under Art. 11*a* AMLA and national and international administrative mutual assistance. This information, which MROS forwards to the national prosecution authorities spontaneously, facilitates the exchange of information and cooperation with foreign authorities and, if necessary, the freezing and confiscation of any assets still available.

Figure 6: The steps prior to a possible letter rogatory that can make it more precise and detailed



5.4 Information sharing and cryptocurrencies

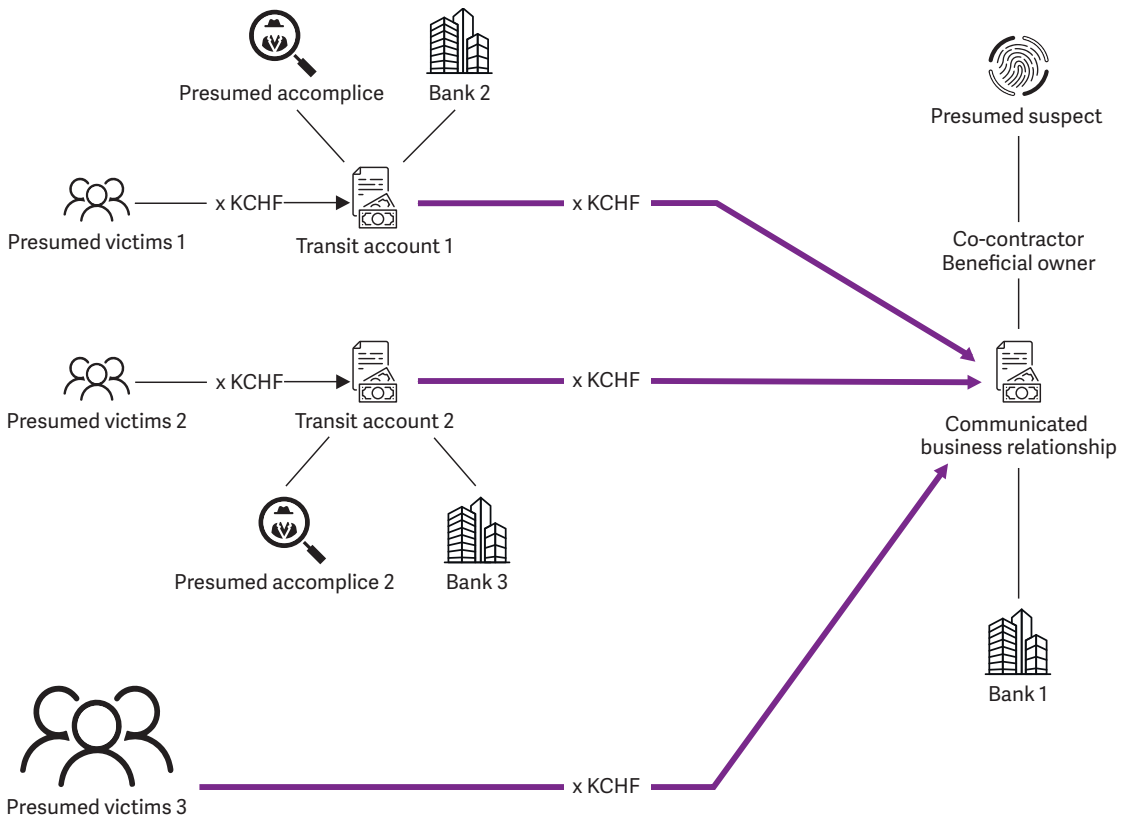
5.4.1 Information sharing principles

Due to their complexity and decentralised or cross-border nature, SARs involving virtual assets or cryptocurrencies can often only be analysed effectively by using different instruments (exchanges with Swiss authorities and between FIUs, requests for information to financial intermediaries under Art. 11*a* AMLA, analyses of virtual assets). The following example illustrates how, by combining these different instruments, MROS can build up a broader picture of suspicious activities.

