

Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra

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

Money Laundering Reporting Office Switzerland (MROS)

Annual Report 2024



Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra

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

Money Laundering Reporting Office Switzerland (MROS)

Annual Report 2024

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

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

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

Table of contents

| 1 | Foreword | 6 |
|-------|---|----|
| 2 | Main strategic developments | 8 |
| 2.1 | MROS priorities and objectives for the 2024 – 27 period | |
| 2.2 | National Risk Assessment (NRA) – Sectoral report on proliferation financing | |
| 2.3 | Swiss Financial Intelligence Public-Private Partnership (Swiss FIPPP) | |
| 2.4 | Financial Intelligence Unit (FIU) 2.0 | |
| 2.5 | MROS projects and events | |
| 2.5.1 | Financial Intelligence against Human Trafficking (FIAHT) | |
| 2.5.2 | Typology Report | |
| 2.5.3 | MROS Crypto Symposium 2.0 | |
| 2.5.4 | Round table on the Chinese underground banking system | 12 |
| 3 | MROS annual statistics | |
| 3.1 | General overview for 2024 | |
| 3.2 | Suspicious Activity Reports (SARs) | |
| 3.3 | Number of SARs by financial intermediary category | |
| 3.4 | Legal basis for SARs | |
| 3.5 | Predicate offences | |
| 3.6 | Factors arousing suspicion | |
| 3.7 | MROS cases forwarded to prosecution authorities | |
| 3.8 | Feedback from prosecution authorities | |
| 3.9 | Terrorist financing | |
| 3.10 | Organised crime | |
| 3.11 | SARs involving the use of cryptocurrencies | |
| 3.12 | Requests for information under Art. 11a AMLA | |
| 3.13 | Terminated business relationship notification under Art. 9b AMLA | 24 |
| 3.14 | Information-sharing with foreign financial intelligence units (FIUs) | 24 |
| 3.15 | Information-sharing with Swiss authorities | 24 |
| 4 | Trends | |
| 4.1 | Online gambling | |
| 4.2 | Child pornography and virtual assets | 29 |
| 4.3 | Proscription of Hamas | |
| 5 | From the MROS Practice | |
| 5.1 | Immediate reporting vs depth of clarification – MROS position | |
| 5.2 | Interpretation of Art. 11a AMLA – Reasons for requests for information | |
| 5.3 | Duty to report vs right to report | |
| 5.4 | Definition of the term 'prosecution authority' | |
| 6 | International cooperation in the fight against money laundering | |
| 6.1 | Egmont Group | |
| 6.2 | GAFI / FATF | |
| 6.2.1 | General information | |
| 6.2.2 | Country evaluation | |
| 6.3 | Taskforces | |
| 6.4 | Bilateral meetings | 38 |
| 7 | MROS organisational structure | |

1 Foreword

Record figures were reported again in 2024 in almost all reporting categories. MROS¹ registered a total of 27,901 incoming reports in its goAML² information system, an increase of nearly 30% over the previous reporting period. Since the introduction of goAML, the volume of incoming data has more than tripled. On average, MROS receives 107 incoming reports per working day. These include suspicious activity reports (SARs), replies by financial intermediaries to MROS information requests³, terminated business relationship notifications⁴, information requests from foreign financial intelligence units (FIUs), spontaneous information reports, enquiries and responses from national and international authorities, and judgements of the prosecution authorities.5

In 2024, financial intermediaries sent MROS a total of 15,141 suspicious activity reports (hereinafter referred to as SARs). This represents an increase of 27.5% compared with the previous year (2023: 11,876). On average, MROS received 59 SARs per working day, which corresponds to roughly 55% of daily incoming reports. This figure has been declining steadily in recent years: 10 years ago, SARs accounted for more than 90% of total reporting volume. This development is due to the fact that administrative assistance between MROS and national authorities, as well as international partners, has increased significantly. It clearly shows that authorities are increasingly working together and conducting clarifications with external agencies. This is also true for MROS. Financial intelligence relies on the active exchange of information and interaction with the various stakeholders. In order to process large volumes of data efficiently, reporting must be structured and formalised, and its content must meet certain minimum quality standards. MROS continues to observe differences in the quality of SARs. The reason for this is likely to be cost pressure, but there is probably also tension between the need to report suspicions 'immediately' and the need to 'thoroughly clarify' these suspicions beforehand (see 5.1).

In the year under review, MROS referred a total of 1,043 cases to the prosecution authorities. This is an increase of more than 20% compared with the previous year. When MROS forwards a case to the prosecution authorities, it provides them with an analysis of the relevant information. The analysis is based on information from different SARs sent to MROS (not necessarily in the same year) and information from domestic or foreign authorities. In 2024, the cases referred to the prosecution authorities involved on average 1.9 SARs per case, a figure that has increased in recent years (2021: 1.3; 2022: 1.4; 2023: 1.8). Approximately one in five cases sent to the prosecution authorities in 2024 also contained information obtained by MROS under Art. 11a AMLA6 through requests for information to reporting financial intermediaries or third-party intermediaries. MROS also made increased use of spontaneous information reports (Art. 29 AMLA), sending 358 spontaneous information reports to national authorities, which is an increase of 79% over the previous year. MROS provides its information in a targeted manner and involves the receiving authorities in the transmission process at an early stage.

The number of cases forwarded to the prosecution authorities says little about the efficiency and effectiveness of MROS's analyses. For one thing, the total output must be taken into account, i. e. the number of analyses that lead to a case being forwarded to the prosecution authorities or yield spontaneous information reports. Equally important is throughput, i. e. how much information is actually processed during analysis. Last year, MROS made improvements in both areas.

MROS has formulated its strategic objectives and priorities for the 2024 – 27 period based on its legal mandate, focusing on three areas: intelligence, cooperation and prevention (see 2.1). In addition to defining these priorities and objectives, MROS is also reflecting on future challenges for an FIU and considering what skills and tools will be needed to meet

¹ Money Laundering Reporting Office Switzerland

² government office Anti Money Laundering

³ MROS requests based on Art. 11a AMLA

⁴ Based on Art. 9b AMLA

⁵ Based on Art. 29a AMLA

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

them. These challenges will be defined in a study that is expected to be completed in 2025 (see 2.4).

On 7 November 2024, the Swiss Financial Intelligence Public-Private Partnership (Swiss FIPPP), consisting of 12 financial institutions and MROS, officially became operational. This means that the Swiss financial centre now has a public-private partnership and is thus catching up with other international financial centres (see 2.3). At the end of October 2024, MROS held a second Crypto Symposium aimed at the financial sector active in the field of cryptocurrencies and virtual assets. The response was very positive. The exchange between the authorities and the industry is particularly important in this still young financial segment. MROS will therefore hold the event in the same format again in 2025 (see 2.5.3). In this annual report, the 'typologies' section is omitted and reference is made to a typology report on the MROS homepage (see 2.5.2). This enables MROS to provide the financial sector with up-to-date case studies throughout the year.

2 Main strategic developments

2.1 MROS priorities and objectives for the 2024 – 27 period

MROS is the national reporting office for suspicious financial activities or transactions in connection with money laundering and terrorist financing in Switzerland and performs the tasks of a Financial Intelligence Unit (FIU). Its mandate, as defined by law, covers three core areas:

- Intelligence: MROS receives SARs submitted by financial intermediaries and traders based on the Anti-Money Laundering Act or the Swiss Criminal Code.⁷ It conducts its own analyses and supplements the SARs with additional information. It then decides on a case-by-case basis whether or not to forward it to a prosecution authority.
- Cooperation: MROS exchanges information on operational and strategic matters with other national authorities and foreign FIUs through administrative assistance.
- Prevention: MROS contributes to the assessment of the national risks of money laundering and terrorist financing. It compiles strategic analyses and shares its findings with other authorities, the financial sector and the public.

These three core tasks should not be considered in isolation, but form a single unit: intelligence forms the foundation of cooperation and prevention.

MROS has reformulated its strategic goals for the 2024 – 27 period, which are derived from its legal mandate.⁸ They show how MROS fulfils its legal mandate, what its priorities are and how it uses its scope for action. These goals, which are periodically reviewed, are a response to developments in the fight against money laundering and crime and the associated challenges. They form a link between the legal mandate and the specific activities of MROS.

The new MROS strategy defines six objectives and thirteen measures. It sets clear priorities on serious crime and offers added value in the fight against crime for its direct partners - national authorities, foreign FIUs and the financial sector - with its analyses. The steadily increasing number of incoming reports and its limited resources force MROS to act on a risk-based approach.9 In addition to focusing on certain areas of crime, MROS is working to streamline reporting and processing, and further develop its IT infrastructure, because cutting-edge analytical tools are key to processing large volumes of data efficiently and producing useful analyses. Pro-active and targeted cooperation with stakeholders - the private and financial sector, national authorities, international partners - is also crucial. Financial crime is a global phenomenon requiring concerted global action. The parties need to sit at the same table and tackle the issues together.

2.2 National Risk Assessment (NRA) – Sectoral report on proliferation financing

Assessing the risks posed by money laundering and terrorist financing is an important part of Switzerland's overall counter-crime strategy. Switzerland has already published two comprehensive national risk assessments (2015¹⁰ and 2021¹¹), commissioned by the Interdepartmental Coordinating Group on Combating Money Laundering and Terrorist Financing (CGMF). MROS is a member of this group and heads the Risk Analysis sub-group. The CGMF compiles regular risk assessment reports, which are updated on a regular basis.

In addition to cross-sector risk assessments, the CGMF regularly publishes sectoral risk analyses. On 17 September 2024, it approved the National Risk Assessment on Proliferation Financing Report, which MROS compiled in cooperation with the State Secretariat for Economic Affairs (SECO).¹²

⁷ Swiss Criminal Code, SR 311.0

⁸ See MROS 2024 – 27 Strategy, available here: <u>https://www.fedpol.admin.ch/dam/fedpol/en/data/kriminalitaet/geldwaescherei/</u> strategie-mros.pdf.download.pdf/strategie-mros-e.pdf

⁹ For information on risk-based approach, see MROS Annual Report 2023, Chapter 2.2

¹⁰ First national report on money laundering and terrorist financing risks, June 2015

¹¹ Second national report on money laundering and terrorist financing risks, October 2021

¹² Federal Council press release of 9 December 2024, Report on the risks of proliferation financing

The proliferation of weapons of mass destruction and their delivery systems poses a threat to international peace and security. Preventing its financing is based on a complex national and international legal framework. The report outlines the global risk landscape and the specific proliferation financing risks, with a focus on Iran and North Korea.

The risk analysis for Switzerland produced the following findings:

- Proliferation financing risks are the highest in commodities trading, cryptocurrency trading and correspondent banking. Furthermore, there is an overarching risk of circumvention through front companies.
- Iran poses trade-related risks because, unlike North Korea, it is not excluded from the value chain. North Korea, on the other hand, poses a higher risk in the area of cybercrime and the associated use of cryptocurrencies.

The report recommends that the strategy to combat proliferation financing be further strengthened by expanding the CGMF's mandate to include proliferation financing and by establishing an interdepartmental working group on this topic. In addition, the data basis should be improved and awareness should be raised in the private sector.

2.3 Swiss Financial Intelligence Public-Private Partnership (Swiss FIPPP)

Information sharing between public authorities and the private sector enhances the effectiveness of anti-money laundering efforts. These bodies should therefore cooperate and exchange information on threats, risks, methods and trends in the area of

money laundering and terrorist financing. To this end, several financial intelligence public-private partnerships have been established at international level over the last decade.

This development prompted Switzerland to launch its own public-private partnership on money laundering and terrorist financing. On 7 November 2024, the Swiss Financial Intelligence Public-Private Partnership (Swiss FIPPP) commenced its activities in a constituent plenary session.13 The official launch of the Swiss FIPPP was preceded by approximately two years of preparatory work. The scope for public-private cooperation in Switzerland was analysed.¹⁴ This strategic partnership between MROS and the Swiss financial sector focuses on the exchange of strategic information, for the purpose of identifying threats and risks as well as jointly and sustainably strengthening the defence mechanism. Tactical cooperation, in which information is exchanged on specific cases and individuals, is not currently planned and would require legal adjustments. The Swiss FIPPP consists of MROS and, initially, 12 financial institutions: Bank Julius Bär & Co AG, Bank Vontobel AG, Banque Lombard Odier & Cie SA, Bitcoin Suisse AG, Deutsche Bank (Switzerland) AG, HSBC Private Bank (Switzerland) SA, Raiffeisen Schweiz Genossenschaft, Societe Generale Corporate & Investment Banking, UBS AG, Valiant Bank AG, Zürcher Kantonalbank and Zürich Versicherungs-Gesellschaft AG. Membership may be subject to change.

