Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Money Laundering Reporting Office (MROS)

Annual Report 2023

May 2024

Money Laundering Reporting Office (MROS)

Annual Report 2023

May 2024

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

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

Website: *www.fedpol.admin.ch*

Table of contents

1. Foreword

Over the past decade, the number of suspicious activity reports (SARs) has risen by an average of 20–30 % per year. While this trend continued in 2023, the increase was much larger than expected. By the end of 2023, the Money Laundering Reporting Office Switzerland (MROS) had received a total of 11,876 SARs which corresponds to an estimated 21,500 business relationships and an average of 47 SARs per working day. This is a 56 % increase compared to the previous year.

The total reporting and data volume has risen overall, with MROS receiving a total of 21,375 reports: SARs, financial intermediary (FI) replies to MROS information requests (Art. 11*a* AMLA[1]), terminated business relationship notifications (Art. 9*b* AMLA), international information requests received from other financial intelligence units (FIUs) as well as spontaneous information reports from national and international authorities (see Chap. 4). Communication with financial intermediaries takes place almost exclusively via the goAML information system. The majority of the data submitted by financial intermediaries is structured. This development is encouraging. However, there is still potential for data submitted by national authorities – the proportion of unstructured data here is still very high and currently accounts for roughly 30 % of the total data volume (see Chap. 3).

In 2023, MROS forwarded a total of 866 cases to the prosecution authorities. This constitutes a decrease of nearly 30 % compared to the previous year. One of the reasons for this is MROS's strategy of taking a risk-based approach and focusing on serious crime. The analyses carried out by MROS in this area go into greater depth and are more complex. In 2023, MROS forwarded 43 % more cases to the Office of the Attorney General of Switzerland (OAG) than in the previous year; in contrast, the volume of cases forwarded to cantonal prosecution authorities – with the exception of the public prosecutor of the Canton of Geneva – are declining. There were also no more cases forwarded relating to COVID fraud in 2023. Furthermore, SARs are increasingly being bundled together in cases forwarded to prosecution authorities. The number of forwarded cases is therefore lower and a comparison with previous years is only meaningful to a limited extent (see Chap. 2.2).

Bern, May 2024
Federal Department of Justice and Police FDJP
Federal Office of Police fedpol
Money Laundering Reporting Office MROS

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

2. Main strategic developments

2.1 High reporting volume – Reasons

Over the past decade, the number of SARs has risen by an average of 20–30 % annually. There are many reasons for this. The main driving factor has been the continuous expansion of regulatory due diligence and reporting requirements since 2013. This has resulted in a significant tightening of financial market supervision and enforcement. The many corruption and money laundering scandals involving a large part of the Swiss banking sector have further heightened awareness of the importance of effectively combating money laundering among financial intermediaries. Many banks have increased the number of staff in their compliance and financial crime departments. In addition, technological progress has enabled them to continuously improve their transaction monitoring capabilities. The switch from paper-based reporting to the IT application goAML (government office Anti Money Laundering) and the XML[2] integration on 1 January 2020 have made it easier for financial intermediaries to submit SARs. All of these developments have led to a surge in the volume of SARs received by MROS.
This trend continued in 2023 – although the increase was considerably steeper than expected. By the end of 2023, MROS had received a total of 11,876 SARs. That is 4,200 more SARs than in the previous year, amounting to a 56 % increase. The reporting volume has risen two-fold over the past two years and ten-fold over the past ten years. This impressive reporting volume requires both an assessment and a forecast for the coming years. MROS and its strategic orientation are significantly affected by this increase.

MROS believes that the marked increase in reporting volume can be attributed to the following factors:

- **Anchoring the definition of reasonable grounds for suspicion in legislation:** The 'SIF proposal'[3] came into force on 1 January 2023. This means that the concept of 'reasonable grounds for suspicion', which had already been established in practice and case law over the past decade, has now also been legally anchored (Art. 9 para. 1^{quater} AMLA). Accordingly, financial intermediaries are now required to always submit a SAR if there is a specific indication or several indications that assets could be of criminal origin and if these suspicions cannot be ruled out through their own clarification procedures. Some of the reporting volume is most likely due to the now unambiguous wording of this new legislative provision.
- **More rigorous application of Art. 37 AMLA**: The criminal penalties for failing to comply with the reporting obligation have been toughened. Analysis of the judgments of the

[2] 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/en/home/kriminalitaet/geldwaescherei/meldung.html.*

[3] *https://www.fedlex.admin.ch/eli/oc/2021/656/de*, see Federal Council Dispatch of 26 June 2019 on proposed changes to the Anti-Money Laundering Act, *BBl 2019 5451, p. 5477 ff*.

Federal Department of Finance (FDF) and the Federal Criminal Court (FCC) shows that compliance officers from lower hierarchies are now increasingly being held accountable as well.[4] The number of convictions for negligent breach of reporting obligations has also increased.[5] Discussions with financial industry representatives have made it clear that this stricter practice is having an impact on the sector and is therefore also influencing behaviour. The prevailing sentiment is that it is better to report too much than too little.

– **Audit firms and (internal) auditors with stricter standards:** Feedback from financial intermediaries suggests that audit firms and internal control bodies tend to assess compliance with regulatory AML requirements more strictly. This is most likely due to the general tightening of the supervisory and AML measures combined with greater media focus on the audit issue.
– **Financial intermediaries with asymmetric business models are under increasing cost pressure:** The cost pressure placed on the financial industry is palpable. In some instances, suspicions are only clarified in a very rudimentary manner and the special duties of due diligence under Art. 6 AMLA, which are mandatory for a SAR to MROS, are no longer or only insufficiently carried out. This trend is particularly noticeable among financial institutions not involved in wealth management that have aggressive onboarding programmes for foreign clients. Most of these inadequately clarified SARs are of no value to MROS. With this behaviour, financial intermediaries are no longer or inadequately fulfilling their role as the 'first line of defence' in the AML system. MROS is in dialogue with FINMA about the financial intermediaries concerned and the measures taken.

It can be assumed that the reporting surge will continue in 2024 and beyond. Experience shows that such developments are generally irreversible. Once the described reporting behaviour has been established, it becomes the standard. The financial industry is unlikely to change course, especially as the signals from the law enforcement and supervisory authorities as well as the Financial Action Task Force on Money Laundering (FATF) tend to point to a tightening of the rules. We can therefore expect even greater reporting volumes in the future. MROS is only partially equipped for a further increase in the reporting volume – similar to what was experienced in 2023 – and is reaching the limits of its human and technical resources. By applying the 'risk-based approach' (see Chap. 2.2), increasing numbers can be absorbed by tightening the criteria for triage. However, this also means that the decisive factor in the decision to analyse a SAR would no longer be the risk but the resource situation.

2.2 Orientation of MROS – further development of the 'risk-based approach'

MROS has substantially changed its working methods over the years. Due to the drastic increase in SARs and reporting volume, MROS is no longer able to analyse and process all information with the same detail as was possible five or ten years ago. MROS is forced to set priorities and focus on specific issues. Since introduction of the goAML information system on 1 January 2020, MROS has adopted a 'risk-based approach' when receiving and processing SARs: all incoming SARs are assigned a risk category using a 'triage matrix'. They are then prioritised and analysed to varying extents based on this categorisation. MROS focuses on combating serious crime – the emphasis is placed on organised crime, terrorist financing and certain forms of white-collar crime. With this approach, MROS is also guided by law enforcement strategies. It carries out its tasks in a success-oriented manner and takes into account potential reputational risks for the Swiss financial sector.

---

[4] Between 2014 and 2022, the FDF/Federal Criminal Court handed down at least 21 final convictions. At the end of 2022, 47 proceedings were pending (Source: 'Strafrechtliche Verantwortlichkeit des Compliance Officers', Speech given by Dr Doris Hutzler on 8 June 2023 at the 14th Symposium on Economic Crime Legislation, Europa Institut Zurich (EIZ)).

[5] See: *Federal Supreme Court Ruling 6B_1176/2022 dated 5 December 2023*.

MROS's strategy is also reflected in current statistics. While cases forwarded to the Office of the Attorney General of Switzerland (OAG) increased in 2023 (+43 % compared to 2022)[6], cases forwarded to cantonal prosecution authorities – with the exception of the Canton of Geneva – decreased compared to previous years. This is because MROS is increasingly forwarding cases related to serious crimes. In 2023, MROS forwarded a total of 866 cases to prosecution authorities. In comparison, 1,232 cases were forwarded in 2022 and 1,486 in 2021.[7] Although this constitutes a decrease in numerical terms, cases forwarded in 2023 contained more SARs and responses from financial intermediaries per case. In 2021, a forwarded case to the prosecution authorities contained an average of 1.3 SARs; in 2023, 1.8. Moreover, additional information from financial intermediaries was processed in 44 % of the cases forwarded to the prosecution authorities in 2023 (in 2021: 18 % and 2022: 25 %). These figures show that MROS's current analyses tend to contain more information and are more complex. MROS is thus moving away from the traditional processing approach of '1 SAR equals 1 case forwarded to the prosecution authorities' towards active intelligence and the networking of existing information. The focus of analysis is no longer on the SAR as such, but on the information that it contains.

MROS will continue to systematically develop its intelligence strategy – focus, triage, prioritise, network – over the coming years. The fact is, however, that the proportion of SARs that can be analysed in depth is steadily decreasing due to the continuous increase in reporting volume.[8] In 2023, one in five SARs was analysed in depth.[9] The remaining 80 % of SARs were analysed less intensively or using holistic analysis methods (e. g. clustering methods). Some of the SARs were already discarded upon receipt. This means that the SAR and the information it contains will not be further processed. However, these SARs can be reactivated and further processed at any time thanks to preparation and storage in the goAML information system. In 2023, over 300 discarded (old) SARs were reactivated in this manner when new information was received (e. g. SAR from another financial intermediary or spontaneous information provided by a foreign FIU).

With the rise in SARs, the risk of significant cases of money laundering remaining undetected is increasing. MROS is endeavouring to improve its processing speed and efficiency. Limiting factors in the receipt and triage of SARs are, in addition to human resources, technical support (automation, intelligent IT support) as well as the data quality of the incoming SARs and the information provided by financial intermediaries. The latter have a significant impact on data processing efficiency. The poorer the data quality, the more time-consuming it is to process the data. To close these gaps, improved IT support and/or more staff resources would be needed.

In 2023, MROS pressed ahead with the 'goAML Futuro'[10] IT project, which seeks to achieve greater interoperability through the automated synchronisation of accessible justice and police databases. MROS has also made progress to reduce data disruptions. The greatest challenge for MROS – and therefore also the greatest potential for increasing efficiency – is the data quality of incoming SARs. The planned introduction of Art. 23 para. 7 AMLA as part of the current revision of the AMLA[11] is essential for MROS as the new provision would empower fedpol to issue a technical ordinance specifying the form and format (data standard) in which data are to be submitted.

---

6 Cases forwarded to the Office of the Attorney General of Switzerland: 2022: 79; 2023: 113.

7 See Chap. 4.7): The statistics for 2021 and 2022 also include 'COVID reports'. The statistics for these years are therefore higher.

8 The number of SARs increased by 56 % and the total reporting volume rose by 63 % in 2023.

9 In-depth analysis: 2021: 45 %; 2022: 32 %.

10 See explanations given in *MROS Annual Report 2022*, p. 13 f.

11 *Federal Council press release*, 30.08.2023: 'Federal Council initiates consultation on strengthening the anti-money laundering framework.'

2.3 National risk assessment – Sectoral report on cryptocurrencies and virtual assets

Every country's anti-crime strategy should include consideration of the risks posed by money laundering and terrorist financing. To date, Switzerland has published two comprehensive national risk assessments (2015[12] and 2021[13]) and comprehensively assessed the risks that arise. The interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF)[14] is responsible for preparing NRAs as well as the underlying sectoral risk reports. MROS is part of this coordination group; as head of the Analysis subgroup, MROS is responsible for preparing the risk reports.
Under MROS's guidance, the sectoral risk report entitled, 'National Risk Assessment (NRA): Risk of money laundering and the financing of terrorism through crypto assets'[15] was adopted by the CGMF on 5 December 2023. The first report on the topic of crypto assets was published in 2018.[16] The report described the threats and vulnerabilities for Switzerland as 'significant'. The influence and importance of virtual assets (VA) have changed dramatically since 2018. There has been a marked increase in understanding and awareness in the market. MROS now receives VA-related SARs on a daily basis and VA-related cases have now become part of the day-to-day work of prosecution authorities. MROS has identified four key developments:

1. In Switzerland, the number of financial intermediaries with VASP activities has risen significantly from less than ten in 2018 to over 204 at the end of 2022. Despite this, at least 180 of these FIs have not submitted a SAR to MROS.
2. Between 2018 and 2023, VA use in Switzerland intensified; a growing number of private individuals and companies are using and accepting VAs for payments in commerce, for services and for investments. The boundaries between the traditional financial sector and the VA sector are becoming increasingly blurred; VAs are being integrated into traditional payment platforms to a larger extent and the 'two worlds' are converging.
3. The criminal use of VAs has risen both in Switzerland and globally. It has also become much more diverse. Prosecution authorities are increasingly confronted with VA-related cases involving different economic sectors. For example, a larger number of criminal charges are being filed in connection with theft or other forms of stealing (e. g. fraud, misappropriation) of VAs. The amount of damage linked to VAs has risen sharply and is expected to be at least in the double-digit millions in Switzerland in 2022 (compared to just under CHF 7 million in 2007). The use of VAs has become routine in certain criminal offences (e. g. investment fraud, ransomware). VAs have become a common tool of financial crime.
4. In recent years, FIs in Switzerland have increasingly identified suspected cases of ML/TF involving VA-related transactions on client accounts. This has led to a sharp increase in the submission of VA-related SARs to MROS: in 2022, nearly 14 % of all SARs were linked to VAs. These included links to politically exposed persons (PEPs), international corruption scandals, transnational organised crime groups or state actors.