5.4.2 Illustrative case

In this example, the financial intermediary suspected that funds credited to a business relationship might be the proceeds of an investment scam based on the sale of virtual assets.
Over a short period of time, several hundred thousands of Swiss francs (fiat money) were credited to a business relationship from various private accounts in individual amounts of up to several tens of thousands of Swiss francs. The results of the financial intermediary's clarifications under Art. 6 AMLA suggested that these were proceeds from the sale of virtual assets and that other persons could also be involved in this activity. It was then found that the bulk of the assets were transferred to various bank accounts in Switzerland and abroad, as well as, in particular, to bank accounts held by cryptocurrency platforms abroad (Virtual Asset Service Providers, VASPs).
In its analyses, MROS examined the origin of the funds and requested information from other banks in Switzerland on the basis of Art. 11*a* AMLA. The information obtained revealed, among other things, the existence of possible transit accounts where the funds of the alleged victims could have been consolidated before being transferred to a reported business relationship (see Figure 7).

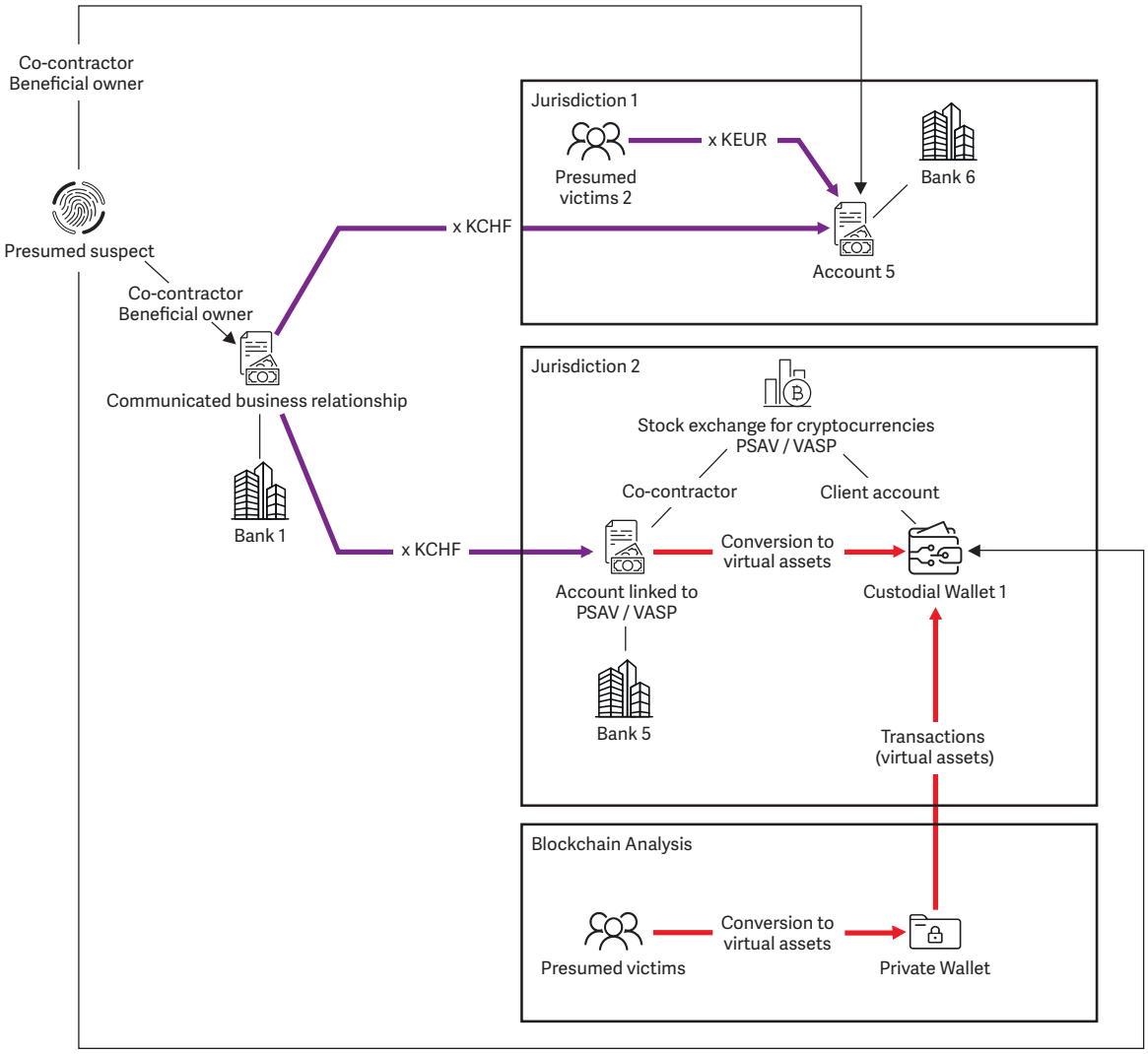
Figure 7: Generic transaction scheme



In order to trace funds of potentially criminal origin transferred abroad, MROS made various requests to partner FIUs. These requests concerned both virtual asset accounts and fiat accounts (in Swiss francs or other currencies).

After several exchanges of information, MROS was able to locate and highlight new funds of potentially criminal origin. The exchanges also provided valuable information on the persons themselves (see Figure 8).

Figure 8: Chain of transactions in fiat and in virtual assets



purple = fiat transactions
red = virtual asset transactions

5.4.3 Role of MROS

Given the typical nature of the activities observed from a transactional point of view and the results from analysing open sources, MROS requested administrative assistance from another Swiss authority under Art. 29 para. 1 AMLA concerning the alleged suspects.
MROS also approached the case from the perspective of virtual assets, relying in particular on distributed ledger technology (blockchain, open sources). The information gathered made it possible to track a series of transactions originating from private or unhosted wallets of interest where the bulk of the funds were ultimately consolidated in favour of deposit addresses held by a VASP in a foreign jurisdiction. A request for information to a partner FIU led to the identification of the holder of the business relationships concerned (see Figure 8.). In general, the infor-