The Swiss FIPPP plans to hold a plenary session at least twice a year. In addition, topic-specific working groups will meet regularly. The activities of the Swiss FIPPP will be coordinated by an executive board,



Figure 1: Swiss FIPPP logo.

¹³ Swiss Financial Intelligence Public–Private Partnership (Swiss FIPPP), last reviewed on 31 January 2025.

¹⁴ MROS report: <u>Public-Private Partnership (PPP)</u>: <u>Strengthening the AML/CET Framework through Information Sharing</u>, March 2023.

whose members are elected by the plenary assembly. MROS is responsible for organisational matters and communication. The Swiss FIPPP will report on its activities and findings in an annual report and provide targeted information on an ad-hoc basis.

2.4 Financial Intelligence Unit (FIU) 2.0

In 1998, its founding year, MROS had four employees and received 173 SARs. Twenty-six years later, its headcount has increased to around 55 employees and the number of SARs has reached 15,000. In its 2023 annual report, MROS explained the regulatory and operational reasons for this remarkable increase in reporting volume.15 But what do such developments mean for an FIU? What does an FIU require in order to continue to fulfil its legal mandate and carry out the associated tasks in the future?

Money laundering is the key driver of organised crime and has become much more complex in recent years. The expansion of international networks and the use of new money laundering techniques and modern technologies (e.g. virtual assets) means that the fight against money laundering and terrorist financing has become increasingly complex. While MROS's activities used to comprise largely of receiving and forwarding SARs, the focus has clearly shifted in recent years towards gathering intelligence: the linking of information, providing law enforcement agencies with in-depth analyses and working collaboratively with national authorities, foreign FIUs and the financial sector are at the forefront today. These activities are essential for combating money laundering and terrorist financing effectively. However, these tasks require FIUs to further develop in key areas, such as IT infrastructure and human resources, so that they can keep pace with global policy developments and the increasing scope of tasks and requirements.

IT infrastructure

For their work, FIUs need software solutions that meet the requirements of an FIU and global developments within the legal framework (in particular data protection regulations). The ability to collect and analyse large amounts of data from multiple sources, including open source intelligence (OSI- tools for authorities and the private sector and rais-

NT), is becoming ever more important. FIUs need to be able to interpret information from financial transactions and databases, as well as from open sources. Artificial intelligence and machine learning play a critical role in helping to identify suspicious activities at an early stage. New technologies offer FIUs the opportunity to improve their effectiveness and deepen their understanding of the threats from money laundering and terrorist financing.

Human resources planning

The complexity of the information to be analysed, the legal issues and the use of specialised tools require strategic human resources planning by FIUs. It is therefore crucial to recruit specialists and retain qualified staff. FIUs must offer attractive working conditions and have the necessary funding in order to attract and retain talent over time. They also need flexibility to plan and deploy resources in a targeted way.

The rapid pace of technological progress, which is providing money laundering and terrorist financing with ever more possibilities, poses enormous challenges for FIUs worldwide (not only for Switzerland). As a Federal Administration body, MROS is caught between the ever-increasing volume of reports and data, limited resources, budget restrictions and the existing legal framework. Despite these constraints, MROS has a legal mandate to fulfil and therefore requires the necessary instruments. The above-mentioned limitations should not be allowed to completely contradict the necessity of these instruments. A consideration aimed at the effectiveness of an FIU is necessary.

In light of this, MROS will present a study on the topic 'FIU 2.0' in 2025, which will address the above-mentioned challenges and offer appropriate solutions. The study will also include a benchmarking analysis showing where Switzerland stands in international comparison.

2.5 MROS projects and events

In 2024, MROS launched the following projects and events. These have the aim of providing useful

¹⁵ See <u>MROS Annual Report 2023</u>, Chapter 2.1.

ing their awareness. All of them provide important trends and indicators to combat money laundering and terrorist financing more comprehensively.

2.5.1 Financial Intelligence against Human Trafficking (FIAHT)

Human trafficking is one of the most lucrative forms of organised crime. It is a hidden, transnational crime. The International Labour Organization estimates that this crime, whose sole objective is financial gain through human exploitation, generates USD 236 billion in annual profits worldwide. The indepth analysis of payment flows and account transactions, the so-called 'follow the money' strategy, as practised by MROS, makes a significant contribution to uncovering illegal activities related to human trafficking and to identifying its victims.

Background

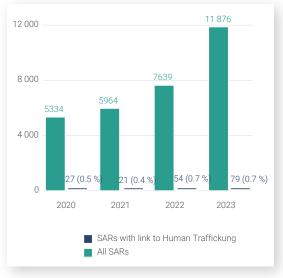
Under Swiss legislation, human trafficking is a predicate offence to money laundering. Financial • intermediaries must therefore report suspicious activities related to human trafficking and other offences to MROS. In Switzerland, as in many other European countries, the number of SARs linked to human trafficking is extraordinarily low: there is a N huge discrepancy between the extent of criminal tractivity and the number of SARs filed.

Project FIAHT

With the support of the Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings of the Organisation for Security and Cooperation in Europe (OSCE), MROS launched the Financial Intelligence Against Human Trafficking project.

The aims of this project were as follows:

 creation of a guide to raise awareness among financial intermediaries;



11

Figure 3: Human-trafficking related SARs in relation to overall reporting volume; 2020 – 2023.

 strengthen cooperation and optimise operational procedures between MROS and other relevant actors by developing a multi-stakeholder partnership.

MROS took on the management of the project at the official launch, which took place in the form of a round table on 24 January 2024. In cooperation with various law enforcement and federal authorities, as well as representatives from the financial sector and a victim protection organisation, data and information were collected for the FIAHT guide. This set the scene for a greater exchange between stakeholders, which was also a key focus. The final event of the FIAHT project took place on 25 November in Bern, where the FIAHT guide was presented.

FIAHT Guide¹⁶

The guide provides clear approaches and tools to help financial intermediaries and traders identi-



Figure 2: Financial Intelligence Against Human Trafficking (FIAHT) project logo

¹⁶ Information published in MROS report: <u>Financial Intelligence against Human Trafficking</u>.

fy transactions and activities linked with serious MROS intends to publish the first typologies on its crime. These include: website in May 2025.¹⁸ The collection will be contin-

- **Indicators** that point to human trafficking and related crimes.
- **Practical examples** of how perpetrators hide their profits and how financial intermediaries can identify such patterns.
- **Best practices** in submitting SARs efficiently and accurately in order to support analysis and investigations.

Such guidelines are crucial in the fight against money laundering, its predicate offences and organised crime in order to reduce the discrepancy between the number of SARs submitted and the financial relevance of these crimes.

2.5.2 Typology Report

MROS's prevention mandate includes raising the awareness of money laundering, its predicate offences, organised crime and terrorist financing among financial intermediaries and traders. In addition to regular publications such as the annual report and national risk analyses, MROS publishes newsletters and compiles topic-related guidelines (e. g. the HAMAS Alert or the FIAHT Guide; see 2.5.1). These publications serve as orientation, guidelines and best practices for financial intermediaries.

A further awareness-raising tool is MROS's new typology report¹⁷. Money laundering typologies are based on a systematic classification and analysis of typical methods and practices used by criminals to introduce illegal funds into the legal economy. These modi operandi include a variety of techniques that enable perpetrators to conceal the origin of the money and prevent confiscation. The typology report helps financial intermediaries to identify possible indicators. MROS uses anonymised and simplified case studies which enable a clear analysis of complex relationships, promote a more nuanced approach and provide a useful structure for identifying recurring patterns.

MROS intends to publish the first typologies on its website in May 2025.¹⁸ The collection will be continuously updated and is primarily intended for financial intermediaries and traders. It will be published initially in English.

2.5.3 MROS Crypto Symposium 2.0

As in the previous year, MROS organised a Crypto Symposium at the end of October 2024. The first symposium in 2023 focused on the challenges of tracing cryptocurrencies and detecting crimes involving cryptocurrencies. In 2024, the focus was on the specific risks and opportunities in the misuse of cryptocurrencies. Around 270 participants from the financial, consulting and public sectors attended. Speakers included representatives from national and international authorities and the private sector.

The topics discussed included various criminal activities in which cryptocurrencies are misused. These range from cybercrime, the circumvention of sanctions, asset recovery and gambling to fraud and unlawful use by private security companies. In addition to providing a classification of virtual assets in the context of the upcoming FATF country evaluation, several authorities shared their experiences in dealing with digital crime and reported on the fight against investment fraud. The misuse of cryptocurrencies to fund wars and mercenaries was also discussed. It was noted that calls for donations to fund military activities are being organised on platforms such as Telegram, posing new challenges for law enforcement.

In summary, there is a need for increased national and international cooperation and the targeted use of technological tools to combat growing cryptocrime.¹⁹

2.5.4 Round table on the Chinese underground banking system

'Hawala' in the Middle East and Africa, 'Hundi' in South Asia, 'Fei Ch'ein' and 'Daigou' in China: the system of underground banking has existed as long as there has been cross-border trade. These systems operate outside the conventional banking

¹⁷ Will be transferred to a database at a later date.

¹⁸ Further information: <u>Publications of the Money Laundering Reporting Office (MROS)</u>.

¹⁹ Fedpol press release of 29 October 2024, <u>MROS Crypto-Symposium 2.0: Gemeinsam gegen den Missbrauch von Kryptowährungen</u>

system, without state authorisation or supervision. Documents, account details and bank accounts do not exist. Transactions are quick, cheap and anonymous. This is what makes the system so attractive for concealing and moving criminal assets and terrorist funds. Despite their furtive nature, law enforcement authorities continue to uncover such systems and identify their money flows. Exchanging information, analyses and best practices on successful law enforcement operations is essential. MROS therefore organised the first Swiss-wide round table on the Chinese underground banking system. The event was aimed primarily at Swiss and international law enforcement authorities and FIUs that are actively involved in the fight against organised crime. The roundtable was attended by fedpol, Europol and prosecuting authorities as well as FIUs from several European countries.²⁰

²⁰ Fedpol press release of 31 October 2024, <u>Erster Runder Tisch zur Bekämpfung von Untergrundbanken.</u>

MROS annual statistics 3

MROS produces anonymised statistics on money submitted by financial intermediaries, requests for laundering and its predicate offences, organised information from foreign authorities and criminal crime and terrorist financing during the reporting proceedings as a result of the SARs (see Art. 23 year.²¹ The statistics include, in particular, SARs para. 1 MROSO²²).

3.1 **General overview for 2024**

- Reporting volume increased again significantly in 2024: MROS received a total of 15,141 SARs, that is approximately 59 SARs per working day. This is an increase of 27.5% compared with 2023 (11,876 SARs). Since the introduction of the goAML information system in January 2020, reporting volume has almost tripled.
- 92.3% of the SARs came from financial intermediaries in the banking sector (average for 2015 24: 90.1%).
- The number of Art. 11a AMLA information requests to financial intermediaries comprised 1,016 in 2024.
- MROS referred 20.4% more cases to the prosecution authorities than in the previous year.²³ These may contain information from several SARs, which have not necessarily been received by MROS in the same year, and information from various domestic and foreign authorities. On average, MROS referred 1.9 SARs per case to the prosecution authorities: here, too, the average number of SARs per case has risen steadily.²⁴ Approximately one in five forwarded cases (18.9%) also contained information from one or more MROS requests to reporting or third-party financial intermediaries under Art. 11a AMLA.
- The volume of information exchanged between MROS and the Swiss authorities also increased. In comparison with the previous year, spontaneous information reports from MROS to other Swiss authorities increased by 79%. On the other hand, the volume of information requests (447, -35.8% compared to the previous year) and spontaneous information reports (106, -10.9%) from Swiss authorities to MROS declined.
- The exchange of information with foreign FIUs is also increasing. In 2024, MROS received 780 requests from 96 FIUs and 751 spontaneous information reports from 45 countries.

¹⁴ MROS Annual Report 2024 3 MROS annual statistics

²¹ Reporting year: 1 January to 31 December of the given year.

