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 2020

May 2021

Money Laundering Reporting Office Switzerland MROS

Annual Report 2020

May 2021

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

Tel.: (+41) 058 463 40 40
email: mros.info@fedpol.admin.ch

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

Table of Contents

1. Foreword

Once again, 2020 turned out to be a challenging year for the Money Laundering Reporting Office Switzerland MROS. The exceptional situation resulting from the COVID pandemic was mitigated by the introduction of the new goAML information system however. The pandemic has provided criminals with new opportunities for criminal activity and has therefore increased the risk of money laundering, a fact that is reflected in the renewed rise in reporting volume. The 5,334 SARs submitted to MROS in 2020 concerned over 9,000 business relationships – around 25% more than in 2019. Therefore, the rate of increase in 2020 is similar to those in the years 2018 and 2019. In the past year, MROS also processed more than 6,000 SARs submitted since 2016 that were still pending at the end of 2019.

More than 1,000 SARs filed during 2020 concerned suspicions of fraud involving government-backed loans granted by financial institutions. These SARs led to more than 800 notifications to the prosecution authorities, with hundreds of criminal investigations having since been opened. This is reflected in the statistics. Fraud was mentioned as the predicate offence in more than half of the SARs submitted to MROS in 2020 (58%) – a significant increase over 2019 (25%). And, for the first time, transaction monitoring was the main factor arousing financial intermediaries' suspicions and prompting them to submit a SAR.

The new goAML system has become established among financial intermediaries. By December 2020, almost 90% of all SARs to MROS were submitted electronically. This excellent result is thanks to major efforts by financial intermediaries to adapt to the new system. MROS, for its part, devoted substantial resources to supporting financial intermediaries and the authorities in this transition. Nonetheless, MROS still had to correct and tidy up a substantial volume of the data transmitted before conducting its analyses – resources that in future must be spent on analysis. Improvements and modifications of the system are therefore required in order to make full use of the potential offered by submitting SARs electronically.

For the first time, MROS presents thematic typologies intended to draw the attention of financial intermediaries to money laundering, organised crime and terrorism financing risks that are difficult to detect. With this in mind we have chosen specific cases involving terrorism financing, participation in a criminal organisation, human trafficking, money laundering using crypto currency and the risks posed by online identification. The development of strategic analysis and raising awareness among financial intermediaries are key objectives of MROS's new strategy. The electronic processing of SARs offers new opportunities in this respect, which MROS will make even greater use of in the coming years.

A further new feature of the annual report are the statistics on the exchange of information with national authorities. This exchange has taken on a new importance, both in terms of the content of the information and the increased work volume for MROS. The exchange of information

with foreign counterparts also increased again in 2020. In September, the legislature passed an amendment to the Anti-Money Laundering Act of 10 October 1997 (AMLA)[1] granting MROS greater powers in this area. In future the Reporting Office will be able to request information from financial intermediaries – under the provisions of the new Art. 11a para. 2bis AMLA – on business relationships that are the subject of information from a foreign counterpart only. These improvements will help to make the anti-money laundering system in Switzerland more effective.

MROS could not have achieved all this without the efforts of its staff. To them we would like to express our appreciation and thanks.

Bern, May 2021

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

Money Laundering Reporting Office Switzerland
MROS

[1] RS **955.0**

2. MROS given new structure and strategy in 2020–2021

The changes and innovations that took place in 2020 marked a turning point for MROS. On 1 January 2020, the MROS information system, goAML, went online and the revised draft of the Ordinance of 25 August 2004 on the Money Laundering Reporting Office Switzerland (MROSO)[2] came into effect. On the same day, MROS adopted a new strategy aligned with the Counter-Crime Strategy for 2020–2023 adopted by the Federal Department of Justice and Police's (FDJP).[3] Finally, these changes resulted in the internal restructuring of MROS to ensure implementation of goAML and the new MROS strategy (see Chapter 2.3). These interrelated developments stem from the desire to transform MROS into a modern, proactive authority, capable of facing the challenges posed by the constant evolution of the techniques of money laundering and its predicate offences as well as organised crime and terrorism financing.