The report concludes that ML/TF risks in the VA sector have grown compared to 2018. Threats and vulnerabilities that were already identified

---

[12] CGMF, *1st National report on the risks of money laundering and terrorist financing*, June 2015

[13] CGMF, *2nd National report on the risks of money laundering and terrorist financing in Switzerland*, October 2021

[14] The interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF) is run by the State Secretariat for International Finance (SIF). *Link* to CGMF remit.

[15] CGMF, *National Risk Assessment (NRA), Risk of money laundering and the financing of terrorism through crypto assets*, January 2024

[16] CGMF, *National Risk Assessment: Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018

in 2018 have largely become more acute and broader. Due to their heightened importance and the risks associated with them, VAs require the necessary attention from all stakeholders (financial intermediaries, FIUs, prosecution authorities, supervisory authorities as well as supervisory and self-regulatory organisations).

Despite the identified threats and vulnerabilities for Switzerland in relation to ML/TF in the VA sector, various factors help to mitigate these risks:
- International cooperation in VA-related investigations shows that increased tracing, freezing and confiscation of VAs are effective in combating money laundering and terrorist financing.
- Many small VASPs have now disappeared or merged. This has also prompted large crypto exchanges to strengthen their compliance measures, which has the effect of reinforcing AML/CFT efforts worldwide.
- Blockchains are inherently more transparent than traditional payment systems. This leads to better traceability of VAs; blockchain analytics tools can identify and track suspicious activity more easily.
- Finally, in Switzerland, the expansion of the definition of financial intermediation in the VA sector helps to bring a broader range of actors under the scope of the Anti-Money Laundering Act. This closes gaps within the AML/CFT system.

Based on the findings of the report, the CGMF proposes four measures to strengthen the current AML/CFT framework in the VA sector:
1. **Improve the level of data and knowledge about the VA sector in Switzerland**
   Information on the VA sector and the criminal use of VAs in Switzerland is essential to adequately identify, understand and assess ML/TF risks.
2. **Encourage FIs with VASP activities to become more proactive in their reporting practices**
   In the future, VASP FIs should step up their ML/TF monitoring activities in order to be in a better position to detect suspicious transactions and report them to MROS.
3. **Provide sufficient capacity and resources for AML/CFT efforts in the VA sector**
   Cooperation between all relevant stakeholders must be improved in order to address ML/TF challenges in the VA sector.
4. **Intensify international cooperation**
   Switzerland should continue to work at international level to effectively tackle criminal risks in the financial sector and expedite implementation of the FATF's Recommendation.

The NRA concludes by emphasizing the need for Switzerland to take VA-related risks seriously and adopt appropriate measures to effectively counter money laundering and terrorist financing. VAs are becoming an increasingly important part of the financial sector; Switzerland must rise to the challenge in order to keep pace with rapid developments.
The sectoral report 'National Risk Assessment (NRA): Risk of money laundering and the financing of terrorism through crypto assets' was published in the first quarter of 2024.[17] MROS is currently planning to produce additional sectoral risk assessments: 'Proliferation financing' (expected publication date Q3/2024), 'Legal entities' (expected publication date Q4/2024) and 'Real estate market' (expected publication date sometime in 2025).

2.4 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 is to further enhance AML/CFT capabilities in Switzerland. In 2022, MROS 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 experts consisting of representatives from the financial sector on the appropriateness

[17] CGMF, *National Risk Assessment (NRA) - Risk of money laundering and the financing of terrorism through crypto assets*, January 2024.

and framework conditions of a PPP. The various authorities and experts concluded that a PPP can greatly improve anti-crime efforts, particularly in terms of prevention. MROS drafted a report[18] detailing the key outcomes of discussions with authorities and experts. This report was submitted to the Federal Council for consideration in April 2023. A working group consisting of MROS, SIF and representatives from various areas of the financial industry has been set up for this purpose. Work to establish a 'Swiss PPP' is still ongoing. By the end of 2024 at the latest, all outstanding issues should have been clarified and a viable exchange between the public and private sector, based on rules to be established, should have taken place.
MROS is already part of a PPP. It is a member of the Europol Financial Intelligence Public Private Partnership (EFIPPP).[19] Established in 2017 by the European Financial and Economic Crime Centre (EFECC), which is part of Europol, EFIPPP seeks to encourage cross-border cooperation and the exchange of information between Europol, prosecution authorities, FIUs, supervisory organisations and regulated financial service providers. EFIPPP is the first cross-border information exchange platform. When it was founded in 2017, EFIPPP consisted of 28 public and private institutions from eight EU and non-EU member states. By early 2022, 79 institutions from 18 EU and non-EU member states had joined EFIPPP.

EFIPPP objectives are as follows:

- Build a common level of information and understanding;
- Jointly develop risk indicators and threat typologies;
- Facilitate the exchange of operational and/or tactical intelligence associated with ongoing investigations (in accordance with the applicable national and international legal frameworks);
- Identify gateways for the exchange of information and legal barriers in this regard (in accordance with the applicable national and EU legal frameworks);
- Promote the use of new tools for combating financial crime, leveraging new technologies and exchanging common experience and methods for innovation and trainings;
- Support domestic cooperation forums in relevant jurisdictions with the goal to act as an effective hub between the different platforms and facilitate public-private-partnership information and intelligence sharing.

EFIPPP is built around four levels:
- **Strategic Oversight Body:** provides strategic advice and coordination in matters related to EFIPPP's development and focus areas (meets annually).
- **Steering Group**: directs the activities of EFIPPP and acts as its decision-making body. The group defines the priorities for every calendar year, approves new members and regulates the activities of the working groups.
- **Working Groups:** implement the objectives of EFIPPP and develop the EFIPPP products and papers. There are currently seven working groups. They are the operational heart of EFIPPP.
- **Threat and Typologies Group:** dedicated to building knowledge on specific threats.

MROS greatly benefits from the information shared within EFIPPP. MROS's 'Alert' to the Swiss financial sector on terrorist financing dated 3 November 2023 and the 'Addendum' dated 5 December 2023 were largely based on information and analyses obtained from EFIPPP. Today, the reliable exchange of information at international level is crucial in ensuring efficient and credible action to combat money laundering. MROS is actively involved in EFIPPP and has been a member of the Steering Group since December 2023.

[18] *MROS report: Strengthening the AML/CFT Framework through Information Sharing, March 2023*.

[19] *EFIPPP Homepage - EFIPPP.*

2.5 Draft legislation on the transparency register and revised AMLA

2.5.1 Main features

At its meeting on 12 October 2022, the Federal Council instructed the FDF to draft a bill to increase transparency and facilitate the identification of the beneficial owners of legal entities. The aim of the draft legislation is to strengthen the integrity of Switzerland as a financial and economic centre. It provides for the introduction of a federal register of beneficial owners (transparency register) as well as other measures needed to enhance the effectiveness of the system used to fight money laundering and white-collar crime. The proposed measures will enable Switzerland to respond to the latest international standards (FATF and Global Forum) and ensure its compliance with these standards. The draft legislation contains the following points:

- The creation of a federal **transparency register** of beneficial owners of legal entities. This is a register that is not publicly accessible and is managed by the Federal Department of Justice and Police (FDJP). The control body, which is part of the FDF, ensures that the quality of the register is checked and has appropriate sanction instruments at its disposal.
- The introduction of **due diligence obligations** in accordance with the Anti-Money Laundering Act for particularly **high-risk advisory activities** (subjecting advisors and lawyers to the AMLA).
- Additional **measures** covering trade in real estate, precious metals and gemstones. Finally, the obligations of financial intermediaries in monitoring the implementation of coercive measures under the Embargo Act[20] will be clarified.

2.5.2 Impact on MROS

The draft legislation also includes provisions that would require financial intermediaries to notify the transparency register if the information at their disposal does not match information contained in the register and, in particular, if these discrepancies raise doubts as to the accuracy, completeness or timeliness of the information on the beneficial owner of a legal entity (Discrepancy Reporting; DR). MROS, in turn, has a duty to report to the transparency register if its analyses cast doubt on the register information regarding the beneficial owner. [21] The sharing of information between register authorities and MROS takes place by virtue of the revised administrative assistance provisions contained in the AMLA.[22]

The inclusion of high-risk advisory activities under the AMLA creates a new reporting population for MROS, particularly – but not only – in connection with the formation and structuring of legal entities, which will lead to a further increase in the reporting volume. The further amendments to the AMLA (including those relating to trade in real estate, precious metals and gemstones) close important gaps and help to further reinforce Switzerland's ML/TF defences.

MROS supports and welcomes the draft legislation on the transparency register and further revision of the AMLA, not least because successful implementation of the draft legislation will also be decisive for the FATF's country evaluation. A good outcome of the FATF evaluation rounds is of great strategic importance to Switzerland as an international business hub and financial centre.

---

[20] Federal Act on the Implementation of International Sanctions (Embargo Act, EmbA), CC 946.231.

[21] Draft LETA (Federal Act on the Transparency of Legal Entities and the Identification of Beneficial Owners [Legal Entity Transparency Act; LETA]).

[22] New Art. 29 para. 1 AMLA.

2.6 International developments

2.6.1 Sanctions against Russia

Sanctions in response to Russia's military aggression against Ukraine and the Federal Council's decision of 28 February 2022, in which Switzerland adopted the sanctions of the European Union (EU) against Russia[23], continued to keep MROS busy in 2023. In its previous annual report, MROS clarified that a distinction must be made between the various reporting systems and responsibilities (sanctions: State Secretariat for Economic Affairs SECO; money laundering: MROS).
SECO is responsible for monitoring compliance with the reporting obligation and the sanctions regime. While reporting to SECO does not necessarily mean that a SAR needs to be sent to MROS, financial intermediary due diligence and reporting obligations under the AMLA still apply. If investigations into a possible violation or evasion of sanctions also provide indications of money laundering, then the financial intermediary must carry out additional clarifications (Art. 6 AMLA). Depending on the outcome of these clarifications, a SAR may be submitted to MROS.[24] The prerequisite for a SAR is always that the assets involved in a business relationship are suspected to be connected with the support of a criminal or terrorist organisation or are being used for money laundering purposes, originate from a felony or an aggravated tax misdemeanour, 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 only qualifies as a felony in serious cases – a simple violation of sanctions therefore does not constitute a predicate offence within the meaning of money laundering legislation.[25]
As in 2022, MROS did not find any significant change in reporting behaviour with regard to sanctions in the reporting year. Although some SARs related to sanction violations and circumventions, most were also linked to suspected money laundering, organised crime or terrorist financing. From MROS's perspective, the impression remains that financial intermediaries are able to clearly differentiate between the different reporting systems and responsibilities and file their corresponding reports accordingly.
In 2023, MROS also regularly responded to information requests and provided spontaneous information reports in connection with sanctions-related measures within the international information exchange with partner authorities. Where legal requirements were met, incoming requests from foreign FIUs were answered and/or brought to the attention of the competent domestic authority by way of administrative assistance.
In early 2022, MROS joined the Russia-Related Illicit Finance and Sanctions FIU Working Group (**RRIFS**). This is an FIU task force in which other FIUs are represented alongside Switzerland.[26] The exchange of information is based on AMLA provisions and Egmont Principles. The international exchange of information is both a core task of MROS and a necessity.

2.6.2 Hamas' terrorist attacks against Israel

In addition to Russia's military aggression against Ukraine, MROS was also concerned with another international issue: Hamas' terrorist attacks on Israel. In this context, MROS has joined the Counter Terrorist Financing Taskforce Israel (CTFTI).[27] The legal basis for involvement in this taskforce is the same as that of the RRIFS Working Group. Unlike Russia's military aggression against Ukraine, Switzerland has not imposed any sanctions against Hamas. On 11 October

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

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

[25] Art. 9 para. 1 and 2 Federal Act on the Implementation of International Sanctions (Embargo Act; SR 946.231).