²² Ordinance on the Money Laundering Reporting Office Switzerland (MROSO), SR 955.23.

²³ 2024: 1043; 2023: 866.

²⁴ 2022:1.4; 2023: 1.8.

3.2 Suspicious Activity Reports (SARs)

In 2024, MROS received a total of 15,141 SARs; that corresponds to an average of 59 SARs per working day. This represents an increase of 27.5% over the previous year. Since the introduction of goAML in 2000, the number of SARs submitted has almost tripled (see Figure 4).²⁵

As Figure 4 shows, the number of business relationships reported every year has increased almost twelvefold since 2015. In 2015, a total of 2,367 suspicious business relationships were reported to MROS; in 2024, the figure was around 27,300. There are several reasons for this increase: not only do financial intermediaries have a greater awareness and understanding of money laundering issues these days and are therefore more likely to submit a SAR to MROS, but new legal provisions and improved tools for transaction monitoring and internal analysis have also contributed to greater reporting volume.²⁶

3.3 Number of SARs by financial intermediary category

The vast majority of SARs – 92.3% – come from financial intermediaries in the banking sector. Their reporting behaviour has a significant influence on the number and type of SARs that MROS receives. The distribution of SARs among reporting FI categories has changed little since the introduction of goAML (see Table 1).

Since 2024, Virtual Asset Service Providers (VASP) and FinTech Providers have been classified as an individual category. In 2024, VASP und FinTech financial intermediaries submitted 227 SARs to MROS (1.5% of total reporting volume). 15

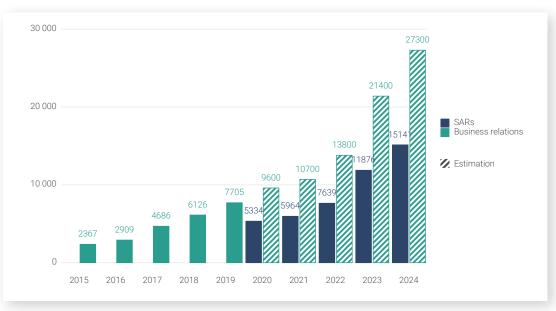


Figure 4: Number of business relationships and SARs 2015 – 2024

²⁵ The method of counting SARs changed with the introduction of goAML. In order to be able to compare the figures with previous years, Figure 4 takes the number of SARs submitted and multiplies this number by 1.8 (i. e. the average number of business relationships per SAR in 2019). This means that the 15,141 SARs submitted in 2024 are the equivalent of 27,300 business relationships.

²⁶ See information in <u>MROS Annual Report 2023</u>, Section 2.1.

Table 1: SARs by FI category, 2015 – 2024²⁷

| FI category | 2015 ^A | 2016 | 2017 ^A | 2018 ^A | 2019 ^A | 2020 [₿] | 2021 [₿] | 2022 [₿] | 2023 ⁸ | 2024 ⁸ | 2024 in absolute figures | Average 2015 - 2024 |
|---|--------------------------|------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------------|---------------------------|
| Bank | 91.3% | 86% | 91% | 88.8% | 89.9% | 89.5% | 90.0% | 91.6% | 90.5% | 92.3% | 13.973 | 90.1% |
| Payment service provider | 2.4% | 4.4% | 3.1% | 4.4% | 4.0% | 3.5% | 2.5% | 2.0% | 2.8% | 2.2% | 339 | 3.1% |
| Credit card company | 0.5% | 0.7% | 0.3% | 1.2% | 1.3% | 1.6% | 1.7% | 1.6% | 1.3% | 1.6% | 235 | 1.2% |
| VASP / FinTech | | | | | | | | | | 1.5% | 227 | |
| Asset manager | 1.9% | 2.2% | 1.9% | 1.0% | 0.9% | 0.8% | 1% | 0.6% | 0.8% | 0.9% | 137 | 1.2% |
| Casino | 0.1% | 0.5% | 0.6% | 0.5% | 0.7% | 0.5% | 0.5% | 0.7% | 0.5% | 0.3% | 47 | 0.5% |
| Loan, leasing, factor- ing and non-recourse financing | 0.3% | 0.3% | 0.3% | 0.3% | 0.3% | 0.4% | 0.3% | 0.3% | 0.2% | 0.2% | 37 | 0.3% |
| Securities trader | 0.1% | 0.1% | 0.3% | 0.1% | 0.3% | 0% | 0.2% | 0.1% | 0.2% | 0.2% | 32 | 0.2% |
| Fiduciary | 2% | 1.5% | 1.1% | 0.7% | 0.8% | 0.6% | 0.5% | 0.1% | 0.2% | 0.2% | 30 | 0.8% |
| Other financial inter- mediary | 0.2% | 0.7% | 0.4% | 2.3% | 0.6% | 2.3% | 2.1% | 2.1% | 2% | 0.2% | 24 | 1.3% |
| Commodity and pre- cious metal trader | 0.3% | 0.1% | 0.2% | 0% | 0.3% | 0.2% | 0.5% | 0.3% | 0.3% | 0.2% | 23 | 0.2% |
| Insurance | 0.5% | 3.1% | 0.5% | 0.6% | 0.3% | 0.4% | 0.3% | 0.3% | 0.4% | 0.2% | 23 | 0.7% |
| Currency exchange | 0% | 0% | 0% | 0% | 0% | 0.1% | 0.1% | 0.3% | 0.6% | 0% | 5 | 0.1% |
| Attorney or notary | 0.3% | 0.2% | 0.1% | 0.1% | 0.1% | 0.1% | 0.1% | 0% | 0.1% | 0% | 5 | 0.1% |
| SRO | 0% | 0% | 0% | 0% | 0.1% | 0% | 0% | 0% | 0.1% | 0% | 4 | 0% |
| Supervisory authority (FINMA/FGB/GESPA) | 0% | 0% | 0% | 0% | 0% | 0% | 0.1% | 0% | 0% | 0% | 0 | 0% |
| Foreign exchange trader | 0% | 0.1% | 0% | 0% | 0.3% | 0% | 0% | 0% | 0% | 0% | 0 | 0% |
| Trust and loan com- panies | 0% | 0% | 0% | 0% | 0% | 0.1% | 0.1% | 0% | 0% | 0% | 0 | 0% |
| Distributor of invest- ment funds | 0% | 0% | 0.1% | 0% | 0% | 0% | 0% | 0% | 0% | 0% | 0 | 0% |
| Total | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 15.141 | 100.0% |

^A Based on former calculation method (business relationship)

^B Based on new calculation method (SARs)

²⁷ The absolute figures for the years 2014 – 2023 are published in the MROS annual reports for the corresponding years.

3.4 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 to report to MROS under Art. 9 para. 1 let. a AMLA.28 In the case of simple suspicion, they have a right to report under Art. 305ter para. 2 SCC.²⁹ In 2024, financial intermediaries subject to the AMLA provisions reported 72.5% of SARs based on the duty to report (see Figure 5). The right to report under Art. 305ter para. 2 SCC was used in 21.7% of the SARs submitted. In 5.6% of cases, financial intermediaries reported that they had terminated negotiations to establish a business relationship due to reasonable grounds for suspicion in accordance with Art. 9 para. 1 let. a AMLA (Art. 9 para. 1 let. b AMLA; not shown in the chart).30

Since 2018, the number of SARs based on the duty to report has steadily gained ground on the right to report, with a significant increase in 2023 (see MROS 2023 Annual Report, Chapter 4.4). After a steady increase in the volume of 'duty to report' SARs in recent years, this year's statistics show some consolidation taking place in the two categories. While the use of the duty to report in an existing business relationship increased by 2.1% compared with the previous year, the right to report showed a marginal increase of 0.1%. There was a decrease of 2.3% in the number of SARs submitted by financial intermediaries regarding the termination of negotiations to establish a new business relationship in accordance with Art. 9 para. 1 let. b AMLA.



Figure 5: SARs according to legal basis 2015 – 2024

Art. 9 para. 1 let. a AMLA: A financial intermediary must immediately file a report with the Money Laundering Reporting Office Switzerland (MROS) 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. 260^{ter} or 305^{bis} SCC; (2) are the proceeds of a felony or an aggravated tax misdemeanour under Art. 305^{bis} no. 1^{bis} SCC; (3) are subject to the power of disposal of a criminal or terrorist organisation, or; (4) serve the financing of terrorism (Art. 260^{quinquies} para. 1 SCC).

²⁹ Art. 305^{ter} para. 2 SCC: The persons included in paragraph 1 above are entitled to report to MROS at the Federal Office of Police any observations that indicate that assets originate from a felony or an aggravated tax misdemeanour in terms of Art. 305^{bis} no. 1^{bis}.

³⁰ Art. 9 para. 1 let. b AMLA: A financial intermediary must immediately file a report with the Money Laundering Reporting Office Switzerland (MROS) 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.

3.5 Predicate offences

When submitting their SARs, financial intermediaries indicate which predicate offences they suspect. Over the past few years, around the same ten most frequent predicate offences have been reported (see Figure 6).31 The predicate offence most frequently reported by financial intermediaries is fraud: in 2024, it was cited in 59.4% of all SARs, either on its own or in combination with other offences (2020 - 23: 57.2%). Other predicate offences such as forgery (7.1%, compared to 12.1% in 2020 - 23) or embezzlement (4.1%, compared to 6.1% in 2020 - 23) are mentioned much less frequently.

The information provided by financial intermediaries on the suspected predicate offence is an important initial categorisation based on their clarifications. Figure 6 shows what predicate offence financial intermediaries suspected at the time of that triggered a SAR were information from third submitting a SAR. However, the analysis carried out parties (external sources of information) (26.9%)

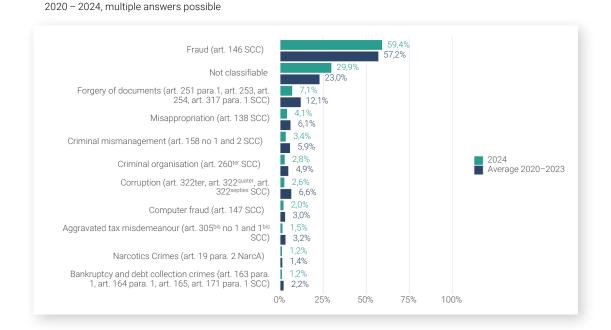
Figure 6: Frequency of suspected predicate offences

by MROS may lead to suspicion of a different predicate offence.32

In 2024, financial intermediaries stated in almost one in three SARs (29.9%) that they were unable to identify a predicate offence. This trend has increased over the years and continued in the current reporting year. The fact that around one-third of SARs submitted to MROS does not indicate a predicate offence has far-reaching consequences. It means that MROS has to use additional resources, to clarify what the predicate offence might be.

3.6 Factors arousing suspicion

Transaction monitoring is generally the most frequent reason why financial intermediaries submit a SAR: in 2024, it was mentioned in 29.6% of SARs (2020 - 23: 32.0%; see Figure 7).33 Other factors



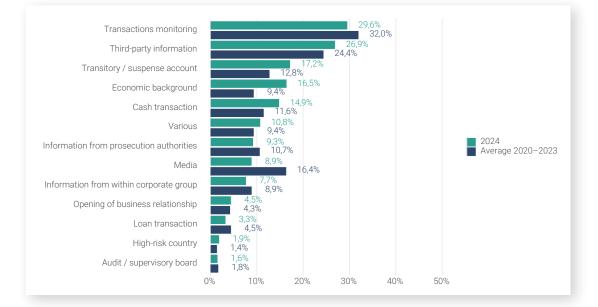
With the introduction of goAML 2020, multiple answers are possible. It is therefore not possible to compare with statistics prior to 2020

18

The interdepartmental Coordinating Group on Combating Money Laundering and the Financing of Terrorism (CGMF) conducted a detailed analysis of the various predicate offences to money laundering, which can be found in the Second national report money laundering and terrorist financing risks, October 2021, p. 25 - 29.

³³ Unlike in the years prior to 2020, financial intermediaries can now indicate several suspicious elements in their SARs submitted via goAML. However, it is no longer possible to make a meaningful comparison with the figures from the years prior to 2020.





and transitory accounts (17.2%). The unclear economic background of a business relationship was mentioned significantly more often in 2024 than in previous years (2024:16.5%; 2020 – 23: 9.4%).