mation available through the distributed ledger technology on a given virtual asset also allows an assessment on the market liquidity for the virtual asset itself or the overall trading volume of the virtual asset over a period of interest. This data can also be taken into account in the analyses carried out by MROS.
Soliciting the various intelligence channels available to MROS and consolidating the information received made it possible to construct a more comprehensive picture of the suspicious activity.

5.5 MROS and sanctions

5.5.1 Principles and legal bases

As mentioned in subchapter 2.2, the military aggression by Russia against Ukraine and the economic and financial sanctions imposed by Switzerland on Russia have led to SARs being sent to MROS. In some cases, these SARs concern deposits of more than CHF 100,000 from Russia into Swiss accounts where the account holders or beneficial owners are Russian citizens residing in Russia. In other cases, they concern donations made by wealthy Russian citizens to their relatives shortly before the former were placed on the sanctions list. In yet other cases, the facts reported to MROS concern changes in the structure of trusts in order to avoid the blocking of the accounts in which the assets are held. This has provided MROS with an overview of conduct that could amount to serious violations of the Embargo Act (EmbA).
It should be noted that the State Secretariat for Economic Affairs (SECO), not MROS, is responsible for monitoring the implementation of international sanctions.[62] Violations of the Embargo Act only constitute predicate offences to money laundering in 'serious' cases as defined in Art. 9 para. 2 EmbA. MROS has engaged in proactive exchanges with SECO, the OAG and certain cantonal prosecutors' offices to determine whether the facts brought to its attention fall into this category. The difficulty here lies in the absence of case law on the definition of a serious violation within the meaning of Art. 9 para. 2 EmbA.
MROS may send spontaneous information to SECO under Art. 29 para. 2bis AMLA, if it knows or suspects the existence of a predicate offence. According to Art. 32 para. 3 of the Ukraine Ordinance, SECO prosecutes and judges violations of Art. 9 and 10 EmbA. The Federal Act on Administrative Criminal Law (ACLA)63 is applicable. If the criminal provisions of the Embargo Act are applicable, the OAG may initiate a police investigation at the request of the competent administrative unit, in this case SECO, if this is justified by the importance of the offence (Art. 14 para 2 EmbA). If the police investigation is opened by the OAG, it falls under federal jurisdiction. To the knowledge of MROS, this has never happened in connection with a circumvention of the sanctions adopted by the Ukraine Ordinance.