[26] *Russia-Related Illicit Finance and Sanctions FIU Working Group (RRIFS Task Force).*

[27] *Counter Terrorist Financing Taskforce – Israel (CTFTI Task Force).*

2023, the Federal Council decided to ban Hamas in Switzerland. On 22 November 2023, it instructed the FDJP and the Federal Department of Defence, Civil Protection and Sport (DDPS) to prepare the consultation draft of special-purpose legislation (known as the Hamas Act) by the end of February 2024. On 21 February 2024, the Federal Council decided to initiate the consultation procedure, which will continue until 28 May 2024. However, entry into force will still take some time.[28]

A financial intermediary is already subject to a reporting obligation if it has reasonable grounds to suspect that financial flows are connected with a terrorist organisation or are being used to finance or support it. [29] In practice, however, it is very difficult to clarify this. As long as Hamas has not been clearly designated as a terrorist organisation or banned, any payment made to Hamas, for example, does not in itself justify a SAR under the Money Laundering Act in connection with the support for a terrorist organisation within the meaning of Art. 260ter SCC, as there must also be a suspicion that the funds in question are being used for terrorism or are connected with a crime or an aggravated tax misdemeanour. The qualification of Hamas as a terrorist organisation and a corresponding ban established in the Hamas Act would create clarity here, so that a mere transaction would be enough to give rise to a sufficient suspicion of a predicate offence under the Money Laundering Act.

2.7 'Top-30 project' in the international division

International cooperation is a cornerstone of MROS's activities. Money laundering is a global phenomenon that does not conform to national borders. Much of the information analysed by MROS includes intelligence obtained from partner authorities abroad (foreign FIUs). Conversely, the latter are increasingly requesting (financial) information that MROS either already has in its system or can obtain from financial intermediaries in Switzerland. The exchange of information has intensified in recent years. Information requests to and from foreign FIUs are not only increasing in quantity, but are also much more extensive in terms of content than in the past. One of the main reasons for this development is the expanded powers given to MROS in 2021 to obtain further information from financial intermediaries based on the analysis of information from foreign FIUs (Art. 11*a* para. 2bis AMLA). Foreign FIUs have realized that they can obtain information from Swiss financial intermediaries via MROS. The exchange of information across national borders is subject to strict requirements, but is actively utilised.

In order to improve international cooperation, streamline processes and share information more efficiently, it is important to understand the needs and special characteristics of partner FIUs. For this reason, MROS launched the 'Top 30 Project' in 2023, in response to a recommendation made by the Swiss Federal Audit Office (SFAO) on 20 December 2021.[30] The aim of the project was to analyse the incoming information from foreign FIUs and the outgoing replies from MROS in order to identify cooperation patterns, peculiarities and weaknesses of the collaboration. Data from 1 July 2021 (date of entry into force of Art. 11*a* para. 2bis AMLA) to 30 June 2022 was analysed. Unsurprisingly, eight of the ten FIUs that submitted the most information requests to MROS were from Europe. In addition, the top 30 included FIUs that have major financial centres themselves or other close (economic) ties to the Swiss financial centre. Well-known jurisdictions that are attractive for the creation of domiciliary companies were also among the top 30. The same applied to spontaneous information reports received from foreign partner FIUs and MROS information requests to FIUs abroad.

Cooperation was assessed both qualitatively and quantitatively. Foreign FIUs were asked about their level of satisfaction with the content and timeliness of the replies from MROS. The feedback was positive – both for the requests sent by

[28] *Federal Council opens consultation on draft legislation to ban Hamas*

[29] Art. 9 AMLA in connection with Art. 260ter SCC.

[30] *SFAO, Evaluation Report on Money Laundering Reporting Office*, 20 December 2021

MROS to foreign FIUs as well as for the responses from MROS to other FIUs.
The replies from foreign FIUs were assessed both in terms of information content and processing time. It should be noted that the exchange of information always depends on the legal framework of the respective country. For example, some information may only be available for a short period of time (short retention period) or the disclosure of other information may require a court order. Bilateral and personal exchanges between MROS and foreign FIUs greatly helps to improve the quality of information requests and replies (on both ends). This leads to greater mutual understanding of the legal and actual possibilities and hurdles.
The processing time for information requests was discussed many times, as it can vary greatly for a number of reasons. The information must be obtained from the financial intermediaries – unless it is already available in the information system due to a SAR – and then processed. It usually takes some time before MROS can begin to analyse an information request in depth.
Fast processing is a challenge partly because of the steadily increasing number of information requests and partly because of the many manual processing steps. Increased efficiency thanks to a modern IT infrastructure is also key for information sharing at international level. A global comparison clearly shows that FIUs or countries with a high level of technology at their disposal (e. g. in connection with database queries, accessible registers) tend to respond more quickly. Processing time is a key factor in the fight against money laundering and terrorist financing and therefore crucial for MROS to avoid having to compromise on quality.
FIU satisfaction with MROS replies to information requests greatly improved following introduction of Art. 11*a* para. 2bis AMLA. Since the introduction of this article on 1 July 2021, MROS now has the legal authority to approach financial intermediaries and request that they disclose the requested information, even if there is no SAR in the information system, which was previously not permitted.

2.8 MROS Crypto Symposium

MROS is receiving a growing number of SARs with a connection to cryptocurrencies. The number of financial intermediaries operating as VASPs has multiplied in recent years.[31] In order to highlight and discuss the associated challenges, MROS held its first crypto symposium in Zug on 30 October 2023. The event drew around 160 participants (mainly representatives of VASPs and self-regulatory organisations [SROs]). The speakers (representatives of national and international authorities as well as the private sector) discussed regulatory and supervisory issues as well as risks associated with cryptocurrencies. They spoke about the various challenges involved in tracing incriminated cryptocurrencies, combating money laundering and terrorist financing and detecting criminal offences involving the use of cryptocurrencies.
The State Secretariat for International Finance (SIF) focused on the regulatory framework at national and international level and on the legal status of cryptocurrencies in Switzerland. The Swiss Financial Market Supervisory Authority (FINMA) highlighted the legal challenges in supervision and enforcement proceedings. MROS stressed the importance of identifying risks and thus the need for national risk assessments (NRA). The FIU of Luxembourg emphasised the need for national and international cooperation in the fight against money laundering using practical examples of terrorist financing. The Zurich Public Prosecutor's Office focused on the prosecution of organised crime and the role of cryptocurrencies. This picture was completed by the Guardia di Finanza from Italy, which presented new investigative approaches and methods in connection with cryptocurrencies, including the Metaverse. The event concluded with a presentation by a commercial law firm, which used practical examples to bridge the gap between the private sector and the authorities and emphasised the complexity of the subject matter from a consultant's perspective.

[31] See Chap. 2.3.

Figure 1 – Invitation to MROS Crypto Symposium

3. goAML information system

The goAML information system introduced in January 2020, which allows SARs to be received and processed electronically, is a key element in the implementation of MROS's strategy to digitalise and increase efficiency. Four years after its introduction, the system has become fully established among financial intermediaries. It has been running smoothly with minimal service disruption. Over 96 % of all incoming SARs and FI replies to MROS information requests under Art. 11*a* AMLA take place via goAML. This is an encouraging development. Virtually all communication with financial intermediaries takes place via goAML. The data is transmitted in a structured form. Currently, only the terminated business relationship notifications[32] under Art. 9*b* AMLA are submitted mostly in an unstructured way through the goAML Message Board. However, this is a transitional solution: with the introduction of goAML version 5.2, unstructured transmission will no longer be possible. In the future, financial intermediaries will be required to make all transmissions using an XML file or through the web interface.

There are still deficits in the quality of the data records submitted by financial intermediaries. The rejection rate fell to 10 % in 2023.[33] However, one in every ten SARs is still rejected and sent back to financial intermediaries due to non-compliance with the submission requirements.

[32] The financial intermediary is authorised to terminate the business relationship after 40 working days from receipt of the SAR, provided that MROS does not forward the SAR to a prosecution authority within this period. The reporting financial intermediary must notify MROS if the business relationship is terminated (see Art. 9*b* para. 3 AMLA).

[33] Previous year: 2022: 14 %; 2021: 24 %; 2020: 41 %.

Table 1 – Information received by MROS 2023

Information received in 2023 (as of 31.12.2023)	Total (number)	Unstructured: by post or via secure email[34]	Proportion per category	Total proportion
All national and international reports *	21375	5857		
All national reports	19944	4426	–	22.2%
Sender: Financial intermediaries	16436	1502	9.1%	7.5%
• Suspicious activity reports (SARs)[35]	11876	158	1.3%	
• Replies received from FIs in response to information requests made under Art. 11a AMLA[36]	1891	70	3.7%	
• Terminated business relationship notifications[37]	2669	1274	47.7%	
Sender: National authorities	3508	2924	83.4%	14.7%
• Prosecution authorities	2643	2643	100%	
(of which by post)		(1799)	68%	
(of which by secure email)		(844)	32%	
• Other authorities	865	281	32.5%	

** The figures also include incoming international information requests and spontaneous information from foreign FIUs.*

While only 9% of FI submissions contained unstructured data, the proportion for national authorities is over 80%. These submissions are sent to MROS either by post or via a the goAML Message Board, with 68% of submissions from national authorities being sent by post. In such cases, MROS is responsible for manual data entry, which increases workload. MROS has discussed the issue with the prosecution authorities and will continue to engage with them in 2024 in order to reduce the proportion of unstructured data in the medium term.
In summer 2023, MROS introduced goAML version 5.2 (from 4.9), initially only internally for testing and introduction purposes. This change will result in IT adjustments for financial intermediaries in 2024. The financial intermediaries concerned were notified of these changes in December 2023. In order to ensure a smooth transition, MROS has provided information on the technical requirements and set up a test environment. All financial intermediaries are expected to have completed the transition from the old XSD schema to the new one by the end of 2024. During this transition phase, MROS will continue to accept old XML files. The new version of goAML will improve the analytical capabilities of MROS. When programming version 5.2, UNODC[38] took into account many of MROS's concerns and requirements. This new version simplifies data processing for both financial intermediaries and MROS financial analysts.

[34] The goAML system has a secure email function (goAML Message Board), which ensures E2EE (end-to-end encryption) communication between goAML-registered parties and MROS.

[35] SARs submitted by virtue of duty to report (Art. 9 AMLA) and right to report (Art. 305ter para. 2 SCC) provisions.

[36] This includes all requests pursuant to Art. 11*a* AMLA (para. 1, para. 2 and para. 2bis).

[37] Notifications under Art. 9*b* AMLA (termination of the business relationship).

[38] United Nations Office on Drugs and Crime (UNODC).

4. MROS annual statistics

MROS compiles anonymised statistics to analyse information on money laundering, its predicate offences, organised crime and terrorist financing during a given financial year.[39] These statistics include, in particular, the number of SARs received from financial intermediaries, the number of information requests received from relevant foreign authorities and the proceedings that follow SAR submission (see Art. 23 para. 1 MROSO[40]).

4.1 General Overview for 2023

*The volume of incoming **SARs** continued to increase in 2023: In 2023, MROS received **11,876** SARs, which corresponds to around 47 SARs per working day. Compared to 2022 (7,639), this amounts to a 55.5 % increase. Since introduction of the goAML information system in January 2020, the figure has more than doubled (see Figure 2).*
***90.5 %** of SARs come from financial intermediaries in the **banking sector** (average 2014–2023: 89.4 %).*
*In 2023, MROS sent **866 cases to prosecution authorities.** Compared to the previous year, this corresponds to a decrease of 29.7 % (1,232); however, the cases were more extensive (see Chap. 4.7). The average number of SARs submitted to the prosecution authorities per case increased (2023: 1.8; 2022: 1.4). MROS sends the prosecution authorities an analysis report containing relevant information. These analysis reports may consist of several SARs, which were not necessarily received by MROS in the same year and originate from various national and foreign authorities.*
*The number of **information requests** under **Art. 11a AMLA** increased further (+7.1 % compared to the previous year): MROS's aim is to provide prosecution authorities with the best possible support, which requires certain SARs to be analysed in depth. Art. 11a para. 2bis AMLA, which came into force in 2021[41], resulted in MROS increasingly obtaining information from financial intermediaries not directly involved in the SAR (third-party intermediaries).*
***Information sharing** between MROS and **Swiss authorities** is becoming more frequent: in 2023, MROS received 696 information requests from other Swiss authorities (+4.3 %). At the same time, MROS transmitted 200 spontaneous information reports to domestic supervisory authorities or authorities responsible for combating money laundering and its predicate offences, organised crime or terrorist financing (+13.0 %).*

[39] Financial year: 1 January to 31 December of the given year.

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

[41] Art. 11a para. 2 und para. 2bis AMLA form the legal basis for MROS to also obtain information from third-party intermediaries who have not submitted a SAR (see Chap. 4.12).

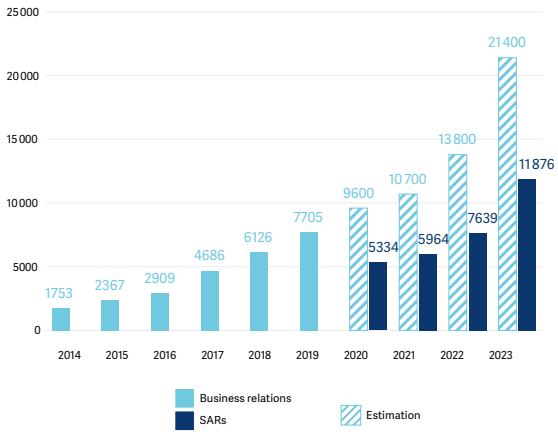
4.2 SARs

The number of SARs has been increasing from year to year. In 2023, MROS received a total of 11,876 SARs, which amounts to an average of 47 incoming SARs per working day in 2023. This corresponds to an increase of 55.5 % over the previous year. Since the introduction of the goAML information system in 2020, the total volume of SARs submitted has more than doubled (see Figure 2).