3.7 MROS cases forwarded to prosecution authorities

In 2024, MROS forwarded 1,043 cases to the prosecution authorities under Art. 23 para. 4 AMLA. This is an increase of 20.4% over the previous year (2023: 866). In recent years, the forwarded cases have also been more detailed: in 2022, a case was based on an average of 1.4 SARs, compared with an average of 1.9 SARs in 2024.

The 1,043 cases contained information from:

- 1,481 SARs received in 2024
- 432 SARs received in 2023
- 32 SARs received in 2022
- 13 SARs received in 2021
- 5 SARs received in 2020
- 2 business relationships reported prior to 2020

Of the total number of cases forwarded, 89.7% were sent to cantonal public prosecutors' offices

and 10.3% to the Office of the Attorney General of Switzerland (OAG).

In 2024, as in previous years, the public prosecutors' offices of the cantons of Zurich (17.9%), Vaud (12.4%) and Geneva (10.2%) as well as the OAG (10.3%) accounted for about half of all cases forwarded by MROS (see Table 2).

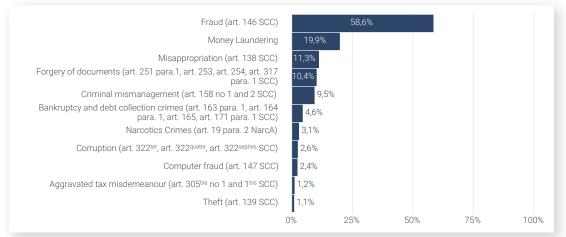
In 2024, MROS forwarded just under 60% of cases to the prosecution authorities on the basis of reasonable suspicion that the assets could be the proceeds of fraud. In one fifth of the cases forwarded, MROS reported the direct offence of money laundering (see Figure 8). This occurs, for example, when the person accused of a predicate offence is not necessarily the same person who is involved in money laundering activities.

| Canton | 2020 | 2021 | 2022 | 2023 | 2024 | 2024 in absolute figures | Average 2020 – 2024 |
|------------------------|--------|--------|--------|--------|-------|--------------------------------|------------------------|
| Zurich | 18.9% | 21.1% | 20.4% | 16.3% | 17.9% | 187 | 18.9% |
| Vaud | 11.1% | 11.6% | 10.6% | 8.3% | 12.4% | 129 | 10.8% |
| OAG | 9.0% | 9.1% | 6.4% | 13.0% | 10.3% | 107 | 9.6% |
| Geneva | 11.5% | 11.3% | 11.6% | 17.6% | 10.2% | 106 | 12.4% |
| Bern | 7.5% | 6.7% | 6.9% | 6.5% | 7.7% | 80 | 7.1% |
| Aargau | 5.3% | 5.2% | 6.7% | 4.2% | 5.7% | 59 | 5.4% |
| Ticino | 5.0% | 4.8% | 3.6% | 4.6% | 5.5% | 57 | 4.7% |
| St Gallen | 3.5% | 4.0% | 6.3% | 5.3% | 5.3% | 55 | 4.9% |
| Lucerne | 3.5% | 2.9% | 2.6% | 2.5% | 3.9% | 41 | 3.1% |
| Basel-Stadt | 2.6% | 2.3% | 2.3% | 1.8% | 3.2% | 33 | 2.4% |
| Wallis | 2.7% | 2.4% | 3.0% | 2.2% | 2.9% | 30 | 2.6% |
| Basel-Landschaft | 2.1% | 1.7% | 2.3% | 1.8% | 2.2% | 23 | 2.0% |
| Fribourg | 2.7% | 3.1% | 2.1% | 1.3% | 2.1% | 22 | 2.3% |
| Solothurn | 1.9% | 2.0% | 2.1% | 1.4% | 2.1% | 22 | 1.9% |
| Thurgau | 3.0% | 2.1% | 2.6% | 3.2% | 1.7% | 18 | 2.5% |
| Schwyz | 1.0% | 1.1% | 1.9% | 2.1% | 1.5% | 16 | 1.5% |
| Zug | 2.5% | 2.6% | 2.2% | 2.2% | 1.2% | 12 | 2.1% |
| Graubünden | 1.5% | 1.0% | 1.1% | 0.6% | 1.1% | 11 | 1.1% |
| Neuchâtel | 2.3% | 1.9% | 1.7% | 1.3% | 1.0% | 10 | 1.6% |
| Schaffhausen | 0.5% | 0.5% | 0.6% | 0.7% | 0.6% | 6 | 0.6% |
| Appenzell Ausserrhoden | 0.6% | 0.8% | 1.3% | 0.9% | 0.5% | 5 | 0.8% |
| Jura | 0.3% | 1.0% | 0.2% | 0.7% | 0.4% | 4 | 0.5% |
| Appenzell Innerrhoden | 0.0% | 0.1% | 0.2% | 0.2% | 0.3% | 3 | 0.2% |
| Nidwalden | 0.3% | 0.4% | 0.6% | 0.6% | 0.3% | 3 | 0.4% |
| Glarus | 0.2% | 0.1% | 0.4% | 0.6% | 0.2% | 2 | 0.3% |
| Obwalden | 0.2% | 0.1% | 0.2% | 0.0% | 0.2% | 2 | 0.1% |
| Uri | 0.3% | 0.1% | 0.2% | 0.1% | 0.0% | 0 | 0.1% |
| Total | 100.0% | 100.0% | 100.0% | 100.0% | 100% | 1043 | 100.0% |

Table 2: Cases forwarded to prosecution authorities n 2020 – 2024

Figure 8: Frequency of cases forwarded to prosecution authorities, 2024

multiple answers possible



3.8 Feedback from prosecution authorities

Under Art. 29*a* AMLA, the prosecution authorities must notify MROS of all pending proceedings, in particular those relating to money laundering, criminal or terrorist organisations, or the financing of terrorism.³⁴ In addition, prosecution authorities must notify MROS promptly of any rulings that they have issued that are connected to a case forwarded to them by MROS.³⁵ This feedback is important for MROS to fulfil its mandate of providing the best possible support to the prosecution authorities.

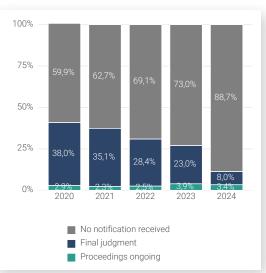
Statistics from the 2023 annual report showed that MROS had not yet received feedback on a large proportion of the cases, which is due to the time-consuming nature of the work done by the prosecution authorities.³⁶ If we look only at those cases forwarded to the prosecution authorities more than 12 months ago (period 2020 – 23), we find that as of December 31 2024, MROS was still awaiting feedback for around two-thirds of the cases (64.3%). This applies to more than half of the cases forwarded in 2020 for which proceedings are still pending.

The prosecution authorities reported a total of 2,024 penalty orders and 82 judgments issued in connection with MROS cases, as well as 262 no-proceedings orders (Art. 310 para. 1 CrimPC) or rulings abandoning proceedings (Art. 320 CrimPC).

The absence of such feedback in the overwhelming majority of cases prevents MROS from properly assessing the proportion of judgments, no-proceedings orders and rulings abandoning proceedings. MROS will therefore continue working with the prosecution authorities to find ways to obtain the legally required feedback under Art. 260^{ter}, 260^{quinquies} para. 1, 305^{bis} and 305^{ter} para. 1 SCC.

Figure 9: Feedback on forwarded cases and current status

2020 - 2024



3.9 Terrorist financing

In 2024, MROS received 106 SARs reporting suspected terrorist financing and/or violations of the Federal Act on the Proscription of Al-Qaeda, Islamic State and Associated Organisations.³⁷ This corresponds to 0.7% of overall reporting volume. Most of these SARs were also linked to other predicate offences. The most common additional grounds for suspicion were:

- Participation in a criminal or terrorist organisation³⁸ (25 mentions)
- Fraud³⁹ (9 mentions)
- Violation of the Embargo Act⁴⁰ (4 mentions)
- Violation of the Narcotics Act⁴¹ (3 mentions)
- Recruiting, training and travel with a view to committing a terrorist offence⁴² (3 mentions)
- Criminal mismanagement⁴³ (3 mentions)

21

³⁴ Art. 29a para. 1 AMLA: The prosecution authorities shall notify the Reporting Office without delay of any pending proceedings connected with Art. 260^{ter}, 260^{quinquies} para. 1, 305^{bis} and 305^{ter} para. 1 SCC. They shall provide the Reporting Office without delay with judgments and decisions on the closure of proceedings, including the grounds therefor.

³⁵ Art. 29*a* para. 2 AMLA.

³⁶ See MROS Annual Report 2023, p. 26 f.

³⁷ Federal Act of 12 December 2014 on the Proscription of Al-Qaeda, Islamic State and Associated Organisations, SR 122, fully repealed on 1 December 2022.

³⁸ Art. 260^{ter} SCC.

³⁹ Art. 146 SCC.

⁴⁰ Art. 9 para. 2 Federal Act of 22 March 2002 on the Implementation of International Sanctions (Embargo Act, EmbA), SR 946.231.

⁴¹ Art. 19 para. 2 Federal Act on Narcotics and Psychotropic Substances (NarcA).

⁴² Art. 260^{sexies} SCC.

⁴³ Art. 158 nos 1 and 2 SCC

SARs involving suspicion of terrorist financing came predominantly from banks (76 reports); another 15 SARs came from payment services providers.

Financial intermediaries most often mentioned the following as factors arousing suspicion:

- Media reports (36 mentions)
- Transaction monitoring (33 mentions)
- Third-party information (26 mentions)
- Cash transactions (24 mentions)
- Unclear economic background (19 mentions)

Of the 106 SARs that MROS received in 2024, a total of 10 cases had been forwarded to the relevant prosecuting authorities as of 31 December 2024.

3.10 Organised crime

Of the 15,141 SARs received by MROS in 2024, the financial intermediary suspected participation in a criminal organisation in 424 cases (2.8%). The vast majority of these SARs came from the banking sector (90.5%). According to the financial intermediaries, the SARs were triggered mainly by media re-

SARs involving suspicion of terrorist financing ports (28.5%) and/or transaction monitoring (17.2%; came predominantly from banks (76 reports); an- see Table 3).

In addition to suspected links to a criminal organisation, financial intermediaries often cited fraud (42.9%) and/or bribery (8.5%) as further possible predicate offences. The 424 SARs that MROS received in 2024 led to 33 cases being forwarded to the relevant prosecution authorities.

3.11 SARs involving the use of cryptocurrencies

In 2024, 1,799 SARs related to virtual currencies (virtual assets [VA]⁴⁴; see Figure 10), which is higher than in the previous reporting year.⁴⁵ This trend creates additional challenges for MROS: virtual currencies make it more difficult to trace money flows and thus determine the origin of assets and clearly identify the beneficial owner. A detailed report published in the first quarter of 2024, 'National Risk Assessment (NRA): Risk of money laundering and the financing of terrorism through crypto assets', describes in detail the greater risks posed by cryptocurrencies.⁴⁶

Table 3: Frequency of factors arousing suspicion in SARs submitted in relation to suspected links to criminal organisations

| Factors arousing suspicion (multiple answers possible, most frequently mentioned) | Number of mentions | in % of total SARs |
|---|--------------------|-----------------------|
| Media reports | 121 | 28.5% |
| Transaction monitoring | 73 | 17.2% |
| Unclear economic background | 59 | 13.9% |
| Third-party information | 54 | 12.7% |
| Cash transaction | 52 | 12.3% |
| Opening of business relationship | 36 | 8.5% |
| Information from prosecution authority | 34 | 8.0% |
| Pass-through account | 34 | 8.0% |
| Information from within corporate group | 29 | 6.8% |
| Audit / supervision | 20 | 4.7% |

⁴⁴ The term 'virtual currency' was used in Swiss legislation for the first time in Art. 4 para. 2 let. a of the Ordinance on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Ordinance, AMLO), SR 955.01, which came into effect on 1 January 2016.

⁴⁵ To date, it has not been possible to directly ascertain the extent to which the suspicious activity mentioned in SARs involved virtual currency transactions, as such transactions are not clearly identifiable. SARs with a relevant VA 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 activities and, on the other hand, by means of a list of relevant keywords. It can therefore be assumed that the significance of cryptocurrencies in SARs is likely to be underestimated.

⁴⁶ National Risk Assessment (NRA) – <u>Risk of money laundering and the financing of terrorism through crypto assets</u>, January 2024.