5.5.2 Illustrative case

There are situations in which the possible violation of the Embargo Act, whether serious or not, is accompanied by suspicions of other predicate offences to money laundering, in particular forgery of documents as defined in Art. 251 SCC. This is the case when MROS suspects that a Form A[64] has been backdated to allow the transfer of assets from a person subject to sanctions to a relative who is not. The new Form T[65] can also be provided to financial intermediaries by trust representatives, even if the trust structure has not been changed by an authentic instrument in its jurisdiction of registration. The aim is to amend the list of beneficiaries, removing those of Russian nationality and domiciled in Russia in order to avoid falling under the terms of Art. 28*d* of the Ukraine Ordinance.

---

62 Although MROS is not responsible for monitoring the implementation of international sanctions, as FINMA has pointed out, a notification to SECO does not exempt financial intermediaries from immediately notifying MROS if the requirements of Art. 9 AMLA are met or from exercising their right to report under Art. 305ter para. 2 SCC.; *Aktualisierte Sanktionsmeldung | FINMA. (web page available in German, French and Italian)*

63 Federal Act on Administrative Criminal Law (ACLA; RS 313)

64 See the 2020 Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (*CDB 20*), Art. 28.

65 See the 2020 Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (*CDB 20*), Art. 41.

MROS forwarded a number of such cases to cantonal public prosecutors. In several cases, however, the adoption of sanctions by Switzerland against Russians has given new prominence to suspicions of concealment of the true beneficial owners. In several SARs received by MROS, the reported accounts have been held for a long time by relatives of politically exposed persons (PEPs) or major Russian businessmen. When the latter were placed on the sanctions list, the question arose as to whether the declared holders of the assets were not acting as nominees. In one case, the assets were luxury yachts owned by an individual who is known to be close to a PEP subject to sanctions and who the press accuses of acting on behalf of that person. In another case, a relative of the director of a major commodity extraction company inherited his fortune in a deed of gift that appeared to have been forged. In a third case, a trustee produced a new Form T which stated that, contrary to what had been declared a few years earlier, the settlor of the trust of which they were the trustee was in fact a person on the sanctions list and that the trust assets should be blocked. MROS referred the latter case to the competent prosecution authorities, who opened criminal proceedings for forgery of documents against the trustee, who for years had been providing a false Form T. In other cases where the suspicion of forgery was less well-founded, spontaneous information repots were sent to SECO.

5.5.3 Role of MROS

These examples illustrate that even though SECO, not MROS, is responsible for monitoring the implementation of international sanctions, MROS can send spontaneous information reports to SECO under Art. 29 para. 2bis AMLA if it knows or suspects that there has been a predicate offence to money laundering. This was the case in 2022 in the context of the Ukraine Ordinance, where MROS forwarded such cases to the cantonal public prosecutors' offices and also sent spontaneous information reports to SECO.