The number of reported business relationships since 2014 has skyrocketed: in 2014, 1,753 suspicious business relationships were reported to MROS; in 2023, the figure was around 21,400.[42] The number of business relationships reported annually has increased more than twelvefold during this time.

There are several reasons for this increase. For one thing, financial intermediaries have become more sensitive and aware of the issue of money laundering. Secondly, changes in legislation – particularly with regard to the definition of reasonable grounds for suspicion – and advances in the area of digitalisation (e. g. improved transaction monitoring and internal analysis tools) have also had an impact (see Chap. 2.1).

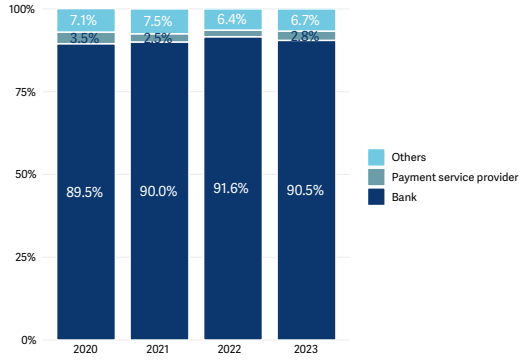
Figure 2: Number of business relationships reported, 2014–2023



4.3 Number of SARs by financial intermediary category

The vast majority of SARs received by MROS come from financial intermediaries in the banking sector. In the current reporting year that reflected 90.5 % of the reports (- 1.1 percentage points compared to 2022; see Figure 3). The reporting behaviour of these financial intermediaries therefore has a significant influence on the number and type of SARs that MROS receives. The distribution of SARs among reporting entities has hardly changed since introduction of the goAML information system.

Figure 3: SARs by financial intermediary category, 2020–2023



The same pattern can be seen in the number of business relationships reported by the various financial intermediary categories prior to 2020 (see Table 2).

[42] The method of counting SARs changed with the introduction of goAML. In order to be able to compare the figures with previous years, Figure 2 takes the number of SARs submitted and multiplies this figure by 1.8 (i. e. the average number of business relationships per SAR in 2019). This means the 11,876 SARs submitted in 2023 are the equivalent of 21,400 business relationships.

Table 2: SARs by branch, 2014 to 2023[43]

Financial intermediary category	2014[1]	2015[1]	2016[1]	2017[1]	2018[1]	2019[1]	2020[2]	2021[2]	2022[2]	2023[2]	2023 in absolute figures	Average 2014–2023
Bank	85.3%	91.3%	86.0%	91.0%	88.8%	89.9%	89.5%	90.0%	91.6%	90.5%	10744	89.8%
Payment service provider	6.1%	2.4%	4.4%	3.1%	4.4%	4.0%	3.5%	2.5%	2.0%	2.8%	328	2.9%
Fiduciary	2.8%	2.0%	1.5%	1.1%	0.7%	0.8%	0.6%	0.5%	0.1%	0.2%	25	0.8%
Asset manager	2.3%	1.9%	2.2%	1.9%	1.0%	0.9%	0.8%	1.0%	0.6%	0.8%	90	0.8%
Insurance	0.6%	0.5%	3.1%	0.5%	0.6%	0.3%	0.4%	0.3%	0.3%	0.4%	47	0.3%
Other financial intermediary	0.2%	0.2%	0.7%	0.4%	2.3%	0.6%	2.3%	2.1%	2.1%	2.0%	240	2.1%
Credit card company	0.5%	0.5%	0.7%	0.3%	1.2%	1.3%	1.6%	1.7%	1.6%	1.3%	154	1.5%
Casino	0.5%	0.1%	0.5%	0.6%	0.5%	0.7%	0.5%	0.5%	0.7%	0.5%	65	0.6%
Attorney	0.6%	0.3%	0.2%	0.1%	0.1%	0.1%	0.1%	0.1%	0.0%	0.1%	14	0.1%
Loan, leasing and factoring business	0.2%	0.3%	0.3%	0.3%	0.3%	0.3%	0.4%	0.3%	0.3%	0.2%	26	0.3%
Securities trader	0.6%	0.1%	0.1%	0.3%	0.1%	0.3%	0.0%	0.2%	0.1%	0.2%	22	0.1%
Commodity and precious metal trader	0.2%	0.3%	0.1%	0.2%		0.3%	0.2%	0.5%	0.3%	0.3%	38	0.3%
Foreign exchange trader			0.1%			0.3%	0.0%					0.0%
SRO	0.1%					0.1%	0.0%			0.1%	6	0.0%
Currency exchange							0.1%	0.1%	0.3%	0.6%	75	0.4%
Supervisory authority (FINMA/ESBK/Gespa)	0.1%							0.1%		0.0%	2	0.0%
Distributor of investment funds				0.1%								0.0%
Trust and loan companies							0.1%	0.1%				0.0%
Total	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**11876**	**100.0%**

[1] *Based on former calculation method (business relationships)*

[2] *Based on new calculation method (SARs)*

4.4 The legal basis for SARs

The legal basis for a SAR depends on the degree of suspicion. If there are reasonable grounds for suspicion, financial intermediaries have a duty under Art. 9 para. 1 let. a AMLA[44] to report to MROS. In the case of simple suspicion, financial intermediaries have a right to report under Art. 305ter para. 2 SCC[45]. Since 2018, SARs submitted by virtue of the duty to report – as opposed to the right to report – have become more prevalent. This trend further intensified in 2023. In that year, financial intermediaries subject to AMLA provisions reported 70.4% of SARs based on the duty to report under Art. 9 para. 1 letter a AMLA. The right to report under Art. 305ter para. 2 SCC was used in 21.6% of the SARs. The prevalence of the right to report has once again decreased significantly compared to the previous year (-9.1 percentage points). It can be assumed that the significant increase in the volume of SARs submitted under the duty to report in 2023 is partly due to the entry into force of the revised AMLA on 1 January 2023:

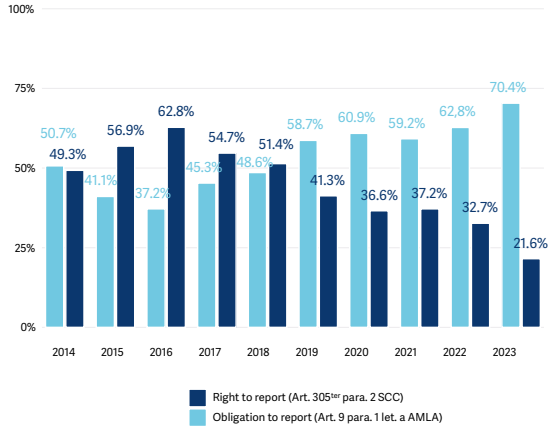
[43] The absolute figures for 2014–2022 are published in the respective *MROS annual reports*.

[44] Art. 9 para. 1 let. a AMLA: A financial intermediary must immediately file a report with the Money Laundering Reporting Office Switzerland (the Reporting Office) as defined in Art. 23) if it knows or has reasonable grounds to suspect that assets involved in the business relationship (1.) are connected to an offence in terms of Art. 260ter or 305bis SCC, (2.) are the proceeds of a felony or an aggravated tax misdemeanour under Art. 305bis no. 1bis SCC, (3.) are subject to the power of disposal of a criminal or terrorist organisation, or (4.) serve the financing of terrorism (Art. 260quinquies para. 1 SCC).

[45] Art. 305ter para. 2 SCC: The persons included in paragraph 1 are entitled to report to the Money Laundering Reporting Office in the Federal Office of Police any observations that indicate that assets originate from a felony or an aggravated tax misdemeanour in terms of Art. 305bis no. 1bis.

Art. 9 para. 1quarter AMLA now clarifies 'reasonable grounds for suspicion'.[46]

Figure 4: SARs referring to existing business relationships, by legal basis, 2014–2023

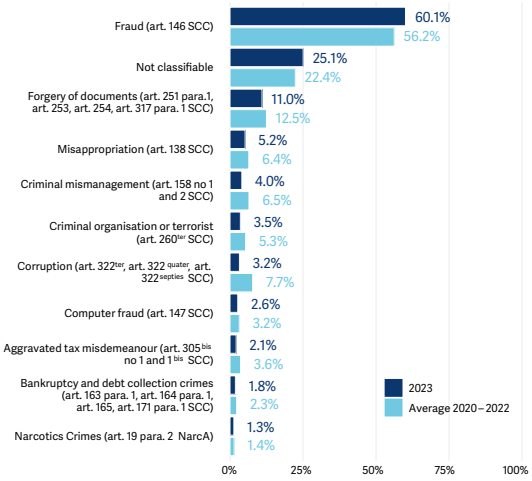


In 941 cases (7.9 %), the financial intermediaries reported that they had broken off negotiations to enter into a business relationship due to reasonable grounds for suspicion under Art. 9 para. 1 letter a AMLA.[47]

4.5 Predicate offences

When submitting their SARs, financial intermediaries indicate which predicate offences they suspect. There has been little change in the frequency distribution of suspected predicate offences since 2020 (see Figure 5). In 2023, the top ten were the same as in 2020, with financial intermediaries citing fraud in most SARs (2023: 60.1 %; 2020–2022: 56.2 %).

Figure 5: Frequency of suspected predicate offences, 2020–2023, Multiple answers possible



There is a slight tendency for financial intermediaries to increasingly cite fraud as a suspected predicate offence, while predicate offences such as bribery and criminal mismanagement are becoming less common. The available figures do not enable us to establish whether this trend is the result of a change in the reporting behaviour of financial intermediaries or of a shift in the underlying actual predicate offences.
Generally speaking, the information provided by financial intermediaries on suspected predicate offences does not allow conclusions to be drawn about the actual money laundering predicate offence committed. These figures only reflect the predicate offences suspected at the time the financial intermediary submitted the SAR. The analysis carried out by MROS may also lead to suspicion of another predicate offence. A detailed analysis of predicate offences was carried out by the Interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMT) in 2022.[48]

[46] Art. 9 para. 1quarter AMLA stipulates that 'reasonable grounds to suspect' under Art. 9 para. 1 let. a AMLA exist if the financial intermediary has specific evidence or several indications that Art. 9 para. 1 let. a AMLA may apply to the assets involved in the business relationship, and that this suspicion cannot be dispelled on the basis of additional clarifications within the meaning of Art. 6 AMLA.

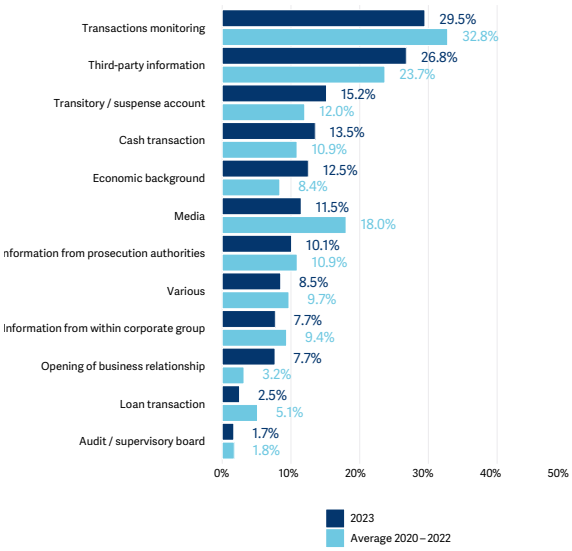
[47] Art. 9 para. 1 let. b AMLA: A financial intermediary must immediately file a report with the Money Laundering Reporting Office Switzerland (the Reporting Office) as defined in Article 23 if it terminates negotiations aimed at establishing a business relationship because of a reasonable suspicion as defined in Art. 9 para. 1 let. a AMLA.

[48] See Interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMT): *National report on risks of money laundering and terrorist financing*, October 2021, p. 25–29.

4.6 Factors arousing suspicion

As in previous years, transaction monitoring is the most frequently mentioned reason why financial intermediaries submitted a SAR to MROS in 2023 (2023: 29.5 %; 2020–2022: 32.8 %; see Figure 6). In 15.2 % of the SARs received in 2023, transitory accounts were the trigger for suspicion. However, external sources of information also played a significant role in the financial intermediaries' assessment: in 2023, 26.8 % of SARs were based on information from third parties (2020–2022: 23.7 %).

Figure 6: Main factors arousing suspicion 2020–2023[49], Multiple answers possible



4.7 MROS cases forwarded to prosecution authorities

In 2023, MROS forwarded 866 cases to prosecution authorities under Article 23 para. 4 AMLA. This corresponds to a 29.7 % decrease compared to the previous year (2022: 1,232). The cases forwarded in 2023 are more detailed compared to the previous year: in 2022, a MROS case sent to the prosecution authorities was based on an average of around 1.4 SARs that MROS had received from financial intermediaries; in 2023, in contrast, the cases were based on an average of 1.8 SARs.