2.1 A decade of progress in the fight against money laundering, organised crime and terrorism financing

Between 2010 and 2019, the number of business relationships reported by Swiss financial intermediaries to MROS increased sevenfold. The sharing of information with foreign financial intelligence units (FIUs) intensified, and MROS was contacted more frequently by national authorities in the context of mutual administrative assistance. These trends continued in the year under review (see Chapter 4). There is no indication of any change in this trend. Since 2013, MROS has been given additional authority, particularly in the area of information exchange with its foreign counterparts and with financial intermediaries.[4] These powers are set to expand again starting from 1 July of this year (see Chapter 6.2).
Many FIUs have experienced similar developments, each to its own pace and extent. The volume of financial information that they receive is growing; money laundering techniques have evolved, particularly through the use of new technologies (see Chapter 5.5); FIUs are playing a greater role within the anti-money laundering system; their powers have expanded, particularly with regard to information exchange both at national and international levels. The overall improvement of arrangements combating money laundering, its predicate offences, organised crime and the financing of terrorism are behind these developments: the alerts that they produce have become more numerous, but not all alerts make sense to criminal prosecution authorities. The filtering role of FIUs is crucial.
The paradigm in which FIUs operate has changed globally. Over twenty years ago, when international money laundering standards first emerged, the legal framework was intended to enable the identification and seizure of assets derived from criminal activities. Now, legislation is being adapted to enable the authorities to take not just

[2] SR **955.23**

[3] See *Crime Prevention Strategy of FDJP for 2020–2023* (not available in English)

[4] For more details, see the *MROS Annual Report 2013* p. 56 et seqq. This report can be downloaded from the MROS web site.

repressive but also preventive action. The role of the FIUs has evolved accordingly: their mission is not only to identify information useful to the prosecuting authorities, but also to use all the alerts sent by the system combating money laundering, its predicate offences, organised crime and the financing of terrorism to identify their weak points. To this end, they produce strategic analyses to identify methods and trends in these areas and share their findings with financial intermediaries, dealers, third party authorities, policymakers or the interested public ('follow the money').
Over the past decade, MROS resources have increased, but at a rate insufficient to ensure that it is able to continue to pursue its activities using existing methods. The changes made in early 2020 are intended to reflect developments of the past decade in order to better meet future challenges.
The cornerstone of this strategy is the new goAML system, which is capable of digitally processing information reported to MROS. This system also enables fast and secure communication with financial intermediaries and national authorities. It also enables MROS analysts to use the information received without having to go through the time-consuming process of entering data. In addition to efficiency gains, this step towards digitalisation is only one step towards the increased use of artificial intelligence-based applications to analyse large volumes of data ('criminal intelligence-led policing'). Below is an initial assessment of the use of goAML, one year after it was introduced (see Chapter 3).

2.2 MROS 2020–2021 strategy

With the beginning of 2020, MROS adopted a new strategy for the 2020–2021 period. The strategy is based on seven interdependent pillars:

1) Ensuring effective MROS analyses
2) Improving the quality of SARs
3) Reinforcing preventive action against the most serious forms of crime
4) Providing optimal support to prosecuting authorities
5) Intensifying effective international collaboration
6) Developing MROS technical capacities
7) Ensuring that MROS staff members regularly deepen and update their knowledge.

The first objective of this strategy is to ensure that the information that reaches MROS is processed more effectively. This requires rapid sorting – adequately determining the type of analysis required – in order to optimally allocate MROS resources. Ultimately, this sorting process also requires the use of artificial intelligence tools, which enable rapid identification of the salient features of a given SAR or whether it relates to other ongoing cases, for example. Since 1 January 2020, this sorting process has determined the depth of MROS analysis (e.g. the number and type of verifications to be carried out by staff). Sorting takes into account the key features of the given SAR (e.g. the complexity of the reported facts), the priorities set forth in the FDJP's Counter-Crime Prevention Strategy for 2020–2023 and the needs of prosecution authorities. The sorting process is also based on internal prioritisation criteria.
Since 1 January 2020, major efforts have been made to ensure that the MROS analysis best matches the needs of criminal prosecution authorities. Regular exchanges with MROS partners have taken place on this subject. The new information system allows MROS to deliver information from SARs in digital form. In addition, minor cases can be handled quickly and MROS internal processes have been redesigned to reduce resource load.
The second objective of this strategy is to give greater importance to preventive action in MROS activities. The aim here is to improve strategic analysis of risks, trends and methods of money laundering or terrorism financing and to share findings with financial intermediaries, dealers or the authorities concerned, e.g. as part of the national risk assessment process conducted under the aegis of the Interdepartmental Coordinating Group on Combating Money Laundering and the Financing of Terrorism (CGMT). This work will continue in 2021.
Implementation of this strategy implies closer exchanges between MROS and its partners, whether they be national or international author-