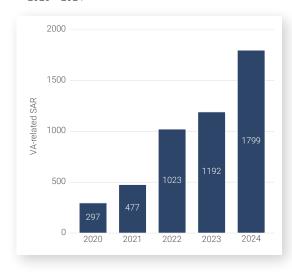


Figure 10: Number of VA-related SARs 2020 – 2024

intermediaries (see Table 1). By 31 December 2024, 30 financial intermediaries in the VASP/FinTech category had registered with the goAML system.

3.12 Requests for information under Art. 11a AMLA

In 2024, MROS submitted 1,016 information requests to financial intermediaries based on Art. 11*a* AMLA. The number of information requests had been steadily increasing since 2020; in 2024, MROS recorded a slight decline, back to the level of 2021 (see Figure 11). Of the 1,016 information requests, MROS most frequently sent requests to so-called third-party intermediaries (40.7%, Art. 11*a* para. 2 AMLA⁴⁸), who are or were involved in a transaction or business relationship alongside the reporting financial intermediary. One in four requests was addressed to the financial intermediaries that had submitted the original SARs (24.8%, Art. 11*a* para. 1 AMLA⁴⁹).

Around one third of the information requests were sent by MROS to a financial intermediary based

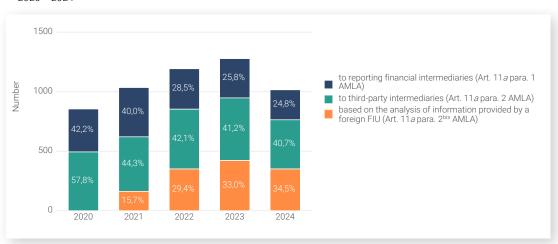


Figure 11: Requests for information under Art. 11a AMLA 2020 – 2024

Since the spring of 2024, MROS has placed finan-

cial intermediaries that consider themselves as vir-

tual asset providers (VASP) into a separate category.⁴⁷ This enables statements to be made regarding

the reporting behaviour of this category of financial

⁴⁷ In March 2024, financial intermediaries registered in goAML were asked to notify MROS if their main activity placed them in the category of a VASP.

⁴⁸ 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 MROS with all related information that is in their possession.

⁴⁹ Art. 11a para. 1 AMLA: If MROS 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.

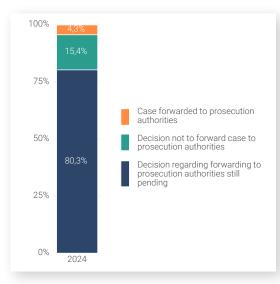
on the analysis of information provided by a foreign FIU (34.5%, Art.11*a* para. 2^{bis} AMLA⁵⁰). Since the introduction of Article 11*a* para. 2^{bis} AMLA in 2021, these requests have gained increasing relevance compared to other requests under Article 11*a* AMLA (+1.5% compared to the previous year).

3.13 Terminated business relationship notification under Art. 9b AMLA

According to Art. 9b AMLA⁵¹ if MROS does not inform the financial intermediary within 40 working days that it is transmitting the reported information to a prosecution authority, the financial intermediary may terminate the business relationship. The termination of the business relationship must be notified to MROS without delay.⁵²

In 2024, MROS received 7,118 terminated business relationship notifications; this is almost three times as many as in the previous reporting year (2023: 2,669 terminated business relationship notifica-





tions). Of this number, 4.3% of terminated business relationship notifications related to cases that had been forwarded to the prosecution authorities in the course of 2024 (see Figure 12).

3.14 Information-sharing with foreign financial intelligence units (FIUs)

In the fight against money laundering and its predicate offences, terrorist financing and organised crime, MROS and foreign FIUs share information through mutual administrative assistance. This information is essential for MROS's analyses, as a large proportion of SARs from Swiss financial intermediaries have a foreign connection.⁵³

While the number of information requests that MROS has sent to foreign FIUs had increased in recent years, there was a slight decline in 2024. In 2024, MROS sent 239 information requests to 56 different foreign FIUs (-14.0% compared to the previous reporting year). In 2024, MROS received 780 information requests from 96 foreign FIUs. MROS processed 422 incoming requests alongside 188 requests from the previous years.

Foreign FIUs and MROS can also share information spontaneously, whether it comes from abroad and relates to Switzerland or is sent by MROS to a foreign FIU. In such cases, there is no prior request. In 2024, MROS received 751 spontaneous information reports from 45 countries (2023: 726 from 53 countries). MROS in turn sent 189 spontaneous information reports to 41 foreign FIUs (2023: 160 to 47 FIUs).

3.15 Information-sharing with Swiss authorities

According to Art. 29 AMLA, MROS may share relevant information with Swiss authorities upon request or spontaneously. These are supervisory

24

⁵⁰ Art. 11a 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.

⁵¹ Art. 9b AMLA stipulates that financial intermediaries may terminate a business relationship after submitting an SAR under Art. 9 para. 1 let. a AMLA or under Art. 305^{ter} para. 2 SCC, if MROS does not inform the financial intermediary within 40 working days that it is transmitting the reported information to a prosecution authority.

⁵² Art. 9b para. 3 AMLA.

⁵³ Second national report money laundering and terrorist financing risks, October 2021.

authorities or other authorities active in the fight against money laundering and its predicate offences, organised crime or terrorist financing.⁵⁴

In the current reporting year, MROS received 447 information requests from 35 Swiss authorities in relation to specific bank accounts, persons or companies (-35.8%; 2023: 696). As in previous reporting years, around 80% of these requests came from police authorities. MROS also provided information to Swiss supervisory and other authorities in 358 cases without being asked (+79.0%; 2023: 200). In addition, MROS received 106 spontaneous information reports from domestic authorities in 2024 (-12.3%, 2023: 119).

⁵⁴ The figures do not include requests for information made by MROS to other federal, cantonal and municipal authorities in the course of its analyses.

4 Trends

The new section 'Trends' in this annual report replaces 'Typologies', which will be posted on the MROS website starting in May 2025 (see 2.1). The trends provide a holistic view of MROS findings on selected topics. This year's focus is on online gambling, child pornography, virtual assets and the proscription of Hamas.

4.1 Online gambling General information

The pursuit of good fortune and quick gains is not a modern or culturally specific phenomenon, but rather a deeply rooted human behaviour that continues to play a major role in the world today. It is something that has captivated people for thousands of years.⁵⁵ The figures suggest that the gambling market – both online and in person – is growing.

In 2023, the global gambling market grew to around USD 774 billion (approx. CHF 691 billion), which represents a significant increase since 2006 when the turnover was still around USD 70 billion (approx. CHF 62 billion).⁵⁶ Similar growth is also evident in Switzerland: between 2017 and 2022, the turnover of the entire Swiss gambling sector rose by 13%, with revenues increasing from around CHF 2.2 billion to around CHF 2.5 billion.⁵⁷ About six out of ten people in Switzerland have gambled for money at least once in their lives.⁵⁸ The online gambling market is also growing rapidly. Global revenues are expected to climb from around USD 85 billion (approx. CHF 76 billion) in 2023 to around USD 173 billion (approx. CHF 155 billion) by 2039.⁵⁹

for example, experienced a heightened money laundering risk from the surge in new online gambling platform providers. The Maltese NRA also identified a significant risk associated with online gambling, highlighting the fact that some of these platforms could be run by criminal entities.⁶¹

Given the increasing money laundering risks observed abroad, it is worth taking a look at the risk situation in Switzerland.

Potential money laundering risk

In the case of a casino, money laundering risk can appear in all three stages of money laundering (placement, layering and integration):

- Placement (preparation for gambling): casinos convert cash (fiat money) into cheques (book money), exchange different denominations (smurfing). At the player level, currency exchange can take place. In physical casinos, players wager chips that they have previously obtained, often in exchange for cash, either directly at the table or at the cash desk. To conceal the actual ownership structure, straw men may be used.
- Layering (during gambling): Criminals make increasing use of the financial services (e. g. customer deposits or international payments) provided by casinos. Criminals are also willing to lose some of their bets in order to obtain seemingly legal assets.
- **Integration:** In order to be able to launder money on a large scale via gambling, criminals seek to operate casinos, particularly abroad.⁶²

Risk and legislative situation in Switzerland

Many countries see a rapid increase in revenues, National assessment reports on money launderparticularly from online gambling activities, as a significant risk factor for money laundering. The USA⁶⁰, 2015⁶³ and 2021⁶⁴ rate the risk of money laundering

⁵⁵ Homepage Spielbanken Sachsen, article dated 2 November 2022, <u>Die Geschichte des Glücksspiels, last consulted on 31</u>

January 2025.

⁵⁶ FATF Report, <u>Vulnerabilities of Casinos and Gaming Sector, 2009, p.9</u>.

⁵⁷ Report by the Fachdirektorenkonferenz Geldspiele, <u>Marktanteile des legalen und des illegalen Geldspielangebots in der Schweiz,</u> Internet- und Sekundärdaten-Analyse, April 2024, p. 3.

Study conducted by the Swiss Research Institute for Public Health and Addiction, <u>Geldspiel: Verhalten und Problematik in der Schweiz 2022, Zusammenfassung, Zürich, October 2024.</u>

⁵⁹ Global Strategic Business Report, Mobile Gambling Market Assessment and Investment Opportunities, September 2024.

⁶⁰ The Department of the Treasury, 2024 National Money Laundering Risk Assessment (NMLRA), p. 81 ff.

⁶¹ National Coordinating Committee on Combating Money Laundering and Funding of Terrorism, <u>Malta's National Risk</u> <u>Assessment 2023</u>, p. 115 ff.

⁶² <u>First national report on money laundering and terrorist financing risks</u>, June 2015, p. 85.

⁶³ <u>First national report on money laundering and terrorist financing risks</u>, June 2015, p. 5.

⁶⁴ Second national report money laundering and terrorist financing risks, October 2021, p. 45.

adds that the risk associated with Swiss online casinos, which were only introduced in 2019, is difficult erations. The applicants must also be able to prove to assess.

The strict conditions for awarding a licence, which is required in order to operate a casino in Switzerland, could be one reason for the low risk of money laundering. At the end of 2024, the Federal Council awarded 10 licences for the years 2025 to 2044 without any legal restriction on maximum stakes⁶⁵ and 12 with a limit on maximum stakes,66 amount- require approval from the Federal Gaming Board ing to a total of 22 licences.⁶⁷ The awarding of li-

in relation to casinos as very low. The 2021 report and all other persons involved must have a good reputation 68 and guarantee flawless business opthat they have an adequate system in place to prevent crime and money laundering.⁶⁹

Since 1 January 2019, the Gambling Act has made it possible for the existing casinos to also offer their games online.⁷⁰ To do so, they require a licence extension, which is issued by the Federal Council. In addition to this licence extension, casinos also (FGB) for individual games before they can comcences is subject to strict criteria. The applicants mence their online activity.⁷¹ Swiss casinos must



Figure 13: Federal Gaming Board FGB, New licences: new casino landscape from 2025 (zone map), November 2023 (only available in German).

⁶⁵ Type A licence.

⁶⁶ Type B licence

⁶⁷ Federal Council press release of 29 November 2023: '<u>Bundesrat vergibt Spielbankenkonzessionen: Kontinuität in der</u> Casinolandschaft'

⁶⁸ Federal Council Dispatch on Gambling Act, BBI 2015 8387, 8441: A key criterion, for example, is previous conduct on the Swiss market. It can therefore be assumed that, under the new legislation, anyone who has deliberately operated on the Swiss online casino market without a licence in the past or has been convicted of an offence in Switzerland or abroad will not fulfil the criterion of having a good reputation.

⁶⁹ Art. 8 Federal Act of 29 September 2017 on Gambling (Gambling Act, GamblA), SR 935.51.

⁷⁰ Art. 9 GamblA

⁷¹ Federal Gaming Board FGB: Online-Spielbanken, last consulted on 31 January 2025.

comply with AMLA due diligence requirements in the fight against money laundering. So far, ten applicants have received such a licence in Switzerland for the new period starting in 2025.⁷²

When awarding a licence, care must be taken to identify potential high-risk providers at an early stage and to exclude them before the licence is granted. During operations, providers are also required to comply with AML/CFT requirements.⁷³ For example, AMLA due diligence must be carried out when opening a player account for an online game, and clarifications must be sought when transactions take place via the player account.⁷⁴ During operation, the focus is therefore on the players.