The 866 MROS cases contained information from:

- 1,201 SARs received in 2023
- 276 SARs received in 2022
- 28 SARs received in 2021
- 12 SARs received in 2020
- 5 business relationships reported in 2019
- 3 business relationships reported in 2018
- 2 business relationships reported in 2017

This year again shows that the size of a canton's financial sector has a significant impact on the number of MROS cases submitted to the respective public prosecutor's office (see Table 3). In 2023, as in previous years, most MROS cases were forwarded to the public prosecutor's offices of the cantons of Geneva (17.6 %) and Zurich (16.3 %). The Office of the Attorney General of Switzerland (OAG) came in third at 13.0 % – which constitutes a 6.6 percentage point increase over the previous year.

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

Table 3: Cases forwarded to prosecution authorities, 2020–2023

Autority	2020	2021	2022	2023	2023 in absolute figures	Average 2020–2023
Geneva	11.5%	11.3%	11.6%	17.6%	152	13.0%
Zurich	18.9%	21.1%	20.4%	16.3%	141	19.2%
Office of the Attorney General of Switzerland	9.0%	9.1%	6.4%	13.0%	113	9,4%
Vaud	11.1%	11.6%	10.6%	8.3%	72	10.4%
Bern	7.5%	6.7%	6.9%	6.5%	56	6.9%
St. Gallen	3.5%	4.0%	6.3%	5.3%	46	4.8%
Ticino	5.0%	4.8%	3.6%	4.6%	40	4.5%
Aargau	5.3%	5.2%	6.7%	4.2%	36	5.3%
Thurgau	3.0%	2.1%	2.6%	3.2%	28	2.7%
Lucerne	3.5%	2.9%	2.6%	2.5%	22	2.9%
Valais	2.7%	2.4%	3.0%	2.2%	19	2.6%
Zug	2.5%	2.6%	2.2%	2.2%	19	2.4%
Schwyz	1.0%	1.1%	1.9%	2.1%	18	1.5%
Basel-Stadt	2.6%	2.3%	2.3%	1.8%	16	2.3%
Basel-Landschaft	2.1%	1.7%	2.3%	1.8%	16	2.0%
Solothurn	1.9%	2.0%	2.1%	1.4%	12	1.8%
Friburg	2.7%	3.1%	2.1%	1.3%	11	2.3%
Neuchâtel	2.3%	1.9%	1.7%	1.3%	11	1.8%
Appenzell Ausserrhoden	0.6%	0.8%	1.3%	0.9%	8	0.9%
Schaffhausen	0.5%	0.5%	0.6%	0.7%	6	0.6%
Jura	0.3%	1.0%	0.2%	0.7%	6	0.6%
Graubünden	1.5%	1.0%	1.1%	0.6%	5	1.0%
Nidwalden	0.3%	0.4%	0.6%	0.6%	5	0.5%
Glarus	0.2%	0.1%	0.4%	0.6%	5	0.3%
Appenzell Innerrhoden	0.0%	0.1%	0.2%	0.2%	2	0.1%
Uri	0.3%	0.1%	0.2%	0.1%	1	0.2%
Obwalden	0.2%	0.1%	0.2%	0.0%	0	0.1%
Total	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**866**	**100.0%**

All in all, MROS sent 13% of its cases (113) to the OAG and 87% to cantonal prosecutor's offices (753).

4.8 Feedback from prosecution authorities

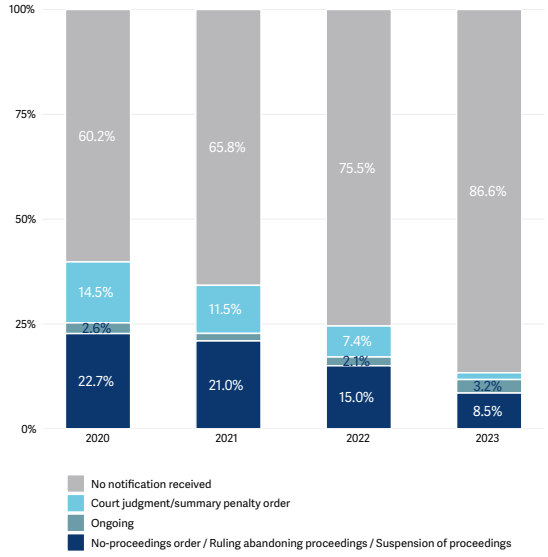
According to Art. 29*a* AMLA, prosecution authorities notify MROS of all pending proceedings, in particular those relating to money laundering, criminal and terrorist organisations and/or the financing of terrorism. They promptly send MROS the relevant judgments or ruling abandoning proceedings.[50] In addition, they immediately notify MROS of any ruling on the basis of a case forwarded to them by MROS.[51] This feedback is crucial to MROS's mission of providing the best possible support to prosecution authorities.

[50] Art. 29*a* para. 1 AMLA: The prosecution authorities shall notify the Reporting Office without delay of any pending proceedings connected with Art. 260ter, 260quinquies para. 1, 305bis and 305ter para. 1 SCC. They shall provide the Reporting Office without delay with judgements and decisions on the closure of proceedings, including the grounds therefor.

[51] Art. 29*a* para. 2 AMLA.

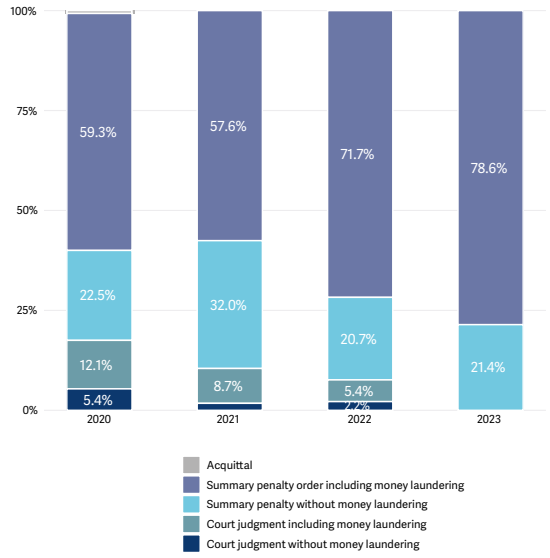
The prosecution authorities have not yet provided any feedback on most of the cases that MROS forwarded to them (see Figure 7 as well as information provided in Chap. 6.2). It is therefore not possible to draw any conclusions regarding the ratio of judgments to ruling abandoning proceedings on the basis of currently available figures.

Figure 7: Feedback in relation to cases forwarded in the given year, 2020–2023



Of the cases forwarded to the prosecution authorities between 2020 and 2022[52], MROS lacks information on the status of proceedings in two thirds of cases. The response rates vary significantly depending on the canton.
Money laundering was the main offence in the feedbacks received by MROS from the prosecution authorities up to the end of 2023 that resulted in a summary penalty order or a judgement (78,6 %; see Figure 8). In 2022, 77,1 % of judgements or summary penalty orders related to money laundering; In 2021, the figure stood at 66,3 % and in 2020 71,4 %.

Figure 8: Breakdown of the communicated judgements/ summary penalty orders, 2020–2023



4.9 Terrorist financing

In 2023, 93 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.[53] This represents 0.8 % of the total number of SARs received in 2023, most of which are also linked to other predicate offences. Other grounds for suspicion were membership in a criminal and terrorist organisation (30 cases)[54], fraud[55] (7 cases), and two cases each of aggra-

[52] Considering that it takes a certain amount of time for prosecution authorities to report back to MROS, the figures for the current reporting year have not been included in the statistics.

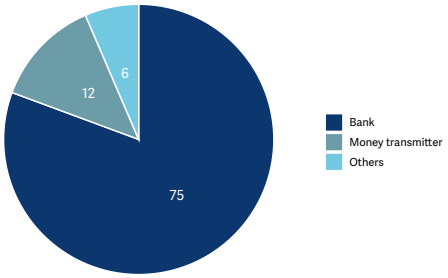
[53] Federal Act on the Proscription of Al-Qaeda, Islamic State and Associated Organisations (SR 122), repealed with effect from 1 December 2022.

[54] Art. 260ter SCC.

[55] Art. 146 SCC.

vated tax misdemeanour[56], bribery[57], forgery of a document[58] and/or embezzlement[59].
Most SARs of suspected terrorist financing come from banks (75 out of 93; see Figure 9); twelve came from payment service providers.

Figure 9: SARs submitted on suspicion of terrorist financing, by financial intermediary category, 2023



In 2023, the triggers of suspicion most frequently mentioned by financial intermediaries were press reports (37 cases), transaction monitoring (19 cases) as well as information from third parties (16 cases), from a group of companies (13 cases) or from prosecution authorities (10 cases) as well as cash transactions (13 cases).
Of the 93 terrorism-related SARs in 2023, MROS forwarded five cases to the relevant prosecution authority. Three of the SARs received in the previous year 2022 involving suspected terrorist financing were also forwarded to the competent prosecution authorities in 2023.

4.10 Organised crime

In 2023, MROS received 421 SARs indicating suspected ties with a criminal or terrorist organisation. This represents 3.5 % of the total reporting volume.
The vast majority of these SARs (90.0 %) were submitted by the banking sector (see Figure 10). The trigger for a SAR was information obtained in the media (37 %) and/or transaction monitoring (25 %; see Table 5). In addition to suspected ties with a criminal organisation, the financial intermediaries also mentioned fraud (44 %) and bribery (8 %; see Table 4) as possible predicate offences. The 421 SARs indicating suspected ties with a criminal or terrorist organisation resulted in 33 cases forwarded to the relevant prosecution authorities.

Figure 10: SARs submitted on suspicion of ties with a criminal or terrorist organisation, by financial intermediary category, 2023

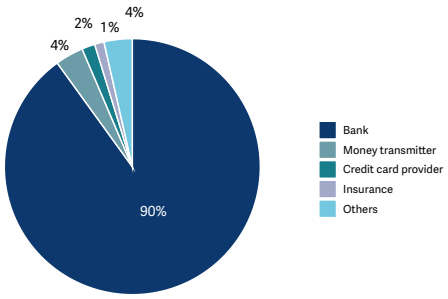


Table 4: Other predicate offences mentioned in SARs relating to suspicion of ties with a criminal or terrorist organisation

Other predicate offences (Multiple answers possible, most frequently mentioned)	**Number of mentions**	**In %**
Fraud (Art. 146 SCC)	185	44 %
Bribery (Art. 322ter, Art. 322^{quater}, Art. 322^{septies} SCC)	33	8 %
Financing of terrorism (Art. 260quinquies SCC)	27	6 %
Narcotics Act (Art. 19 para, 2, NarcA)	26	6 %
Misappropriation (Art. 138 SCC)	23	5 %
Document forgery (Art. 251 no 1, Art. 253, Art. 254, Art. 317 al. 1 SCC)	18	4 %

[56] Art. 305bis Ziff. 1 and 1bis SCC.
[57] Art. 322ter, Art. 322^{quater} or Art. 322^{septies} SCC.
[58] Art. 251 Ziff.1, Art. 253, Art. 254, Art. 317 Ziff. 1 SCC.
[59] Art. 138 SCC.

Other predicate offences (Multiple answers possible, most frequently mentioned)	**Number of mentions**	**In %**
Aggravated tax misdemeanour (Art. 305 bis no 1 and 1 bis SCC)	15	4%
Criminal mismanagement (Art. 158 no 1 and 2 SCC)	15	4%
Extortion (Art. 156 SCC)	8	2%

Table 5: Frequency of other factors arousing suspicion in SARs submitted on suspicion of ties with a criminal or terrorist organisation

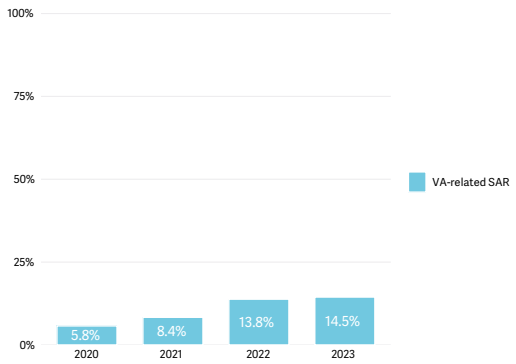
Factors arousing suspicion (Multiple answers possible, most frequently mentioned)	**Number of mentions**	**In %**
Media reports	155	37%
Transaction monitoring	105	25%
Third-party information	80	19%
Transitory / suspense account	49	12%
Various	46	11%
Cash transaction	44	10%
Opening of business relationship	43	10%
Information from prosecution authorities	38	9%
Economic background	31	7%
Information from within corporate group	25	6%
Loan transaction	12	3%

4.11 SARs involving the use of cryptocurrencies

SARs relating to cryptocurrencies (virtual assets, VA) are becoming more prevalent.[60] In 2023, cryptocurrencies featured in 14.5 % of all incoming SARs. This is two and a half times as many as in 2020 (5.8 %; see Figure 11).[61] This development creates greater challenges for MROS: cryptocurrencies make it more difficult to trace money flows and thus the origin of the assets and also make it harder to clearly identify the beneficial owner.