ities, international organisations (primarily the Financial Action Task Force (FATF) and the Egmont Group), or the private sector. The quality of the information exchanged with foreign counterparts must be improved and the new powers given to MROS will contribute to this. Cooperation with financial intermediaries must be institutionalised through a public-private partnership to enable financial intermediaries to better detect risks and suspicious transactions, to produce high-quality SARs and to act preventively ('public-private partnership').

2.3 The new organisation of MROS

In 2019, the Federal Council authorised twelve additional full-time positions at MROS. As of 31 December 2020, MROS had 57 occupied positions, corresponding to a total of 48.8 full-time equivalents (FTEs), of which 10.3 FTEs were on fixed-term contracts. Implementation of the MROS 2020–2021 strategy required restructuring this fedpol division. Since 1 January 2020, MROS has therefore been subdivided into six sectors, each with its own specific tasks. There are three sectors responsible for preliminary and operational analysis of incoming SARs. The 'Preliminary Analysis' sector receives information and coordinates the SARs sorting and allocation process. It also handles cases that require rapid analysis. The two other sectors carry out a more in-depth analysis of cases falling under cantonal jurisdiction ('Operational Analysis Cantons' sector) or under federal jurisdiction ('Operational Analysis Confederation' sector). The other three sectors at MROS are: the 'International Affairs' sector, which shares information with foreign partners and handles the work relating to MROS involvement with international organisations (FATF, Egmont Group); the 'Strategic Analysis' sector, which explores methods and trends in money laundering and performs national risk analysis tasks under MROS authority; and the 'Planning and Policy' sector, which is responsible for handling management support aspects, exchanges with other national authorities and legal processes at MROS.

2.4 Challenges ahead

The year 2020 has been an intense year for MROS. In the first months of the year, priority was given to introducing the new electronic reporting system. This proved to be a wise decision, as goAML enabled MROS activities to be fully operational as early as March, despite the extraordinary circumstances created by the lockdown measures taken in response to the pandemic. However, introduction of the system required several adaptations and the resulting challenges have not all been resolved, particularly in terms of the quality of the information transmitted by financial intermediaries and dealers. This remains a priority area of concern for MROS. Initially, major efforts will be needed. However, over time, SAR processing times will be reduced and the quality of analysis will improve. In 2020, MROS also completed processing over 6,000 business relationships reported to MROS during the 2016–2019 period that were still undergoing analysis by the end of 2019 (see Chapter 4.13). In 2021, MROS will devote most of its attention to implementing the new strategy. Steps will be taken to improve strategic analysis activities and expand information sharing with financial intermediaries.

3. Introduction of new goAML information system

On 1 January 2020, MROS took a vital step towards digitalisation by introducing the goAML information system. The new system enables financial intermediaries, dealers, authorities and organisations (self-regulatory organisations [SROs] and supervisory organisations [SOs]) who are subject to the AMLA to submit SARs to MROS over an online platform. Moreover, it allows MROS to submit analysis reports and their accompanying information and documents electronically, according to Art. 23 para. 4 AMLA to Swiss law enforcement authorities, as well as exchange information under Art. 29 AMLA with other Swiss authorities also in digital form.
Only a few months after its introduction, the goAML web application has proven to be a safe and efficient means of communication between the various partners. Transmitting and processing SARs electronically has led to a drastic reduction in paper and has provided greater possibilities for remote working, which has been extremely useful since the start of the COVID pandemic.
However, the system has also presented MROS with various challenges regarding data transmission. MROS therefore published on 21 July 2020 some adjustments concerning the quantity of transactions submitted electronically.[5] At the latest from 1 April 2021, only suspicious transactions (Art. 3 para. 1 let. h MROSO) should be submitted electronically.
A further difficulty was that submitted data did not always meet the quality criteria (see Chapter 3.5).