Providers are only authorised to carry out their activities in Switzerland if they have first obtained a Swiss licence. Foreign providers are prohibited from offering their online games in Switzerland without a licence. The FGB blocks these websites and publishes a blacklist of these providers.⁷⁵

Reporting patterns in Switzerland

The volume of SARs from Swiss casinos has been consistently low for over a decade. Between 2014 and 2024, an average of 0.5% of incoming SARs were submitted by casinos. In 2024, the figure was 0.3% (47 of 15,141 SARs; see Table 1).

Most of the incoming SARs in 2024 were triggered by background checks into the origin of the assets used for gambling. For example, players bought chips in physical casinos using funds believed to be of criminal origin, gambled only a small amount and then cashed in the chips before leaving the casino.

Other SARs were triggered by clarifications relating to player protection, for example in order to protect players from losing control over their gambling and to discourage them from continuing to gamble to prevent financial losses. Casinos are obliged to impose a gambling ban if they know or suspect that a person is heavily in debt or can no longer meet their financial obligations.⁷⁶ When clarifying the conditions for blocking, it may be determined, for example, that the player cannot plausibly explain the amount of funds used for gambling or their origin. These circumstances prompt the casinos to carry out further duties of due diligence and, if necessary, report the matter to MROS.

While the use of cryptocurrencies is an issue in foreign casinos, it is not yet relevant in Swiss casinos. Cryptocurrencies are currently prohibited as a means of payment in Switzerland.⁷⁷

Criminal prosecution statistics confirm the reporting figures: there have only been a small number of money laundering convictions in connection with Swiss casinos, and these mostly involved small amounts. On 21 July 2023, the public prosecutor of the Canton of Zug secured a conviction under Art. 305^{bis} para. 1 SCC against the holder of a player account (X), who was then issued a fine. The judgment shows that X's user account was used by other people with his knowledge to play in an online casino. Another person (Y) took the opportunity to use X's player account to gamble with money that Y had previously obtained illegally. Y had obtained the bank details of a third person (Z) in order to transfer funds from that person's account to X's player account. X then had the winnings that Y had generated transferred to his account, withdrew the money in cash and gave it to Y.

Overall, it can be said that money laundering in connection with casinos in Switzerland is combated on several levels. Casinos must obtain a business licence and players are subject to anti-money laundering measures that are strict compared to other countries. In addition,

⁷² Federal Gaming Board FGB: Online-Spielbanken, last consulted on 31 January 2025.

⁷³ Art. 67 GamblA and Ordinance of the Federal Gaming Board of 12 June 2007 on the Diligence of Casinos in Combating Money Laundering (Anti-FGB-Money Laundering Ordinance, AMLO-FGB), SR 955.021.

⁷⁴ Art. 52 in conjunction with Art. 47 Ordinance on Gambling (Gambling Ordinance, Gamblo), SR 935.511. Also worth mentioning are the other legal requirements for combating money laundering, in particular that casinos are not permitted to issue statements of winnings (Art. 70 GamblA) and that there are further requirements regarding cheques and deposits (Art. 69 GamblA).

⁷⁵ Federal Gaming Board FGB: <u>Nicht bewilligte Online-Spiele, last consulted on 31 January 2025</u>.

⁷⁶ Federal Office of Public Health (FOPH), <u>Geldspiel, last consulted on 31 January 2025</u>.

⁷⁷ National Risk Assessment (NRA) – <u>Risk of money laundering and the financing of terrorism through crypto assets</u>, January 2024, p. 39.

unauthorised online casinos from abroad are blocked and placed on a blacklist. This implies that the Swiss AML system is effective, which explains why MROS receives only a small number of SARs relating to online gambling.

4.2 Child pornography and virtual assets

Each year, data on pornography offences are collated in the Police Crime Statistics (PCS). These statistics do not indicate how many of the offences specifically involved child pornography. The data on pornography offences within the meaning of Art. 197 SCC show a bleak picture each year.⁷⁸ While the prosecuting authorities have had some success in taking down pornography rings⁷⁹, prosecution has proved challenging.80 Because of digital networking, victims and perpetrators are rarely in the same country. This can also be seen in the crime statistics⁸¹, since even if the abuse occurs locally, the images and videos are distributed and consumed globally. In 2023, 2,967 pornography offences were detected in Switzerland⁸², 85.4% of which occurred online.83

Child pornography is a punishable offence under Art. 197 SCC. Anyone who commits a criminal offence within the meaning of Art. 197 para. 4 SCC⁸⁴, risks up to five years of imprisonment, which qualifies it as a felony and a predicate offence to money laundering.⁸⁵

Given that the offence of child pornography is mostly committed online and that payments are regularly made for the content in question, it is all the more surprising that in 2024 MROS did not receive a single SAR indicating a suspicion of child pornography. However, it did receive 70 spontaneous information reports from foreign FIUs. In some cases, these spontaneous information reports resulted in links to SARs which had been submitted to MROS from financial intermediaries that had been unable to clearly identify the predicate offence.

The foreign FIUs reported potential offenders to MROS. In most cases, the offenders used crypto wallets and other supposedly anonymous payment methods to send small amounts to counterparties or to accounts and wallets abroad. These findings are consistent with the results of a study conducted by the international non-profit organisation Internet Watch Foundation (IWF).⁸⁶ According to this report, cryptocurrencies, credit cards and money transmitters are the main methods used to pay for child sexual abuse material (CSAM). Each of the reporting financial intermediaries abroad were able to show a clear link between the offence and the wallets, accounts or potential perpetrators. The residential addresses of offenders were spread out across the whole of Switzerland, with no geographical focus. In contrast, the victims are mainly located in Asia, Eastern Europe and South America.

Ultimately, neither child pornography nor virtual payment options are new phenomena. However, there is a discrepancy between the lack of SARs from Swiss financial intermediaries and the regular spontaneous information reports received from abroad. MROS therefore intends to close this gap. Since 2024, it has been a member of the 'Sexual Child Abuse' working group at EFIPPP. MROS uses the knowledge gained to

⁷⁸ Federal Statistical Office (FSO), <u>Strafgesetzbuch (SCC)</u>: <u>Straftaten und beschuldigte Personen</u>, 2009 – 2023.

⁷⁹ SRF News: Ermittlungen in Deutschland – Grosse Kinderpornografie-Plattform abgeschaltet, last consulted on 31 January 2025; Blick newspaper: Koordinierte Aktion im Tessin – Zwölf Menschen wegen illegaler Pornografie festgenommen, last consulted on 31 January 2025.

⁸⁰ Neue Zürcher Zeitung (NZZ): <u>Kinderporno-Flut: Ermittler aus Zürich sagt, es werde immer schlimmer</u>, last consulted on 31 January 2025.

⁸¹ FSO, Polizeiliche Kriminalstatistik (PKS) - Jahresbericht 2023 der polizeilich registrierten Straftaten.

⁸² FSO, Polizeiliche Kriminalstatistik (PKS) - Jahresbericht 2023 der polizeilich registrierten Straftaten, p.9.

⁸³ FSO, Polizeiliche Kriminalstatistik (PKS) - Jahresbericht 2023 der polizeilich registrierten Straftaten, p.62.

⁸⁴ Art. 197 para. 4 (second sentence) SCC: Any person who produces, imports, stores, markets, advertises, exhibits, offers, shows, passes on or makes accessible to others, acquires, or procures or possesses via electronic media or otherwise pornographic documents, sound or visual recordings, depictions or other items of a similar nature or pornographic performances, shall be liable to a custodial sentence not exceeding five years or a monetary penalty if the items or recordings contain genuine sexual acts with minors.

⁸⁵ Predicate offences are defined as felonies, i. e. punishable by a custodial sentence exceeding three years (see Art. 305^{bis} no 1 in conjunction with Art. 10 para. 2 SCC).

⁸⁶ Internet Watch Foundation, The Annual Report 2022, p. 85.

raise financial intermediary awareness. (e. g. in the FIAHT Guide, see 2.5.1). 87

Whenever possible, financial intermediaries are required to file a SAR indicating the suspected predicate offence as soon as an indicator is detected. This is the only way to ensure that MROS can properly and effectively analyse a SAR, even without additional information from abroad, and forward it to the prosecution authorities where appropriate.

4.3 **Proscription of Hamas**

Money laundering legislation already imposes a duty on financial intermediaries and traders to report suspicions of terrorist financing to MROS if they know or have reasonable grounds to suspect that assets involved in the business relationship are connected to an offence in terms of Art. 260^{ter} SCC (criminal and terrorist organisations)⁸⁸, are subject to the power of disposal of a criminal or terrorist organisation⁸⁹, or serve the financing of terrorism.⁹⁰

Recognising terrorist financing is a challenge for financial intermediaries. This is because the funds involved are often 'clean', i. e. not incriminated. With suspected cases of money laundering, financial intermediaries are asked to ascertain whether assets might originate from a predicate offence. With terrorist financing, on the other hand, financial intermediaries are asked to determine whether funds might be used for terrorist financing in the future. This is obviously difficult to recognise, especially in situations where assets are paid out to individuals or organisations that have no direct connection to known terrorist organisations and whose activities have not yet been classified as terrorist. The recognition and fight against terrorist financing ex ante is thus more difficult to carry out than focusing on past events - as is the case with money laundering. Furthermore, terrorist financing often involves

small sums (donations from numerous people). Typically, such transactions do not trigger (automated) transaction monitoring on the part of financial intermediaries and therefore do not prompt indepth clarifications.⁹¹

On 4 September 2024, the Federal Council adopted its dispatch on the Federal Act on the Proscription of Hamas and Associated Organisations and submitted it to parliament.92 In December 2024, the Federal Assembly decided to adopt the federal act.93 The Federal Council will determine the date of entry into force after the referendum deadline has expired (19 April 2025). Furthermore, the Federal Council was also instructed to ban Hezbollah. This proscription provides greater legal certainty for financial intermediaries, as they no longer have to judge for themselves whether the organisations in question are terrorist in nature. Classifying a group as a terrorist organisation also clarifies the situation for MROS by unambiguously designating their activities as a predicate offence to money laundering.94 This forms the legal basis for sharing information with foreign partner authorities. If the volume of terrorist-financing SARs filed by financial intermediaries increases, then MROS will also have a greater amount of information to share with foreign countries through international administrative assistance. This, in turn, will lead to more effective prosecution.

Since the Hamas attacks of 7 October 2023, MROS has received around 40 SARs relating to potential Hamas funding. Among these SARs, MROS has identified risks linked to associations and foundations that ostensibly support humanitarian projects. The public 'pro-Hamas' statements of certain members of these institutions have led MROS to conduct an in-depth analysis of the financing of these legal entities and the outflow of funds. The public 'pro-Hamas' statements of private individuals who receive donations and withdraw the money

⁸⁷ This is also the case, for example, in the FIAHT Guide published by MROS, which provides indicators enabling identification of child pornography: <u>Einancial Intelligence against Human Trafficking, Guide</u>, p. 15 as well as p. 19 ff.

⁸⁸ See Art. 9 para. 1 let. a no 1 AMLA.

⁸⁹ See Art. 9 para. 1 let. a no 3 AMLA.

⁹⁰ See Art. 9 para. 1 let. a no 4 AMLA.

⁹¹ Second national report money laundering and terrorist financing risks, October 2021, p. 48.

⁹² Federal Council press release of 4 September 2024, 'Der Bundesrat verabschiedet die Botschaft zum Verbot der Hamas'.

⁹³ Final vote text of 20 December 2024, BBI 2025 21.

⁹⁴ Predicate offences are defined as felonies, i. e. punishable by a custodial sentence exceeding three years.

in cash have also prompted MROS to thoroughly analyse several cases. With regard to the cryptocurrency sector, some financial intermediaries active in this sector have carried out transaction analyses on the blockchain. Often indirect links with flagged wallets have triggered SARs.

MROS endeavours to gain an overview of potential financing of Hamas from Switzerland. When there are reasonable grounds for suspicion of terrorist financing, cases are forwarded to the Office of the Attorney General of Switzerland.

In essence, legal certainty for classification of Hamas as a terrorist organisation was established with the entry into force of the Federal Act on the Proscription of Hamas and Associated Organisations. MROS is constantly analysing the development of incoming SARs related to Hamas. It has observed that associations and foundations that provide financial support for humanitarian projects pose a potential terrorist financing risk (see the information letter and typologies sent to financial intermediaries).⁹⁵

⁹⁵ Alert of 3 November 2023 as well as Addendum of 5 December 2023. This alert was compiled from FATF publications, information from foreign FIUs and MROS findings; available here: <u>Publications of the Money Laundering Reporting Office Switzerland</u> (<u>MROS</u>).