In the sectoral report 'National Risk Assessment (NRA): Risk of money laundering and the financing of terrorism through crypto assets', MROS analysed the risks associated with cryptocurrencies. This report was published in the first quarter of 2024 (see Chap. 2.3).[62]

Figure 11 : Share of VA-related SARs in the total number of SARs, 2020–2023



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

Since 2021, the number of information requests sent to financial intermediaries based on Article 11*a* AMLA has been steadily increasing. In the reporting year, there was again an increase in information requests compared to the previous year (+7.1 %; see Figure 12). This increase is mainly due to the fact that more requests were made to third-party intermediaries that are or were involved in a transaction or business relationship

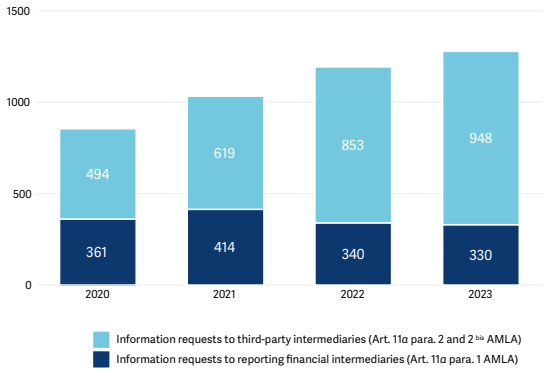
[60] The term 'virtual currency' was used for the first time in Switzerland in a legislative text on 1 January 2006: Art. 4 para. 2 let. a in the Ordinance of 11 November 2015 on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Ordinance, AMLO; SR 955.01).

[61] The extent to which transactions with cryptocurrencies are the subject of suspicion in a SAR cannot yet be determined directly, as such transactions are not clearly identifiable. SARs with a relevant VASP connection were therefore identified on the one hand by means of transactions between the accounts indicated in the SAR and accounts of Swiss or foreign financial intermediaries with VASP activity and on the other hand by means of a keyword list of relevant terms. It can therefore be assumed that the prevalence of cryptocurrencies in SARs tends to be understated.

[62] CGMF, *National Risk Assessment (NRA) - Risk of money laundering and the financing of terrorism through crypto assets*, January 2024.

in addition to the reporting financial intermediary (+11.1 %; Art. 11*a* para. 2[63] and 2[bis] AMLA[64]). In contrast, the number of information requests sent to reporting financial intermediaries under Art. 11*a* para. 1 AMLA[65] remained fairly constant (-2.9 % compared to the previous year).

Figure 12: Requests for information under Article 11a AMLA, 2020–2023

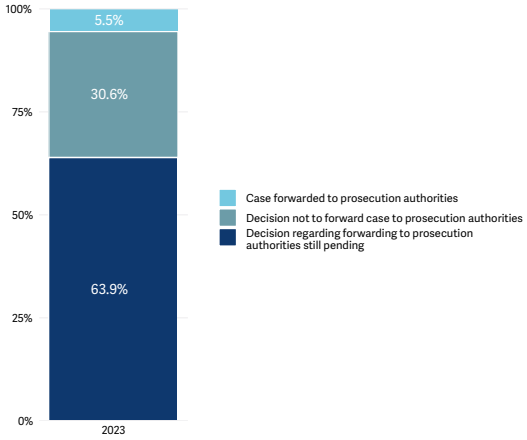


4.13 Terminated business relationship notification under Art. 9*b* AMLA

Since 1 January 2023, financial intermediaries may, by virtue of Art. 9*b* AMLA[66], terminate a business relationship 40 working days after they have reported it to MROS – provided that MROS has not notified them that the case has been forwarded to the prosecution authorities. However, the financial intermediary must notify MROS immediately when a reported business relationship has been terminated.[67]

In 2023, MROS received 2,669 terminated business relationship notifications. 5.5 % of these related to SARs that MROS had forwarded to the prosecution authorities after the period of 40 working days. 63.9 % related to SARs for which MROS had not yet made a decision to forward and 30.6 % related to SARs that MROS chose not to forward (see Figure 13).

Figure 13: Status of SARs for which a terminated business relationship notification was received, 2023



4.14 Information sharing with foreign financial intelligence units (FIUs)

In the fight against money laundering and its predicate offences, terrorist financing and organ-

63 Art. 11*a* para. 2 AMLA: If, based on this analysis, it becomes apparent that in addition to the financial intermediary making the report, other financial intermediaries are or were involved in a transaction or business relationship, the financial intermediaries involved must on request provide the Reporting Office with all related information that is in their possession.

64 Art. 11*a* para. 2[bis] AMLA: If, on the basis of the analysis of information from a foreign reporting office, it becomes apparent that financial intermediaries subject to this Act are or have been involved in a transaction or business relationship in connection with this information, the financial intermediaries involved must, on request, disclose to MROS all related information to the extent that it is available to them.

65 Art. 11*a* para. 1 AMLA: If the Reporting Office requires additional information in order to analyse a report that it has received in accordance with Art. 9 AMLA or Art. 305[ter] para. 2 SCC, the financial intermediary making the report must on request provide such information that is in its possession.

66 Under Art. 9*b* AMLA, a financial intermediary may terminate a business relationship reported under Art. 9 para. 1 let. a AMLA or Art. 305[ter] para. 2 SCC if MROS does not notify the financial intermediary within a period of 40 working days that the reported information has been forwarded to a prosecution authority.

67 Art. 9*b* para. 3 AMLA.

ised crime, the exchange of information between MROS and foreign FIUs works via requests for administrative assistance. If MROS receives SARs on foreign parties (natural persons or legal entities), MROS can obtain information about these from the FIUs in the relevant jurisdictions. This information is essential for MROS's analyses, as many SARs have international links.[68] The number of information requests that MROS has sent to foreign FIUs has risen steadily in recent years. In 2023, MROS sent 280 information requests to 67 different FIUs abroad – an increase of 6.9 % compared to the previous year.
In July 2021, MROS was given expanded powers in the area of information exchange with foreign partner FIUs (Art. 11*a* para. 2bis AMLA). As a result, the number of information requests that MROS received from foreign FIUs rose sharply in 2022 (2022: 851 requests from 89 countries). Since then, MROS has been allowed to enrich its responses to partner FIUs with further relevant financial information. In some cases, this can lead to more complex requests and more time-consuming processing than was the case prior to 2021. In 2023, however, the number of information requests from 92 countries decreased (705; -17.2 %). MROS processed 350 of these as well as 306 requests from the previous year.
Foreign FIUs and MROS can also exchange spontaneous information reports. This type of information sharing does not involve a prior request. In the reporting year, MROS received 726 such spontaneous information reports from 53 countries (2022: 709 from 50 countries). MROS sent 160 spontaneous information reports to 47 foreign FIUs (2022: 178 to 42 foreign FIUs).

4.15 Information sharing with Swiss authorities

Under Art. 29 AMLA, MROS may also share relevant information with Swiss authorities – upon request or spontaneously. These include supervisory or other authorities that are involved in the fight against money laundering and its predicate offences, organised crime or terrorist financing. Statistics from previous years show that information sharing with domestic authorities has become more important since 2020.[69] In the current reporting year, MROS received 696 information requests from 29 Swiss authorities regarding specific bank accounts, persons or companies (an increase of 4,3 % over the previous year).
As in previous years, most of the information requests came from police authorities: 82,0 % of the requests came from a cantonal police or the Federal Criminal Police.
In 2023, MROS also received 119 spontaneous information reports from domestic authorities (2022: 109). For its part, MROS sent 200 spontaneous information reports to Swiss supervisory and other authorities (+13,0 %; 2022: 177). MROS may also request information from other federal, cantonal or communal authorities; these requests are not listed in the figures above.

[68] See interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF): *National risk assessment: risks of money laundering and terrorist financing in Switzerland*, October 2021.

[69] See Federal Office of Police (Fedpol), Publications of the Money Laundering Reporting Office (MROS), *Annual Reports.*

5. Typologies[70]

The system for combating money laundering and terrorist financing is complex. As a hub, MROS can make a substantial contribution to providing a holistic view in situations where information is only available in fragmented form. The efficient use of legally available instruments and the ability to cross-reference information at its disposal provide MROS with an overall picture that brings tangible added value to prosecution and other authorities. MROS refers to these tasks as 'creating intelligence', in which it also sees its central role. In this chapter, specific examples are used to illustrate MROS's understanding of 'intelligence'.

5.1 Typology 1 – National and international cooperation

The following case illustrates the importance of national and international cooperation in the fight against money laundering, its predicate offences, organised crime and terrorist financing. Only through the national and international exchange of information can individual pieces of information in various systems be combined into a holistic picture, which in turn enables appropriate conclusions to be drawn.

Case study: Suspected involvement in the overthrow of a government

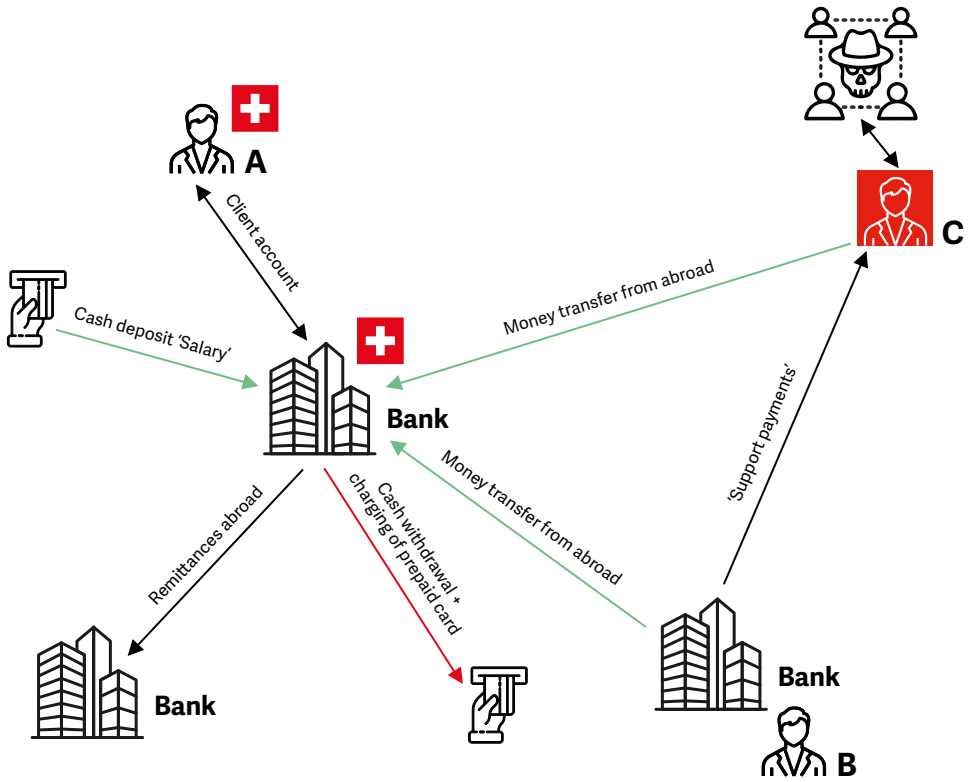
In early 2022, investigations were launched in Switzerland and abroad against various individuals suspected of planning a coup d'état. In the middle of the same year, MROS received its first request for administrative assistance in connection with an investigation abroad. Specifically, it concerned a person (A) residing in Switzerland who, via an intermediary (B), was sending support payments to a recipient (C) outside of Switzerland. This recipient (C) apparently was a high-ranking member of an organisation planning to overthrow a state. Shortly afterwards, MROS received another request from a foreign FIU in the same context, this time focusing on the recipient (C) located abroad and this person's relationship with another individual residing in Switzerland. The information provided by the foreign FIU included reference to a business relationship with a Swiss financial intermediary. MROS then obtained the information concerning the relevant business relationship held at the respective financial intermediary. MROS initiated its own analysis and at the same time requested information from the foreign FIU. For its analysis, MROS needed to know whether any information in connection with money laundering and its predicate offences is known in relation to the foreign senders and recipients or whether criminal proceedings are pending.

For its holistic analysis, MROS collated national and international information as well as SARs and drew the following overall picture: A made an unusually high number of cash deposits in the two and a half years before the first SAR was received. He explained that the cash deposits related to his salary payments, which were made to him in cash. The amounts were either withdrawn in cash shortly after being deposited

[70] The presumption of innocence applies to all of the persons involved.

into the account or were wired directly abroad. MROS categorised these procedures as pass-through transactions. A could not conclusively explain why a stranger had access to his personal account and regularly loaded high amounts to prepaid travel cash cards. In addition, A also received money from other foreign nationals, who (thanks to information obtained through international cooperation) were later identified as the masterminds behind the plot to overthrow the government. MROS also discovered links to the far-right scene in Switzerland and abroad. In January 2023, MROS sent a spontaneous information report to a foreign FIU, which then consolidated the information. MROS also forwarded its analytical report to the competent Swiss prosecution authority (Art. 23 para. 4 AMLA), which initiated criminal proceedings in March 2023 against the defendants residing in Switzerland for involvement in a criminal or terrorist organisation (Art. 260ter SCC).
This example shows that a SAR in and of itself or an information request from abroad often does not provide sufficient substance to identify a possible criminal offence. In this case, it was not a financial intermediary but a foreign FIU that brought the matter to the attention of MROS. Cooperation between MROS and the national and international partner authorities as well as the resulting creation of intelligence were decisive for the transmission of the case to the competent Swiss prosecution authority. Furthermore, this case demonstrates particularly well that information is not always immediately recognisable as relevant when it is sent to MROS. However, when viewed holistically in combination with other information, it can become relevant under criminal law.