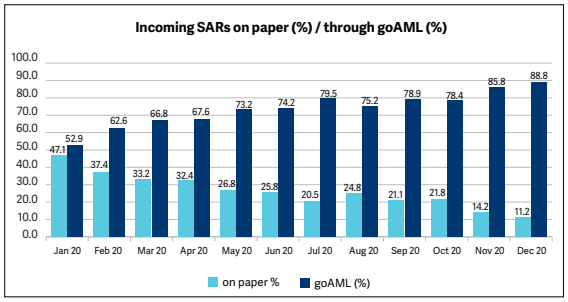
3.1 Number of registered financial intermediaries

Up to 31 December 2020, 728 financial intermediaries comprising 1,494 persons had registered to use goAML. A few financial intermediaries started the registration process portal but did not completed the registration.
Of the 728 financial intermediaries that are registered, only 252 have transmitted a SAR to MROS via goAML so far.

3.2 Proportion of SARs submitted electronically

Since changing to goAML, financial intermediaries have made frequent use of the system. As early as January, more than 50% of SARs were being submitted over the new platform, and this number increased steadily over the following months. By December 2020, the share of SARs transmitted electronically had risen to just below 90%. The following diagram shows the proportion of SARs submitted electronically and on paper:

[5] See *Adjustment to the practice of reporting via goAML* on the MROS website. This publication was replaced by version 2.0 on 30 March 2021 *(Adjustment to the practice of reporting via goAML valid from 01.04.2021).*



During 2020, MROS also used the goAML platform increasingly for information requests to financial intermediaries under Art. 11a AMLA. Financial intermediaries can also use the platform to provide MROS with additional information using a separate type of report. The proportion of documents submitted through goAML by financial intermediaries fulfilling their obligations under Art. 11a AMLA increased from 46% in January to 68% in December. This is a pleasing result and MROS hopes this figure will rise further in 2021.

3.3 Options for submitting SARs via goAML

To meet the needs of financial intermediaries as best as possible, various technical solutions have been developed for submitting electronic SARs to MROS. The goAML system currently provides three options for doing this (see below). Further information and documentation on these different options is available online.[6]

3.3.1 Automatic upload

The automatic generation of a SAR requires the reporting financial intermediary to have an internal IT application that ensures the data from the reporting financial intermediary's system is saved in a clearly structured XML file that is uploaded onto goAML and then transmitted to MROS. Financial intermediaries are responsible for developing their own IT solution for this.

3.3.2 Semi-automatic upload

For the semi-automated option, SARs are entered manually in the goAML application while accounts and transactions are uploaded as an XML file. Any missing information can be added manually afterwards. This option is time-saving for financial intermediaries that do not want to implement an automated solution but that have a large number of transactions to report. It requires transactions in the banking system to be saved locally in a structured and pre-defined format as an XML file and uploaded to goAML.

3.3.3 Manual upload

SARs can also be entered in goAML manually. This option is not subject to any technical requirements besides an internet connection and personal login data. Here, the financial intermediary enters the relevant information manually in the respective field. Depending on the type of SAR, this can be time-consuming however, particularly if many transactions are involved.

3.4 goAML support

The goAML roll-out was accompanied by a user manual providing information on how to submit SARs over the online platform. During the course of 2020, MROS also compiled a list of frequently asked questions[7] from financial intermediaries and updated the goAML manual.[8] Further online documents and a newsletter provide reporting financial intermediaries with information and practical tips on submitting reports. These newsletters are a useful tool for reaching goAML users and MROS therefore plans to publish them more often.

3.4.1 goAML hotline

To provide financial intermediaries, authorities and other users with as much support as possible during the changeover, MROS set up a

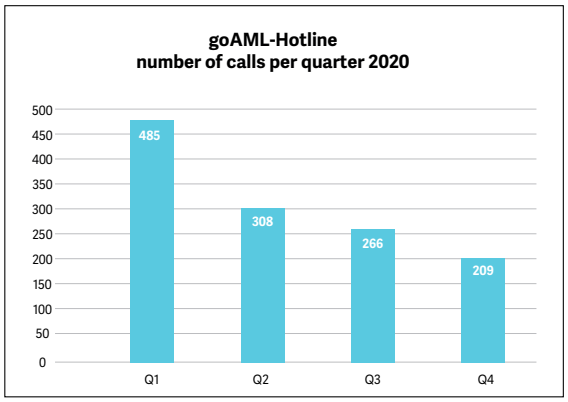
[6] See *Information on the introduction of the new data processing system goAML at MROS* on the MROS website.