6. MROS practice

6.1 Spontaneous transmission of information by the prosecution authorities in connection with an MROS notification

The information provided by MROS to the prosecution authorities in a report may be useful for various purposes. Following a report from MROS under Art. 23 para. 4 AMLA, the public prosecutor decides either to open an investigation (Art. 309 CrimPC[66]) or to issue an order not to proceed (Art. 310 CrimPC). A certain amount of time may elapse between the report and the decision, particularly if the public prosecutor instructs the police to conduct a preliminary investigation (Art. 299 ff. CrimPC).
In addition, over that same period of time, the public prosecutor may have attempted to prepare the ground for international mutual legal assistance in criminal matters by making use of Art. 67*a* of the International Mutual Assistance Act (IMAC).[67] According to case law (see Federal Supreme Court decision 140 IV 123[68]), such a spontaneous provision of information to foreign prosecution authorities is not subject to the condition that it initiates criminal proceedings itself; a well-founded suspicion on the part of MROS, which triggers a report within the meaning of Art. 23 para. 4 AMLA, is sufficient to do so.
To take one example, in the case in question the Zurich public prosecutor's office, having received information from MROS, notified the Colombian authorities about a suspicion and gave them a deadline for sending a request for mutual legal assistance in criminal matters to Switzerland. Once the deadline had passed and before the Colombian authorities' request for mutual legal assistance could be executed, the Zurich public prosecutor's office issued an order not to proceed with the case. When the mutual legal assistance was terminated, the Swiss account holders appealed to the Federal Criminal Court and then to the Federal Supreme Court. According to the appellants, the transmission of information under 67*a* IMAC is subject to the condition that criminal proceedings are launched in Switzerland. According to the Federal Supreme Court, the use of Art. 67*a* IMAC must not lead to an uncontrolled exchange of information, but a reasonable suspicion within the meaning of Art. 309 para. 1 let. a CrimPC is not a prerequisite: a suspicion within the meaning of Art. 23 para. 4 AMLA is sufficient. Insofar as the public prosecutor is legitimately informed by MROS, the spontaneous provision of information to a foreign authority is permissible under Art. 67*a* IMAC.
The activities of Swiss public prosecutors' offices are therefore not limited to decisions to open investigations: they may also mandate the police to conduct investigations or support mutual legal assistance requests. In this respect, it should be noted how important it is for Swiss public prosecutors' offices to provide MROS with copies of these spontaneous transmissions of information within the meaning of Art. 67*a* IMAC.

---

66 Swiss Criminal Procedure Code (CrimPC; SR 312.0).

67 Federal Act on International Mutual Assistance in Criminal Matters (Mutual Assistance Act, IMAC; SR 351.1).

68 *Decision of the Federal Supreme Court 140 IV 123 (document available in German, French and Italian)*.

6.2 Disputed jurisdiction of the prosecution authorities

When there is reason to suspect money laundering, predicate offences to money laundering, participation in or support of a criminal organisation or the financing of terrorism, MROS immediately reports the case to the competent law enforcement authorities (Art. 23 para. 4 AMLA). In doing so, it takes into account Art. 23 and 24 CrimPC, Art. 3 to 8 SCC, the case law of the Swiss courts and the practice of the Swiss public prosecutors' offices with whom it is in close contact. MROS also makes use of information in the databases to which it has access under Art. 35*a* AMLA, in particular criminal records (indicating any ongoing criminal proceedings), and from international mutual legal assistance requests by the OAG or cantonal public prosecutors' offices.
As a long-standing and established practice, MROS has, for practical reasons, based its reports to the prosecution authorities under Art. 23 para. 4 AMLA on the location of the business relationship, since the place where the offence was committed is of primary importance. In addition, information from different SARs concerning the same facts is processed in one report and transmitted to the same public prosecutor's office. This gives the public prosecutor in question a better overview of the factual circumstances of the case, which can serve as a basis for assessing the possible initiation of proceedings. MROS does not take back transmission reports or parts thereof. This procedure could, among other things, lead to practical problems in relation to the freezing of assets under Art. 10 para. 1 AMLA, or to the decision notifications to financial intermediaries under Art. 23 para. 5 and 6 AMLA. Should a prosecution authority consider itself to lack local jurisdiction over a report from MROS, it is referred to the initiation of jurisdiction proceedings with the public prosecutor's office that it considers to be responsible, in application of Art. 39 para. 1 CrimPC.
MROS takes into account the feedback from the Swiss public prosecutors' offices to continue to improve its practice of transmitting information. Through a continuous exchange with the prosecution authorities, MROS seeks to reduce the number of cases where jurisdiction for a case is disputed.