Figure 14 – Typology 1: Suspected involvement in the overthrow of a government



5.2 Typology 2 – Use of range of legal instruments

The following case study shows that MROS tends to focus on combating serious crime when analysing SARs. MROS uses the triage matrix to decide how extensively a SAR should be analysed. It then applies all the necessary and legally available instruments to provide the prosecution authorities with as complete an overview of the situation as possible.

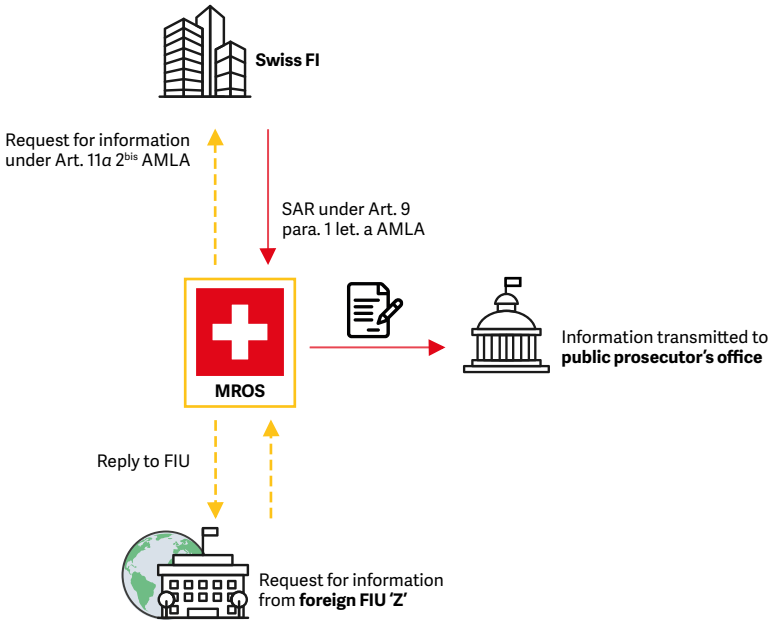
Case study: Human trafficking and forced prostitution

In 2022, MROS received an information request from a foreign FIU regarding a company X based in Switzerland and the transactional activity on its Swiss accounts. It was suspected that incriminated funds for various crimes (including human trafficking and forced prostitution) had been channelled through its Swiss accounts. The foreign FIU had received several SARs with the same modus operandi: a network of natural persons and legal entities based in a region bordering Switzerland would receive funds mainly from natural persons from country Z. These assets would then be transferred to X's accounts in Switzerland. According to the information provided by the foreign FIU, the counterparties in question were, among other things, involved in cases of human trafficking and forced prostitution, whereby these crimes were committed abroad.

Based on the information requests from foreign FIUs, MROS requested information on the Swiss accounts concerned from the relevant Swiss financial intermediaries in accordance with Art. 11*a* para. 2bis AMLA.

Human trafficking and forced prostitution are often difficult to recognise without further indications and only on the basis of the underlying transaction behaviour, as the cash flows and transfers usually involve small amounts. Thanks to the information provided by Swiss financial intermediaries, MROS was able to carry out detailed transaction analysis. The analysis revealed that the same group of natural persons transferred the same amount several times a day to the Swiss accounts in question. Later, further deposits were made by legal entities – with larger amounts and at longer intervals. They replaced the deposits made by natural persons. When the assets were subsequently transferred onwards, it was established, among other things, that payments had been made to migration authorities and to a travel agency based in a country that is considered to be a high-risk jurisdiction for human trafficking and forced prostitution. This information was shared with the foreign FIU. Following MROS's request for information by virtue of Art. 11*a* para. 2bis AMLA, the financial intermediary carried out its own clarifications and then submitted a SAR to MROS under Art. 9 para. 1 let. a AMLA. All information was then forwarded to the competent cantonal public prosecutor's office based on suspicion of human trafficking.

Figure 15 – Typology 2: Human trafficking and forced prostitution

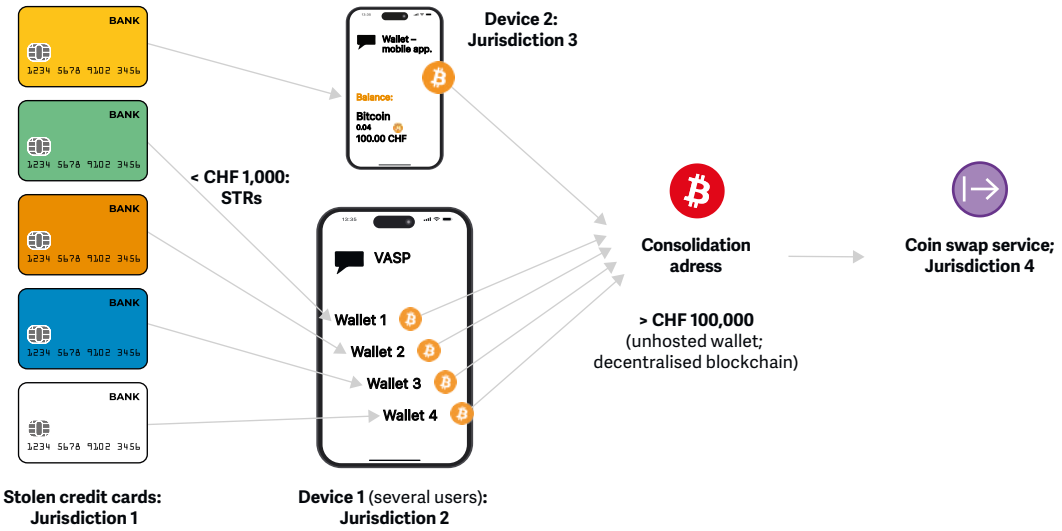


5.3 Typology 3 – Comprehensive analysis

Given the complex, decentralised and cross-border nature of money laundering issues, SARs involving virtual assets and cryptocurrencies can often only be successfully analysed if several cases are considered in a consolidated manner. A holistic analysis procedure is therefore needed to analyse the overall construct (clusters; see Chap. 2.2). The present case shows a constellation where individual cases were analysed and combined into a single consolidated case.
During an analysis conducted by MROS and supported by blockchain intelligence techniques, MROS detected a case of serial crime. The cases analysed (on a consolidated basis) mainly involved information that had not previously been forwarded to a prosecution authority.
After analysis, a number of SARs were identified as involving the same group of suspected perpetrators (cluster). These SARs were submitted by Swiss virtual asset service providers (VASPs) that facilitate the purchase and sale of virtual assets but do not provide custody services to their clients (non-custodial).

The SARs concerned suspected thefts from credit cards issued in a Western European country, which were reported to MROS after the financial intermediary received information from third parties. The victims all reportedly lodged complaints with local police in their countries after discovering that their credit cards had been used to purchase Bitcoin. The SARs all related to different foreign police investigations. However, the total consolidated value of the suspicious transactions reported to MROS was less than CHF 1,000.00 (for this cluster).

Figure 16 – Typology 3: Comprehensive analysis (Cluster)



For each stolen credit card, a new user account was created with the financial intermediary. Because all of these transactions were below a given threshold, the financial intermediary did not collect any identifying information under know-your-customer (KYC). However, computer records (logs) of the transactions (Art. 51*a* AMLO-FINMA) were collected.

When buying bitcoin using a credit card, the financial intermediary will exchange a fiat currency (e. g. euros) for bitcoins. The financial intermediary then transfers ownership of the bitcoins to an address controlled by the customer on the blockchain (distributed ledger technology); for example, to a wallet on an application installed on the customer's smartphone. Only the customer knows the secret code that enables him or her to access these funds. The financial intermediary has no ability to freeze assets, for example.

Each SAR concerned a credit card stolen for a business relationship. MROS is aware of one credit card and one bitcoin address controlled by the contracting party per transaction. Following analysis, MROS was able to determine that at least half a dozen business relationships appeared to have been opened from what seemed to be the same smartphone (same model of cell phone and IP address geolocated in the same Eastern European city). However, another business relationship associated with the target cluster had different characteristics. In this case, the assets on the bitcoin addresses referred to in the SARs were immediately and systematically transferred to the same direct counterparty / bitcoin address (1 hop).

During the analysis, which included the use of various blockchain analysis tools, it quickly became apparent that the beneficiary address in question appeared to be an unhosted wallet used to consolidate funds of criminal origin. This deduction was based on the fact that the funds originated from several hundred different sources and that, after a certain period of time, the funds were systematically transferred in packets to what appeared to be a VASP registered in an offshore jurisdiction. This VASP did not appear to require KYC identification of its users. MROS subsequently discovered that the address had been used to consolidate a total of over CHF 100,000.

When the clarifications were taking place, the blockchain analytics tools used did not reference any cryptographic addresses (clusters) linked to the reporting Swiss financial intermediary in their databases. As a result, it was not possible

to determine whether other suspicious transactions came from the same source. Only a more in-depth blockchain analysis[71], supported by an information request (Art. 11*a* AMLA) made to the financial intermediary, made it possible to identify other potential users who had transferred funds to the so-called consolidation address. It therefore seemed plausible that other clients of the financial intermediary could still be involved in this alleged criminal scheme or that one or more of the alleged perpetrators had created other accounts with the financial intermediary without identifying themselves. Based on the requested information, it was also found that the aggrieved parties appeared to be located in different countries around the world.
In this case, with this fairly typical configuration, MROS notes that the aggrieved parties are domiciled abroad; that the perpetrators appear to be acting as a group from other jurisdictions abroad in schemes through which scams are facilitated or enabled on a larger scale thanks to the Internet (cyber-enabled fraud). The stolen funds are then converted directly into cryptocurrencies through Swiss financial intermediaries, in this case by passing below KYC identification thresholds. Cryptocurrencies of criminal origin are then made directly available to the perpetrators on non-custodial wallets. Suspected criminals or professional money launderers can thus directly transfer the bitcoins to high-risk services in other jurisdictions, in order to convert the profit from their crime. In this case, MROS shared the information at its disposal via the FIU channel.

[71] Identification of transaction patterns

6. MROS practice

6.1 Interpretation of Art. 11*a* AMLA – Disclosure of information by financial intermediaries

Art. 11*a* AMLA authorises MROS to obtain information from financial intermediaries if analysis of SARs submitted under Art. 9 AMLA (duty to report) or Art. 305ter para. 2 SCC (right to report) or information received from foreign FIUs reveals that these financial intermediaries were involved in the matter, either through transactions or business relationships.
The power to obtain information from financial intermediaries under Art. 11*a* AMLA is an important means of effectively combating money laundering, which routinely involves the use of complex schemes that transcend national jurisdictions. On the one hand, it enables SARs from financial intermediaries to be placed in a broader context and, on the other, to provide foreign FIUs with the information needed to combat money laundering.
If MROS receives information requests from foreign FIUs regarding business relationships in Switzerland, it first checks whether there is a connection to Switzerland and thus ensures that no 'fishing expeditions' by foreign authorities is granted (see Art. 31 AMLA). If the client and the respective Swiss financial intermediary are named by the foreign FIU, MROS assumes in practice that there is a sufficient connection to Switzerland, even if no more detailed information on the business relationship (e. g. account numbers) is available. If, on the other hand, the foreign FIU merely assumes the existence of a business relationship in Switzerland without specifying a concrete financial intermediary, MROS will not process the request.
If MROS obtains information regarding certain accounts, it regularly enquires about other accounts within the same business relationship: contracting parties, beneficial owners or associated persons or companies can play a central role. In some cases, MROS is only aware that a client relationship exists between a person or a company and a bank, without having any information on account numbers or transactions. In such cases, MROS requests information from the financial intermediaries about the business relationship in question, indicating the person or company concerned. The swift and complete disclosure of information by financial intermediaries is essential in order to effectively combat money laundering at both national and international level.
Financial intermediaries are required to provide MROS with all relevant information at their disposal. The law does not give financial intermediaries any room for judgement regarding the proportionality of the request or the possibility of contesting or denying it. They must submit the requested information by the deadline[72] set by MROS.
If a financial intermediary fails to comply with MROS's requests, this behaviour may constitute a breach of supervisory legislation. According to Art. 10 para. 2 MROSO, MROS is authorised to contact the competent supervisory authorities,

[72] Art. 11*a* para. 3 AMLA.

supervisory or self-regulatory organisations within the meaning of Art. 29 para. 1 or Art. 29*b* AMLA to report any breaches of supervisory legislation by financial intermediaries – which MROS does on a regular basis. It is the responsibility of the supervisory authorities to investigate alleged breaches of supervisory legislation and, if necessary, to take appropriate measures.