[7] See goAML: *Frequently Asked Questions (FAQ)* on the MROS website.

[8] See *goAML web manual* on the MROS website.

goAML telephone and email hotline. The hotline is operated by MROS staff who provide specialised support on registering with the web application, entering a SAR and uploading XML files. The hotline was used by dozens of persons every day during the initial registration period and in the first six months: today, the goAML application is well accepted by many reporting institutions. The positive feedback from financial intermediaries shows that the additional work for MROS, on top of its day-to-day business, has been worth it.

The diagram below shows the number of calls MROS received over the goAML hotline during 2020 – a total of 1,268. In addition, MROS staff answered many further calls to their direct line (for example in response to follow-up questions).



3.5 Quality of incoming data

After introducing goAML, MROS observed that the quality of the data submitted by financial intermediaries was sometimes poor, particularly with respect to the information on transactions. Correcting this shortcoming created a substantial amount of extra work for MROS, who had to clean up the entries – mostly manually – in order to correct the data so that it could be evaluated and used for its analyses. One particular problem was that it was not always clear who and which business relationship the financial intermediary was reporting. MROS has agreed to explain to financial intermediaries what the systematic errors in the programming of their interfaces are in order to reduce the number of reports rejected by the system due to shortcomings in data quality.

The above remarks show how important high-quality data is for MROS and law enforcement authorities. Improving the quality of incoming SARs will ensure that MROS does not have to systematically clean up incorrect data, which would cancel one of the main advantages of the electronic reporting system.

It is important for financial intermediaries to submit correct and valid data so that it can be analysed efficiently and systematically by MROS and the relevant law enforcement authority. When it comes to reporting transactions, it is essential that the basic information provided by the financial intermediary (e.g. personal data on the person concerned, information on the accounts involved, etc.) is correct and complete.

3.6 Outlook

The UNODC ('United Nations Office on Drugs and Crime'), a United Nations office, is the provider of the goAML software, which is already being used by more than 60 countries. The UNODC plans to develop the software further and is currently working to develop functionalities for crypto currencies, entity relationships and politically exposed persons (PEP). This technical advancement of the application is taking place in close collaboration with, and on the request of financial intermediaries that are already using the system. A new goAML version is currently under development.

4. Annual statistics of the Reporting Office

Following the introduction of the goAML, MROS changed the method for counting SARs. Starting from 1 January 2020 the Reporting Office counts the number of reports submitted instead of the number of business relationships reported, as was the case previously. As individual SARs can contain several business relationships, it is difficult to make comparisons with the figures from previous years.

Nevertheless, to give an idea of the chronological progression of the statistics, we have chosen to publish figures in the form of percentages wherever possible. In the 2019 reporting period, each SAR submitted by a financial intermediary involved on average 1.8 business relationships. This average was used to estimate the increase in the number of SARs submitted to MROS in 2020 and to make comparisons where possible with the figures of the previous years.

4.1 Overview of MROS statistics

Summary of reporting year
(1 January – 31 December 2020)

SAR Reporting Volume	2020 Absolute	2020 Relative
Total number of SARs received	**5,334**	**100.0%**
Analysed SARs	4,505	84.5%
SARs still under analysis as of 31 December 2020	829	15.5%
Type of financial intermediary		
Bank	4,773	89.5%
Payment service provider	185	3.5%
Other	121	2.3%
Credit card company	83	1.6%
Asset manager/Investment advisor	45	0.9%
Fiduciary	30	0.6%
Casino	29	0.5%
Insurance	20	0.4%
Loan, leasing and factoring business	19	0.4%
Commodity and precious metal trader	12	0.2%
Attorney	6	0.1%
Trustees	4	0.1%
Currency exchange	3	0.1%
Securities trader	2	0.0%
Self-regulatory organisations (SROs)/FINMA/SFGB	2	0.0%

The table above gives an overview of the SARs received by MROS in 2020 but not of all SARs processed in that year. At the end of 2019, 6,095 business relationships reported between 2016 and 2019 had not yet been processed. Most of them were then processed in 2020 (see Chapter 4.13) but do not appear in this table.