5 From the MROS Practice

5.1 Immediate reporting vs depth of clarification – MROS position

Over the past two years, MROS has noted deficiencies and qualitative differences in the content of SARs. In some cases, financial institutions submit only very rudimentary or barely clarified facts. In other cases, it is not clear to MROS whether special clarifications have been made under Art. 6 AMLA and thus the elements arousing suspicion have been duly assessed. MROS already noted this trend in its 2023 annual report and attributed it to general cost considerations. In addition, financial intermediaries assert that the pressure to file SARs as guickly as possible has increased considerably. They feel that the authorities have narrowed the definition of the term 'immediacy', which determines how quickly a SAR is to be submitted to MROS. The threat of criminal proceedings hanging over the financial intermediaries and their employees massively intensifies this pressure.

MROS can only comment on these assertions insofar as they relate to its core area of operational reporting. The Swiss AML system operates on the principle that financial intermediaries perform the initial fundamental clarifications with regard to the possibly illicit nature of assets or transactions. Lawmakers have clearly expressed their preference for qualitative reporting. For example, Swiss law has deliberately avoided 'threshold-based' reporting, whereby a SAR is required if a certain transaction threshold or other quantitative trigger is reached. AMLA due diligence requirements are structured in a cascading and repetitive fashion. The first layer, set out in Art. 3 - 5 AMLA, is verification of the identity of the customer, establishing the identity of the beneficial owner and periodic repetition of these two steps. Art. 6 AMLA establishes special duties of due diligence whereby financial intermediaries must clarify the economic background and the purpose of transactions or business relationships as part of a risk-based approach. Financial intermediaries should properly clarify any indications and suspicions and only submit a SAR to MROS under Art. 9 AMLA if their clarifications prove unsuccessful, or if suspicions cannot be allayed and reasonable suspicion has been established. This 'screening programme'

⁹⁶ See MROS Annual Report 2023, Chapter 2.3.

requires financial intermediaries to take the time needed to thoroughly clarify the situation. The required effort varies from case to case, depending on the level of risk, the specific circumstances and the complexity of the business relationship. Financial intermediaries also need a certain amount of leeway in their choice of clarification methods and the time required for such clarification. For this reason, the correct or appropriate length of time that clarifications may take cannot be determined schematically – it always depends on the specific individual case. However, the aim of the clarifications must be for the financial intermediary to be able to get to the bottom of the matter and form a well-founded opinion.

The content of SARs and underlying clarifications must be of a certain quality in order for MROS to properly prepare and process them. Rudimentary clarifications or even entirely unsubstantiated claims make analysis difficult, if not impossible. Such SARs clog up the information system and unnecessarily tie up resources at MROS. They adversely affect SAR processing efficiency and thus weaken the AML system as a whole.

With the introduction of the risk-based approach, MROS has moved away from the traditional processing approach of 'one incoming SAR equates to one case forwarded to the prosecution authorities' and is focusing instead on 'intelligence' and the collation of information. Analysis no longer revolves around the SAR as such, but rather on the information that it contains.⁹⁶ And here, a solid factual basis and the most thorough clarification possible are the key factors. In terms of effectiveness, these factors play a more important role than the time factor. Prompt reporting must not take precedence over thorough clarification.

The completeness of SARs is just as important as thorough clarification. MROS continues to receive a large number of SARs containing insufficient or incomplete data. These SARs have to be returned to the financial intermediary for correction, unless MROS staff are able to manually correct them. This puts a further strain on MROS resources.⁹⁷ Rejection of a SAR means that it cannot be processed.

⁹⁷ See MROS Annual Report 2023. Chapter 3.

MROS sends financial intermediaries a confirmation of receipt under Art. 4 MROSO only after it has received a complete and correct SAR.

MROS requires financial intermediaries to conduct thorough clarification and provide complete and structured documentation in their SARs. This is crucial for effective SAR processing and supporting the prosecuting authorities in the fight against money laundering.

5.2 Interpretation of Art. 11a AMLA – Reasons for requests for information

Art. 11a AMLA allows MROS to request information from financial intermediaries if the analysis of SARs submitted under Art. 9 AMLA or Art. 305ter para. 2 SCC or information received from a foreign FIU indicates that the financial intermediaries in question were involved in transactions or business relationships relating to the matter. MROS information requests to these financial intermediaries are intended, on the one hand, to place incoming SARs within a broader context and , on the other hand, to provide foreign FIUs with the information necessary to combat money laundering and terrorist financing (see MROS Annual Report 2023, Section 6.1). This ability to obtain information is one of the most important tools that MROS has in the fight against money laundering and terrorist financing.

MROS receives a considerable amount of personal and financial data in the SARs submitted under Art. 9 AMLA or Art. 305^{ter} para. 2 SCC or in the information supplied by foreign FIUs. In some cases, the data is particularly sensitive. MROS is legally bound by data protection regulations. This applies in particular to the disclosure of information presented and shared in information requests to financial intermediaries based on Art. 11a AMLA.

The Swiss legal system has a number of safeguards in place to protect the confidentiality of data and in particular of information contained in SARs. The most important of these is Art. 320 SCC, which has to do with the breach of official secrecy. In addition, Art. 9 and 10*a* AMLA stipulate that SARs submitted to MROS must be handled in strict confidence and that financial intermediaries must keep secret information about suspicious transactions in order not to jeopardise possible investigations.

Under AMLA provisions, MROS is not permitted to provide financial intermediaries with any justification for its information requests. Consequently, MROS cannot disclose the reasons for its analysis (or suspicions held) nor indicate the possible connection between the client and the SAR. This is also to prevent financial intermediaries from cherry-picking information, since they are required by law to disclose all information that MROS requests (see MROS Annual Report 2023, Section 6.1).

For this reason, MROS does not provide financial intermediaries with any reasons for its information requests. MROS only requests and discloses information about the business relationship that enables the financial intermediary to identify the business relationship or the account holder. This includes, for example, the account number, IBAN or name.

MROS information requests do not contain any explanations as to why or in what context the information is requested. Giving reasons could lead to the financial intermediaries concerned becoming aware of the context of an analysis being carried out by MROS and thus create a risk of collusion or concealment. By submitting an information request under Art. 11*a* para. 2 and 2^{bis} AMLA, MROS already implicitly discloses that it is conducting analysis of a financial intermediary's clients. The financial intermediaries can therefore reasonably assume that a SAR has been submitted or that a request from a foreign FIU has been made regarding the client in question. Beyond this, MROS is not permitted to share any information with the financial intermediaries; this would constitute a breach of official secrecy.

5.3 Duty to report vs right to report

The Swiss reporting system recognises two reporting regimes: the right to report under Art. 305^{ter} para. 2 SCC and the duty to report under Art. 9 AMLA. The right to report, which has been in force since 1 August 1994, was introduced so that financial intermediaries would have a legal basis for re-

porting suspicions without breaching official secrecy obligations. The duty to report was introduced with enactment of the AMLA on 1 April 1998.

The necessity of maintaining two different reporting regimes was called into question early on when the AMLA came into force. The issue was once again raised with the drafting of the SIF Bill98 and introduction of Art. 9 para. 1quater AMLA, which legally defined and anchored reasonable grounds for suspicion as the trigger for the duty to report. The Federal Council proposed that the right to report be eliminated, leaving only a duty to report. In its explanatory report on the consultation draft,99 the Federal Council argued that there were practically no cases in which the right to report under Art. 305ter para. 2 SCC applies. In previous court rulings, 'right to report' cases have largely been found to fall under the 'duty to report' regime. Moreover, the consequences of a SAR under Art. 9 AMLA and Art. 305ter para. 2 SCC are identical: the assets are not automatically frozen. Even when MROS forwards a case to the prosecution authorities, the two types of SAR have the same consequences: the assets entrusted to the reporting institution are frozen for five days.

During consultation on the SIF Bill, the financial sector strongly criticised removal of the right to report. It expressed concern that employees of financial intermediaries would be increasingly exposed to the risk of criminal liability for violating bank-client confidentiality.¹⁰⁰ Art. 305ter para. 2 SCC and Art. 11 AMLA actually provide adequate legal protection, which should allay such concerns. Nevertheless, this criticism was enough to prevent elimination of the right to report. The Federal Council Dispatch explained that the right to report is subsidiary to the duty to report. Even when exercising the right to report, financial intermediaries are still bound by the special duties of due diligence set out in Art. 6 para. 2 AMLA. The right to report cannot be used to report cases to MROS without prior clarification. With the newly created Art. 9 para. 1quater AMLA and the resulting broad interpretation of 'reasonable grounds to suspect', the Federal Council concluded that the number of 'right to report' SARs would diminish over time in favour of 'duty to report' SARs.¹⁰¹

The statistics (see 3.4) seem to confirm this as the volume of 'right to report' SARs fell sharply in 2023, followed by a slight decrease in 2024. This once again begs the question: is the coexistence of the 'right to report' and 'duty to report' still justified?

In its analysis, MROS draws no distinction between 'right to report' and 'duty to report' SARs. However, it has noticed that some 'right to report' SARs from financial intermediaries are less thoroughly clarified and that the information provided in those reports is not enough to corroborate suspicions. MROS would like to remind reporting financial institutions that the right to report does not release them from their due diligence obligations.

5.4 Definition of the term 'prosecution authority'

MROS forwards cases to the competent prosecution authorities in accordance with Art. 23 para. 4 AMLA if it has reasonable grounds for suspicion based on its analysis of one or more SARs. Depending on the circumstances, MROS will either notify a cantonal public prosecutor's office or the Office of the Attorney General of Switzerland. Other authorities considered as prosecution authorities include the Federal Criminal Police, the cantonal police or authorities that have a criminal law service and also combat predicate offences within the meaning of the AMLA. In line with current MROS practice, however, this information is only forwarded to these other prosecuting authorities as spontaneous information reports for administrative assistance. The question therefore arises as to whether MROS, in addition to providing spontaneous information

⁹⁸ AS 2021 656, see also <u>Federal Council Dispatch of 26 June 2019 on Amendments to the Anti-Money Laundering Act</u>, BBI 2019 5451, 5477 ff.

⁹⁹ Änderung des Bundesgesetzes über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung – Erläuternder Bericht zur Vernehmlassungsvorlage.

¹⁰⁰ See Ergebnisbericht zur Vernehmlassung zur Änderung des Bundesgesetzes über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Gelwäschereigesetz) vom 26. Juni 2019, no. 8.1.1.

¹⁰¹ Federal Council Dispatch of 26 June 2019 on Amendments to the Anti-Money Laundering Act, BBI 2019 5451, 5479.

reports, should also forward specific cases within the meaning of Art. 23 para. 4 AMLA to these other prosecuting authorities in selected instances.

Art. 12 of the Criminal Procedure Code (CrimPC)¹⁰² lists the public prosecutor's office, the police and authorities responsible for prosecuting contraventions as prosecution authorities. While the latter are not involved in the fight against money laundering or its predicate offences, the same does not apply to the police, which have the authority to independently launch investigations, whether on their own initiative or in response to a report (Art. 15 para. 2 CrimPC).

The organisation of the federal prosecution authorities is governed by the Federal Act on the Organisation of Federal Criminal Justice Authorities (CJAA)¹⁰³. Art. 2 CJAA describes federal prosecution authorities as the police and Office of the Attorney General of Switzerland. Art. 4 CJAA defines the police as (a) Federal Criminal Police, (b) other units of the Federal Office of Police, to the extent that they are permitted by federal law to carry out criminal prosecution tasks, (c) other federal authorities, to the extent that they are permitted by federal law to carry out criminal prosecution tasks, and (d) cantonal police forces, which, in cooperation with federal prosecution authorities, carry out criminal prosecution tasks. In the area of administrative criminal law in particular, several federal offices are responsible for prosecuting criminal offences (including felonies that constitute a predicate offence to money laundering).

MROS is therefore authorised to forward cases under Art. 23 AMLA to a much broader range of authorities than simply cantonal public prosecutor's offices and the Office of the Attorney General of Switzerland. MROS thus reserves the right to forward cases to the police or administrative criminal authorities in the future. However, MROS will consult the authorities concerned in advance. The authority concerned must note that forwarding a case will result in the assets being frozen. If the authority wishes to uphold the asset freeze, it must issue an order to that effect within five working days (Art. 10 para. 2 AMLA).