7. International cooperation in the fight against money laundering

7.1 Egmont-Group

The exchange of information with other FIUs represents a key element of MROS's analytical work. MROS's international and holistic approach is crucial, particularly in the case of complex structures, for identifying and grasping the full extent of a potential offence or a case complex.
In order to ensure the best possible exchange with other FIUs, MROS has been a member of the Egmont Group since 1998. The Egmont Group is an international network of 166 independently operating FIUs specialised in detecting and combating money laundering, its predicate offences, and terrorist financing. The Egmont Group is guided by the standards of the Financial Action Task Force (FATF), the leading international body for combating money laundering and terrorist financing (see Chapter 7.2). At the operational level, the Egmont Group facilitates the exchange of information between the FIUs of the various member countries as designed by the FATF Principles. Since the revision of the FATF Recommendations in 2012, membership in the Egmont Group is also a prerequisite for an adequate anti-money laundering and counter-terrorism system.
As a member of the Egmont Group, MROS is committed to adhering to the Egmont Principles. The Egmont Principles are derived from FATF Recommendation 29 (paragraphs 8–12). This recommendation regulates the operational independence of an FIU, which should be free from undue influence or interference. This is one of the basic principles of an FIU and is a prerequisite for international exchange, which is based on reciprocity and confidentiality. The FIU's autonomy also gives the financial intermediaries the necessary basis of trust to submit a SAR in the event of suspicion.
The objectives of the Egmont Group are to:

- create the conditions necessary for an international, systematic exchange of information;
- help FIUs increase their efficiency by developing training strategies and promoting staff exchange programmes;
- enable the international exchange of information between FIUs under secure conditions;
- ensure the operational independence of FIUs; and
- support the establishment of centralised FIUs.

The Heads of Financial Intelligence Units (HoFIU) are the Egmont Group's main governing body. A plenary meeting is held once a year to discuss and make important decisions together. The venue changes annually. In 2022, the 28th Egmont Plenary took place in Riga, Latvia, from 10 to 15 July 2022.
The HoFIUs are supported by the Egmont Committee, a consultation and coordination mechanism, and the Egmont Group Secretariat, based in Canada.

The Egmont Group also has four working groups:

Information Exchange Working Group (IEWG)
The IEWG has the task of identifying synergies in connection with the operational and strategic activities of the individual FIUs and ensuring that these are used accordingly. Furthermore, the working group pursues the goal of constantly improving cooperation and the exchange of information.

Membership, Support, and Compliance Working Group (MSCWG)
The MSCWG ensures that the Egmont Group's high standards and membership criteria are applied to both new members and existing member FIUs.

Policy and Procedures Working Group (PPWG)
The PPWG provides advice on strategic issues, including the effective exchange of information between the FIUs and adherence to international standards (FATF).

Technical Assistance and Training Working Group (TATWG)
The TATWG is responsible for identifying, developing and delivering technical assistance and training to all FIU members of the Egmont Group, FIUs that are in the process of joining, as well as all observer organisations and other international partners of the Egmont Group.
Each of these working groups is led by a Chair and one or more Vice-Chairs from different FIUs around the world. Regular meetings (plenary or working groups) are held throughout the year. MROS takes part in these meetings.
In addition to the working groups, regional groups meet to address region-specific challenges and questions. All FIUs are assigned to a group based on their geographical area. The FIUs in Europe are divided into two groups: Europe I comprises the FIUs of the EU member states and Europe II includes all other FIUs, including MROS. A working and regional group meeting took place in February 2022. The meeting, which was held virtually because of the COVID-19 pandemic, focused on the renewal of the IT infrastructure used by the FIUs to exchange information (IT Renewal Project). In addition, a training session was held on the vulnerabilities of virtual assets in connection with combating money laundering. Strengthening practical know-how in the detection and combating of money laundering and terrorist financing is a constant focus of the working group meetings.