Notifications	1,939	100.0%
To the Office of the Attorney General of Switzerland	175	9.0%
To the cantonal prosecution authorities	1,764	91.0%

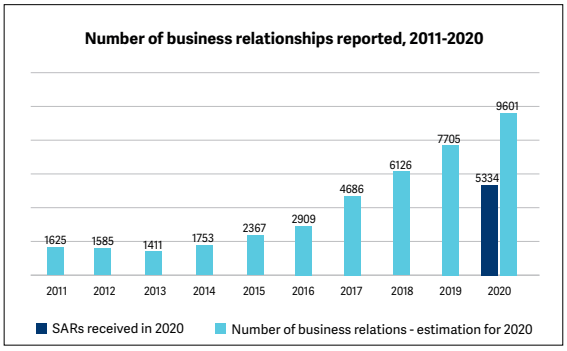
The table above shows the number of notifications made by MROS to the prosecution authorities in 2020. In contrast to the situation up to 2019, notifications no longer comprise the forwarding of SARs to the prosecution authorities after MROS has completed its analysis. Instead, they consist of reports prepared by MROS on the basis of the information at its disposal, of which SARs are the main but not only source. The information contained in a notification to the prosecution authorities may be drawn from different authorities and from several SARs (see Chapter 4.12). In a small number of cases, the notifications submitted in 2020 contained information that had been provided in previous years: this renders it difficult to compare the notifications submitted to the prosecution authorities in 2020 with the number of SARs received in the same period.

4.2 General remarks

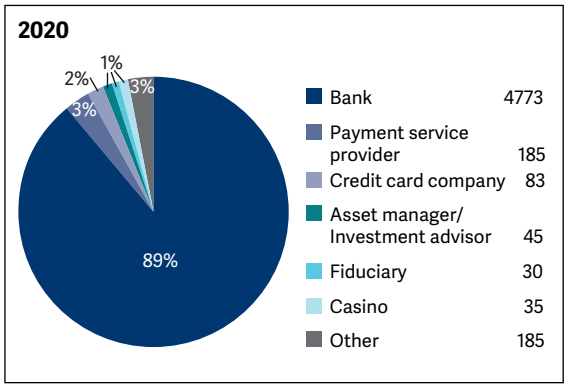
1. In 2019, 7,705 business relationships were reported to MROS. By contrast, the Reporting Office received in 2020 5,334 SARs. Based on the average number of business relationships per SAR reported to MROS by Swiss financial intermediaries in 2019 (i.e. 1.8 business relationships per SAR), the 5,334 SARs received by MROS in 2020 involved approximately 9,601 business relationships. This represents an approximate increase of 25% in the volume of reported business relationships over the previous year (2019: 7,705 business relationships).
2. The increase can be partly explained by the submission of numerous SARs involving fraud or misappropriation in connection with COVID loans.
3. The overwhelming majority of SARs once again came from the banking sector (89.5%), as in the 2019 reporting period.
4. In 58% of the 2020 SARs, fraud was the suspected predicate offence. Even if it is difficult to make an exact comparison with previous years, this figure clearly places fraud at the top of the predicate offences most suspected by financial intermediaries.
5. For the first time, financial intermediaries mentioned transaction monitoring as the main factor for arousing their suspicion (see Chapter 4.8).

4.3 Suspicious Activity Reports SARs

As the method of counting SARs changed with the introduction of the goAML system, MROS has taken the number of SARs submitted in 2020 and multiplied this figure by 1.8 (average number of business relationships per SAR in 2019) as a basis for calculating the business relationships reported, thereby allowing a comparison of the 2020 figures with previous years. It is therefore estimated that the 5,334 SARs received by MROS in 2020 correspond to 9,601 business relationships – an increase of almost 25% over the 2019 reporting period. This indicates a continuation in the upward trend of reporting volume observed since 2015.



4.4 Category of reporting financial intermediary by sector (in %)



- Nearly 90% of SARs were submitted by the banking sector.
- Compared with previous years, the distribution of reporting by the various categories of financial intermediaries shows a high degree of stability. As in 2019, fiduciaries, asset managers / investment advisors and casinos made up 1% of SARs, while the payment service provider sector fell from 4% to 3%.
- The category 'Other' includes in particular providers of financial services in cryptocurrencies (Virtual Asset Service Providers – VASP).[9] The increase in the number of SARs from this category is influenced partially by the change in the counting method however.