¹⁰² Swiss Criminal Procedure Code (Criminal Procedure Code, CrimPC), SR 312.0.

¹⁰³ Federal Act on the Organisation of Federal Criminal Justice Authorities (CJAA), SR 173.71.

6 International cooperation in the fight against money laundering

6.1 Egmont Group

In 2024, the Egmont Group¹⁰⁴, a global network of FIUs, carried out several important activities designed to reinforce international efforts to combat money laundering and terrorist financing.

The 24th annual working and regional group meetings were held in St Julian's, Malta, at the end of January 2024. Over 400 representatives of FIUs, international partners and observers¹⁰⁵ took part. The meetings focused on implementation of the 2022 – 27 strategy and identifying potential support for FIUs in the area of training and technical infrastructure. Participants also discussed new technologies used by criminals and the importance of improving information sharing between FIUs.¹⁰⁶

The 30th annual Egmont Group Plenary took place in Paris from 2 to 7 June 2024. The event was hosted by the French FIU (Tracfin). Some 400 representatives of FIUs and observers were in attendance. High-level speakers, including the French Economy Minister Bruno Le Maire and the then FATF President T. Raja Kumar from Singapore, opened the discussions. The Plenary focused in particular on one topic: 'The next generation FIU'. FIUs are not only confronted with technological and staffing challenges (see 2.4). Criminal networks are working together both more frequently and more effectively, using new technologies. Generally speaking, they are better equipped in terms of resources and IT than many FIUs. This poses ever greater challenges for the global network.107

In order to improve international cooperation, MROS will be playing an even more active role in the work of the Egmont Group over the next two years. MROS' Deputy Head and Head of the International Division was elected Regional Representative for Europe II at the Plenary in Paris for a twoyear term. The members of this region, in addition

to MROS, include, among others, the UK, Monaco, Guernsey, Jersey, Gibraltar, Isle of Man, Israel, Georgia and Ukraine.

6.2 GAFI/FATF

6.2.1 General information

In 2024, the Financial Action Task Force (FATF)¹⁰⁸ reached several important milestones in strengthening efforts in the global fight against money laundering, terrorist and proliferation financing.

In March 2024, the FATF published its risk-based guideline on implementation of Recommendation 25 (Transparency and Beneficial Ownership of Legal Arrangements).¹⁰⁹ Legal entities, trusts and other legal constructs are misused worldwide to obfuscate assets for the purposes of money laundering, terrorist financing, corruption or circumvention of sanctions. This guidance provides countries and the private sector with an understanding of how transparency requirements should be applied to legal arrangements. It contains practical advice on interpreting and assessing the risks associated with legal constructs and trusts. It facilitates detection of criminal actors who attempt to conceal their criminal activities using front companies or other complex structures.

Switzerland is aware of the risks posed by the use of legal structures to conceal the origin of criminal assets. In May 2024, the Federal Council submitted a dispatch to Parliament. The aim is to introduce a federal register (transparency register) in which companies and other legal entities must register their beneficial owners. This register will enable prosecution authorities, in particular, to identify the persons behind a legal structure more quickly and reliably. This will prevent the use of legal entities and trusts in Switzerland for the purposes of monev laundering or concealing assets.¹¹⁰

¹⁰⁴ See MROS Annual Report 2023, Section 7.1.

¹⁰⁵ Observers are not FIUs. They are institutions that are nevertheless given the opportunity to participate in Egmont Group meetings. Examples include Europol, FATF or the World Custom Organization.

¹⁰⁶ Egmont Group, <u>2024 Egmont Group Working and Regional Group Meetings (St. Julian's, Malta</u>), last consulted on 31 January 2025.

¹⁰⁷ Egmont Group, <u>France's Einancial Intelligence Unit (Tracfin) Hosts 400 EG Representatives from Around the Globe</u>, last consulted on 31 January 2025.

¹⁰⁸ Information on the remit and structure of the organisation can be found in the <u>MROS Annual Report 2023</u>, Section 7.2.

¹⁰⁹ FATF, <u>Guidance on Beneficial Ownership and Transparency of Legal Arrangements</u>.

¹¹⁰ Federal Council press release of 22 May 2024: '<u>Bundesrat verabschiedet Botschaft zur Stärkung der Geldwäscherei-Bekämpfung</u>'

The FATF placed Algeria, Angola, Ivory Coast and Lebanon on its grey list in 2024. Senegal was removed from this list.¹¹¹ The FATF publishes its grey list three times a year, drawing attention to countries and territories that have shown deficiencies in their fight against money laundering and terrorist financing. However, these countries are working with the FATF to address the strategic deficiencies in their systems.¹¹²

Finally, the FATF appointed Elisa de Anda Madrazo from Mexico as its new President for the period from 1 July 2024 to 30 June 2026. The new presidency will focus in particular on implementing the risk-based approach, strengthening the global network, implementing FATF standards and promoting financial inclusion.¹¹³

6.2.2 Country evaluation

In October 2024, the FATF concluded the fourth round of mutual country evaluations. This comprehensive, peer-to-peer evaluation analysed the measures taken by over 200 member countries to tackle financial crime, terrorist financing and proliferation. The Mutual Evaluation Reports (MER) analyse the respective progress made by each country, but also reveal their weaknesses. The FATF took stock of the 4th evaluation round and approved adjustments for the 5th evaluation round. These primarily concern the methodology and the mutual evaluation process.

The next round of evaluations will place an even greater emphasis on the effectiveness of defences. The aim is to ensure that countries not only have laws, regulations and guidelines in place, but also implement and enforce them effectively. Moreover, special attention will be paid to the main risks in each country, with more detailed coverage of their specific context. In this manner, the FATF ensures that countries and auditors focus on the highest risk areas. It is comparatively easier to carry out investigations and secure convictions in lower-risk areas. The recommendations made in mutual eval-

uation reports will be more results-oriented in the future, including specific measures and timetables in the fight against money laundering, terrorist financing and proliferation financing. The next round of evaluations will now cover a six-year cycle, which is significantly shorter and more intensive.

With the start of the 5th round of evaluations, Switzerland and thus MROS also began the preparatory work for the evaluation of Switzerland. The State Secretariat for International Finance (SIF) has the lead in coordinating these activities. Preparatory work is not limited to the authorities, but also includes the private sector and, in particular, financial intermediaries. They are an important part of the evaluation, as they represent the 'first line of defence' in the fight against money laundering and terrorist financing.

In the future, Switzerland will also dispatch assessors to evaluate other countries. In order to accomplish this challenging task effectively, Switzerland sends assessors in so-called Joint Assessor Training (JAT) sessions, which are held several times each year, to receive training. Participants include government officials from individual member countries.

6.3 Taskforces

For years, MROS has been actively involved in several operational and strategic task forces. In early 2022, it joined the Russia-Related Illicit Finance and Sanctions FIU Working Group (RRIFS)¹¹⁴; by the end of 2023, it had also joined the Counter Terrorist Financing Taskforce Israel (CTFTI).¹¹⁵ Information on the objectives and activities of these taskforces can be found in the 2023 annual report. Several task force meetings were held in 2024. For each of these two task forces, MROS hosted the meeting once.

¹¹¹ FATF publication of 25 October 2024: 'Outcomes FATF Plenary, 23 – 25 October 2024'.

¹¹² FATF publication, <u>'Black and grey' lists</u>, last consulted on 31 January 2025.

¹¹³ FATF publication, <u>Objectives for the FATF during the Mexican Presidency (2024 – 2026), last consulted on 31 January 2025.</u>

¹¹⁴ Financial Crimes Enforcement Network (FinCen), Russia-Related Illicit Finance and Sanctions FIU Working Group (RRIFS Task Force), last consulted on 31 January 2025.

¹¹⁵ Financial Crimes Enforcement Network (FinCen), Counter Terrorist Financing Taskforce – Israel (CTFTI Task Force), last consulted on 31 January 2025.

6.4 Bilateral meetings

MROS is committed to efficient and smooth cooperation with foreign partner FIUs. Knowledge of the existing limits and legal leeway when obtaining relevant information from the respective partner authorities is not only important for the expeditious clarification of facts, but also for the efficient use of staff resources. Bilateral meetings serve as a strategic means of sharing ideas on how to optimise cooperation, particularly in relation to organised crime and terrorist financing. The technical possibilities for data exchange and the constantly growing information flow are topics that affect all FIUs and were therefore discussed in detail.

In 2024, several bilateral meetings took place, including with the FIUs from France (Tracfin), USA (FinCEN), Italy (UIF), Moldova, Montenegro, Austria (A-FIU), Hongkong (JFIU), Luxembourg (CRF) and Germany.

At the end of September, MROS hosted the threeday Quad Island Forum meeting (new: Quad Forum).¹¹⁶ Among other things, participants discussed the importance of cooperation among authorities and with the private sector. Building on the meeting between MROS and the Quad Forum meeting in London in 2022, MROS presented the Swiss FIP-PP, which had been announced there and was implemented in 2024. The technical challenges and increasing amounts of data were also discussed. A fruitful exchange took place with the World Economic Forum¹¹⁷ and the Wolfsberg Group.¹¹⁸ Additional guests included the FIU from Luxembourg (Cellule de Renseignement Financier [CRF]) and the FIU from Monaco (AMSF - Autorité Monégasque de Sécurité Financière).

The Netherlands hosted the German-speaking FIU meeting in May. Here, too, one of the key topics was how to deal with the exorbitant increase in data volumes, which contrasts with the limited personnel and technical resources. The upcoming FATF country evaluation was also discussed.

During the Egmont Plenary Meeting held in Paris in July, MROS signed a Memorandum of Understanding with the FIUs from the United Arab Emirates (UAE) and Colombia aimed at further strengthening cooperation.

¹¹⁶ The Quad Island Forum (new: Quad Forum) of Financial Intelligence Units is a strategic alliance of FIUs from Gibraltar, Guernsey, Isle of Man und Jersey.

¹¹⁷ Website The World Economic Forum, last consulted on 31 January 2025.

¹¹⁸ Website The Wolfsberg Group, last consulted on 31 January 2025.

7 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.

MROS consists of six divisions, each assigned to carry out specific tasks. As of 2024, it had an average of 60 employees (51 FTEs).

The organisation chart reflects the current structure of MROS.

Planning and Policy (PuP)

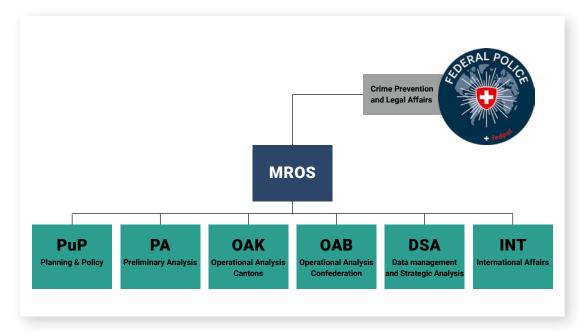
The PuP division is a classic cross-sectional unit and thus deals with complex issues. It focuses on all legal matters as well as policymaking up to the level of the Federal Council (e. g. draft legislation, motions, postulates, etc.). It also monitors and handles projects and publications (incl. annual reports, NRAs, typologies), deals with risk management and serves as the point of contact for all internal and external enquiries regarding formal and substantive aspects. PuP lends support to MROS' operational divisions and ensures unity of doctrine. It 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 SARs in terms of form, technology and content, including manual corrections in case of poor data quality. In addition, it triages SARs, conducts an overall assessment and then passes them to one of the operational divisions or processes and forwards cases directly to a prosecution authority. Furthermore, it is responsible for national administrative assistance under Art. 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 reasonable 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. The cases concern, among other things, criminal offences against property (mainly fraud, embezzlement and criminal mismanagement), human trafficking and forgery.



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 reasonable grounds for suspicion, the aggregated information is usually 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. The cases concern, among other things, international money laundering (mainly bribery of foreign public officials), organised crime, terrorism, stock market offences, right- and left-wing extremism, and the circumvention of sanctions (serious violations of the Embargo Act).

Data Management and Strategic Analysis (DSA)

The DSA division is responsible for the secure operation and development of the MROS information system (goAML). It 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 methods of money laundering.

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 (UNCAC) and the Europol Financial Intelligence Public Private Partnership (EFIPPP).