7.2 GAFI/FATF

The Financial Action Task Force (FATF), also known by its French name, *Groupe d'action financière (GAFI)*, is an inter-governmental body established by the G7 at a ministerial meeting in Paris in July 1989. It is the leading body in the fight against money laundering and sets international standards that aim to prevent these illegal activities. The member states are required to implement the FATF Recommendations. The FATF periodically evaluates the implementation of its recommendations in the individual member states. The results of these evaluations and their corresponding justification are published in a report.
In the fourth round of evaluations now underway, the degree of technical compliance and the effectiveness of the implementation of the recommendations are being assessed. The FATF also carries out compliance evaluations to examine the extent to which certain non-member states combat money laundering and terrorist financing, and draws up two public lists. One list contains states that are considered high-risk countries, i.e. they are not cooperative and do not combat money laundering and terrorist financing effectively, thus they do not meet the international standards set by the FATF with their legislation and measures. A second list includes those countries that show strategic deficiencies but have committed themselves to following an action plan and addressing their shortcomings.
As part of the Swiss delegation to the FATF, MROS participates in the meetings of the FATF's Risk Trends and Methods Group (RTMG). The RTMG works to identify and analyse recurring patterns and characteristics of crimes related to money laundering and terrorist financing on the basis of specific cases in order to combat these illegal activities more effectively.

Reports published in 2022 deal with the tracking of financial flows from human trafficking and the illegal trade in fentanyl and other synthetic opioids. A study on illegal trade in art and cultural assets is planned for 2023. This is a sector with a high risk of money laundering and terrorist financing. Other projects are underway, including projects on ransomware, terrorist financing through crowdfunding and cyber fraud. MROS is actively involved in some of these projects.
Other FATF working groups include the Policy Development Group (PDG), responsible for aspects relating to regulations and guidelines; the Evaluations and Compliance Group (ECG), responsible for assessing and ensuring the quality of the peer review reports conducted of countries and follow-up reports; the International Cooperation Review Group (ICRG); and the Global Network Coordination Group (GNCG).

7.3 Bilateral meetings with FIUs

Bilateral exchanges with other FIUs provide MROS with an important opportunity to discuss specific topics of information exchange bilaterally in a targeted and in-depth manner. Each FIU has developed its own methods to deal with the ever-increasing number of reports, new trends and ever-changing technical challenges. And yet all FIUs pursue the same goal, which is to combat money laundering, its predicate offences and terrorist financing.
In this context, MROS focused in 2022 on deepening exchanges with a number of its key partners. MROS can look back on very successful bilateral meetings with the UK Financial Intelligence Unit, FIU – the Netherlands, Quad Island Forum[69] and FinCen.[70] Topics included the Swiss PPP, which is being planned under the auspices of MROS. Similar projects have already been successfully implemented in other jurisdictions. Furthermore, the possibilities of data processing and dealing with the permanently increasing information load were discussed.

In addition to meetings with individual FIUs, MROS also took part in meetings attended by several FIUs in order to exchange information. The meeting of the French-speaking FIUs, held in Rabat, Morocco, from 27 to 28 September 2022, focused on virtual assets and the associated challenges for FIUs. Further topics were the prevention of the use of non-profit organisations for terrorist financing purposes and the effective implementation of targeted financial sanctions. The meeting of the German-speaking FIUs, which took place in Vienna, Austria, from 12 to 13 December 2022, focused on the exchange of experiences and findings with regard to identifying and preventing individual predicate offences to money laundering.