6.2 Interpretation of Art. 29*a* AMLA – prosecution authorities required to notify MROS of judgments and rulings

Art. 29*a* para. 1 AMLA requires all prosecution authorities[73] to notify MROS of judgments and ruling abandoning proceedings regarding proceedings connected with Art. 260ter, Art. 260^{quinquies} para. 1, Art. 305bis and Art. 305ter para. 1 SCC, and include the grounds for these outcomes. These judgments or ruling abandoning proceedings allow MROS to gain an overview of developments in connection with money laundering and its predicate offences, organised crime and terrorist financing and help MROS to raise awareness of these issues among financial intermediaries. In addition, under Art. 29*a* para. 2 AMLA, prosecution authorities must also notify MROS of any rulings that they have issued on the basis of a case that they have received from MROS. The list of these judgements and rulings include in particular the following:

- Opening the investigation (Art. 309 para. 3 CrimPC);
- No-proceedings order (Art. 310 para. 1 CrimPC);
- Ruling to extend the investigation (Art. 311 para. 2 CrimPC);
- Suspension of investigations (Art. 314 CrimPC);
- Resumption of proceedings (Art. 315 CrimPC);
- Summary penalty order (Art. 353 CrimPC);
- Ruling abandoning proceedings (Art. 320 CrimPC);
- Reopening of proceedings (Art. 323 CrimPC);
- Court judgment (e.g. under Art. 351 CrimPC or under Art. 408 CrimPC).

These notifications not only allow MROS to monitor the progress of proceedings, but also make it possible to quickly transmit information from any other SARs relating to the same case to the competent authority. The information is also needed to maintain relevant statistics. Finally, the notifications provide MROS with feedback on its work, in particular with regard to its transmission practices to the prosecution authorities. The obligation referred to in Art. 29*a* AMLA also includes the spontaneous transmission of information within the meaning of Art. 67*a* of the Mutual Assistance Act.[74] The purpose of this information is to trigger a specific request for mutual legal assistance to Switzerland.
In its evaluation report dated 20 December 2021[75], the SFAO criticised the fact that MROS lacks complete data on the decisions of the prosecution authorities in cases involving money laundering, especially if these cases are linked to a SAR (reference made to Art. 29*a* para. 1 and 2 AMLA). In its report, the SFAO points out that feedback from the cantonal prosecution authorities is incomplete or unsatisfactory: *'MROS lacks an overview of the entire process chain and the life cycle of its SARs. However, this would be crucial in assessing the effectiveness and improvement of its own work. MROS has been complaining for 20 years that the OAG, the cantonal public prosecutors' offices and the sentencing courts are not fulfilling their legal obligation under Art. 29a AMLA. Similar to the systematic comparison of reports practised with the OAG since 2020, the cantonal public prosecutor's offices and the sentencing courts should also comply with the legal requirement.'*

---

[73] The term 'prosecution authorities' includes both cantonal prosecution authorities and the Office of the Attorney General of Switzerland as well as all courts of all instances (Federal Council Dispatch on Implementation of the Revised Recommendations of the Financial Action Task Force [FATF], BBl 2007 6269, 6302).

[74] Federal Act of 20 March 1981 on International Mutual Assistance in Criminal Matters (Mutual Assistance Act, IMAC, SR 351.1).

[75] *SFAO evaluation report on MROS fulfilment of its mandate, 20 December 2021, p. 33 (published in German on 28 March 2022).*

MROS took the SFAO's criticism as an opportunity to remind prosecution authorities of their duty in this regard during the reporting year. The statistics presented in Chapter 4.8 show that there is still room for improvement. In order for MROS to effectively analyse the information based on Art. 29*a* AMLA and bring the added value needed to tackle and prevent crime, the feedback rate must be as complete as possible.

7. International cooperation in the fight against money laundering

7.1 Egmont Group

Switzerland has been a member of the Egmont Group since 1998. This is an international network of 173 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 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 a prerequisite for an adequate AML/CFT system.

The objectives of the Egmont Group are in particular to:
- create the conditions necessary for an international, systematic exchange of information;
- help FIUs improve 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. HoFIUs are supported by the Egmont Committee, a consultation and coordination mechanism, and the Egmont Group Secretariat, based in Canada.

The Egmont Group 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 Principles are adhered to by both new 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 – existing members and candidate FIUs – 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 and Regional Group Meetings) are held throughout the year in which MROS takes part. At regional group meetings, FIUs are assigned to a group based on geographical considerations. European FIUs are divided into two groups: the 'Europe I' regional group is comprised of FIUs from EU member states, whereas the remaining FIUs in Europe, including MROS, are assigned to the 'Europe II' regional group.[76] Regional groups enable discussion of region-specific challenges and issues.

Meeting with Egmont members

A Working and Regional Group Meeting was held in Dakar, Senegal, from 30 January to 3 February 2023. 287 delegates and 12 observers as well as international partners attended this meeting. A total of 15 meetings were held to strengthen the capacities of Egmont Group members, improve information exchange between them and work towards the fulfilment of the development mission, cooperation and the exchange of expertise. The Egmont Group Plenary was held in Abu Dhabi, United Arab Emirates, between 3 and 7 July 2023. It was attended by 533 delegates, 12 observers and one international partner. A major milestone was the decision to switch to a new IT infrastructure, the Egmont Secure Web. IT infrastructure was a key area of concern discussed at the plenary meeting: the sharp increase in SARs and information requests from foreign FIUs can no longer be handled with manpower alone. FIUs need new IT solutions to improve their efficiency.

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 as well as terrorism and proliferation financing. The members are the respective countries, not individual offices. The FATF investigates how money is laundered and terrorism is financed. It promotes global standards[77] to mitigate the risks and assesses whether countries are taking effective measures. In 2023, three plenary meetings were chaired by Singapore at the headquarters of the Organisation for Economic Co-operation and Development (OECD) in Paris.[78]

The FATF published a number of reports in 2023, including the 'Misuse of Citizenship and Residency by Investment Programmes'[79], 'Best Practices on Combating the Abuse of Non-Profit Organisations'[80], 'Illicit Financial Flows from Cyber-enabled Fraud'[81] and 'Crowdfunding for Terrorism Financing'[82]. The latter in particular became particularly relevant in the wake of terrorist attacks by Hamas on Israel on 7 October 2023. In this context, MROS sent an alert and typologies to Swiss financial intermediaries on 3 November 2023; on 5 December 2023, it supplemented the alert with an addendum.[83]

Country evaluation

The FATF's standards on measures to combat money laundering and terrorist financing are intended for member states, which are required to implement them. The FATF periodically assesses the current status of implementation in

[76] Other members of the Egmont II Regional Group include for example: Financial Crimes Investigation Board (MASAK), Turkey; The State Financial Monitoring Service of Ukraine (SFMS), Ukraine, and the UK Financial Intelligence Unit (UKFIU), United Kingdom.

[77] *The FATF-Recommendations 2012 – Updated November 2023*.

[78] The decision to suspend Russia's membership at the first meeting in February 2023 is noteworthy in this respect: *FATF Statement on the Russian Federation (fatf-gafi.org).*

[79] *Misuse of Citizenship and Residency by Investment Programmes (fatf-gafi.org).*

[80] *Best Practices on Combating the Abuse of Non-Profit Organisations (fatf-gafi.org).*

[81] *Illicit Financial Flows from Cyber-enabled Fraud (fatf-gafi.org).*

[82] *Crowdfunding for Terrorism Financing (fatf-gafi.org).*

[83] The MROS Alert combined FATF publications, information from foreign FIUs and MROS's own findings.

the individual member states and publishes the results of its evaluations in a report. While FATF recommendations are not legally binding, they are crucial for Switzerland. Member states that fall short of the FATF recommendations are publicly called out and placed on a list of high-risk jurisdictions (grey and black list), which generally has serious consequences for the countries concerned. Transactions from or to the listed country are scrutinised by the authorities and are therefore more cumbersome and expensive. Foreign investors also hold back accordingly, as the risk seems too great. As a result, the reputation of a country's entire financial centre suffers. Switzerland was last subject to a country evaluation in 2016 during the fourth evaluation round and received positive feedback. However, the FATF identified certain shortcomings in the AML/CFT system, which is why Switzerland was included in the so-called 'Enhanced Follow-up Process'. In order to comply with the FATF recommendations, Switzerland has consistently implemented various measures to improve technical compliance, in particular with the revision of the Anti-Money Laundering Act in July 2021.[84] The FATF has now recognised this progress and released Switzerland from the 'Enhanced Follow-up Process' in October 2023.

The next country evaluation is expected to take place in 2027/2028. The FATF will conduct a new and comprehensive assessment of Switzerland's AML/CFT system based on new evaluation methodology (compared to the 2016 evaluation). In addition to technical compliance with the FATF standards, the review will also focus on the effectiveness of the AML/CFT mechanism. Not only the authorities, but the entire Swiss financial centre, including the private sector, will be included in the assessment. The FATF will seek to determine whether a country is fully aware of the risks that it is exposed to and whether it has introduced measures to mitigate and prevent these risks.

The new methodology comprises two interlinked components:

- The **technical** assessment of compliance addresses the specific requirements of the individual FATF Recommendations. This primarily concerns the legal and institutional framework of a country as well as the powers and procedures of competent authorities. These are the basic building blocks of an effective system to combat money laundering and financing of terrorism and proliferation.[85]
- The **effectiveness** assesses whether a country ensures a robust AML/CFT system. The extent to which a country's legal and institutional framework influences the expected results is also analysed.[86]

The country evaluation takes around 18 months and can be divided into three phases for Switzerland: preparation for the on-site visit (from 2024), the on-site visit itself (approx. July 2027) and preparation for the FATF plenary meeting at which the report on Switzerland is adopted.

---

[84] In particular, introduction of MROS's new powers in obtaining information under Art. 11*a* para. 2[bis] AMLA.

[85] There are four possible levels of compliance with individual recommendations: compliant, largely compliant, partially compliant or non-compliant.

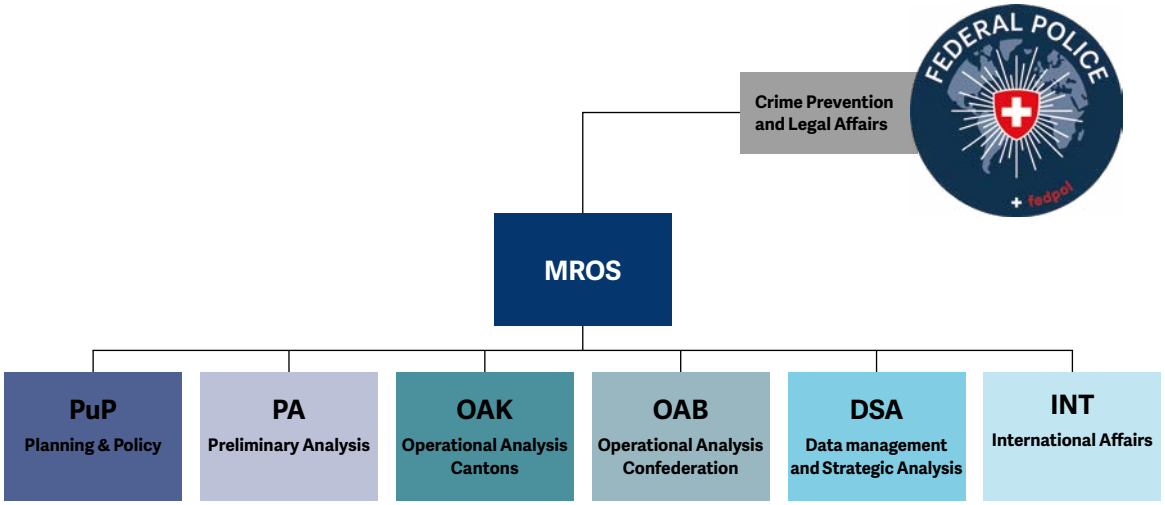
[86] Effectiveness ratings are as follows: high level of effectiveness, substantial level of effectiveness, moderate level of effectiveness and low level of effectiveness.

8. MROS organisational structure

MROS is part of fedpol's Crime Prevention & Legal Affairs Directorate. In its core operational tasks, MROS acts completely independently and thus fulfils international requirements.

In 2020, MROS was reorganised and subdivided into six divisions (see organisation chart; Figure 17). As of 2023, it had an average of 59 occupied positions corresponding to a total of 50.3 full-time equivalents (FTEs).

Figure 17 – MROS organisational structure



Planning and Policy (PuP)
The PuP division is a classic cross-sectional unit and thus deals with complex issues. The focus is on ML/TF-related legal issues, the processing and monitoring of political projects and publications (e. g. annual reports, legislative revisions, legal opinions on MROS-specific topics) as well as support for the operational divisions of MROS. The PuP division maintains regular dialogue with internal and external stakeholders and handles MROS administrative matters.

Preliminary Analysis (PA)
The PA division 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. The PA division also triages cases and transfers them to one of the operational divisions on the basis of an overall assessment. In addition, it is responsible for national administrative assistance under Article 29 AMLA.

Operational Analysis Cantons (OAK)
The OAK division analyses incoming SARs, most of which fall under the jurisdiction of the cantonal prosecution authorities and have been assigned by the PA division. 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 OAB division analyses incoming SARs which a priori fall within the competence of the Office of the Attorney General of Switzerland, i. e. the OAG, and have been assigned by the PA division. 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 DSA division is responsible for the secure operation and the development of the MROS information system (goAML). In doing so, it also provides technical support to financial intermediaries, especially in programming their interfaces. The DSA division is also responsible for developing the technical possibilities for processing SARs. The division 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 INT division deals with all (information) exchanges with foreign FIUs as well as membership and participation in international bodies (including the Egmont Group, FATF, United Nations Convention against Corruption and the Europol Financial Intelligence Public Private Partnership).