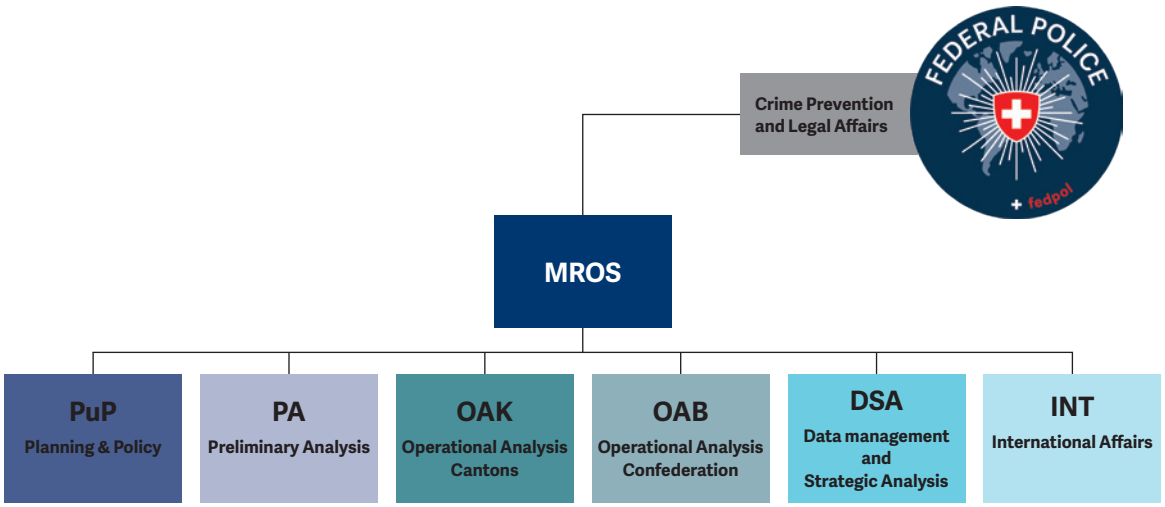
[69] The Quad Island Forum of Financial Intelligence Units is a strategic alliance of the Gibraltar, Guernsey, Isle of Man and Jersey FIUs.

[70] FinCEN stands for 'Financial Crime Enforcement Network'. It is the FIU in the USA.

8. Organisation of MROS

MROS is part of fedpol's Crime Prevention & Legal Affairs Directorate. It conducts its core operational tasks completely independently, which is in line with international requirements.

In 2020, MROS was reorganised and subdivided into six divisions, each with its own specific tasks. As of 2022, it had an average of 61 occupied positions corresponding to a total of 48 full-time equivalents (FTEs).



The individual divisions are shown in the organisation chart above, which reflects the current organisation of MROS.

Planning and Policy (PuP)
The division PuP is a classic cross-sectional unit and thus deals with complex issues. Its main tasks consist of processing political business and providing support for all MROS projects and publications (e.g. annual reports, legislative revisions, legal opinions on MROS-specific specialist topics). The unit supports the operational divisions of MROS and ensures the coherency and consistency of practice. It maintains regular exchanges with other authorities and takes care of MROS's administrative business.

Primary Analysis (PA)
The division PA is responsible for collecting and processing all incoming reports in terms of form, technology and content, including manual corrections in case of poor data quality. PA also

triages the cases and transfers them to one of the downstream divisions on the basis of an overall assessment. In addition, it is responsible for national administrative assistance under Art. 29 AMLA.

Operational Analysis Cantons (OAK)
The division OAK analyses incoming SARs, most of which fall under the jurisdiction of the cantonal prosecution authorities and have been assigned by PA. If there are grounds for suspicion, the aggregated information is forwarded to the competent prosecution authority (usually the cantonal prosecution authorities). Information can also be shared with other national authorities and FIUs of other countries.

Operational Analysis Confederation (OAB)
The division OAB analyses incoming SARs which a priori fall within the competence of the federal prosecution authority, i.e. the OAG, and have been assigned by PA. If there are grounds for suspicion, the aggregated information is forwarded usually to the OAG or, if applicable, to the cantonal prosecution authorities. Information can also be shared with other national authorities and FIUs of other countries.

Data Management and Strategic Analysis (DSA)
The division DSA is responsible for the secure operation of the MROS information system (goAML) and its technical development. In doing so, it also provides technical support to financial intermediaries, especially in programming their interfaces. The DSA is also responsible for developing the technical possibilities for processing SARs. The sector carries out MROS's strategic analyses and evaluates a wide variety of data in connection with money laundering, its predicate offences and terrorist financing in order to identify risks, trends and money laundering methods.

International Affairs (INT)
The division INT deals with all (information) exchanges with foreign FIUs as well as membership in and participation in international bodies (including the Egmont Group, FATF, United Nations Convention against Corruption and the Europol Financial Intelligence Public-Private-Partnership).