For comparison: 2011 to 2020[10] (in %)

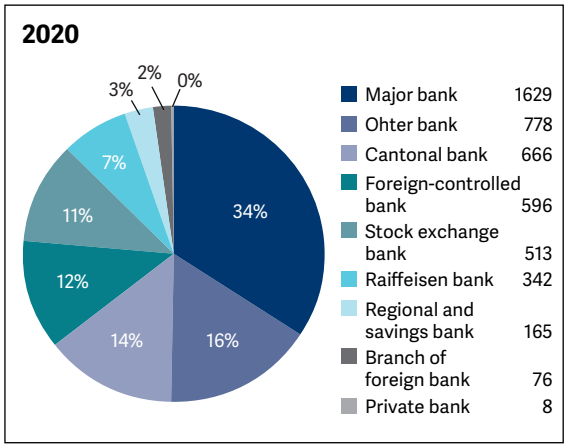
Financial intermediary category	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2020 in absolute numbers	Average 2011–2020
Bank	66.5	66.2	79.6	85.3	91.3	86.0	91.0	88.8	89.9	89.5	4,773	**83.4**
Payment service provider	23.3	22.9	5.2	6.1	2.4	4.4	3.1	4.4	4.0	3.5	185	**7.9**
Other	0.1	0.3	0.1	0.2	0.2	0.7	0.4	2.3	0.6	2.3	121	**0.7**
Credit card	0.6	1.4	1.0	0.5	0.5	0.7	0.3	1.2	1.3	1.6	83	**0.9**
Asset manager / Investment advisor	1.7	3.1	5.2	2.3	1.9	2.2	1.9	1.0	0.9	0.8	45	**2.1**
Fiduciary	3.8	4.1	4.9	2.8	2.0	1.5	1.1	0.7	0.8	0.6	30	**2.2**
Casino	0.4	0.4	0.6	0.5	0.1	0.5	0.6	0.5	0.7	0.5	29	**0.5**
Insurance	0.7	0.6	1.3	0.6	0.5	3.1	0.5	0.6	0.3	0.4	20	**0.9**
Loan, leasing and factoring business	0.3	0.1	0.3	0.2	0.3	0.3	0.3	0.3	0.3	0.4	19	**0.3**
Commodity and precious metal trader	0.1	0.2	0.7	0.2	0.3	0.1	0.2		0.3	0.2	12	**0.2**
Attorney	1.9	0.8	0.6	0.6	0.3	0.2	0.1	0.1	0.1	0.1	6	**0.5**
Trust and loan companies										0.1	4	**0.0**
Currency exchange	0.2									0.1	3	**0.0**
Securities trader	0.0	0.1	0.1	0.6	0.1	0.1	0.3	0.1	0.3	0.0	2	**0.2**
SRO	0.1			0.1					0.1	0.0	2	**0.0**
Foreign exchange trader	0.4		0.4			0.1			0.3	0.0	0	**0.1**
Supervisory authority				0.1							0	**0.0**
Distributor of investment funds							0.1				0	**0.0**
Total	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**5,334**	**100.0**

[9] VASPs include crypto currency trading platforms, wallet providers, financial services providers for issuing, providing and selling virtual assets and other financial intermediation services related to cryptocurrencies.

[10] The absolute figures for 2011-2019 are published in the respective MROS annual reports for the corresponding years. For the sake of completeness, it should be noted that dealers are not included in the statistics, as MROS received only one SAR in 2017 and one in 2019 from this category, corresponding to less than 0.1% of the total of SARs received during these years.

4.5 Types of bank

The diagram below shows the number of SARs submitted to MROS by type of bank.



- The table above shows significant differences compared with 2019. The proportion of reports from private banks, stock exchange banks and foreign-controlled banks has fallen (from 1% to 0%, 25% to 11%, and 27% to 12% respectively), while the proportion of reports from major banks, cantonal banks, Raiffeisen banks and other types of bank has increased (from 28% to 34%, 5% to 14%, 3% to 7%, and 8% to 16% respectively).
- These differences can be explained in part by the fact that the way in which SARs is counted has changed (see Chapters 4 and 4.3). The weight of financial intermediaries who tend to report SARs concerning several business relationships is not as high as it was, since the SARs – and not the business relationships – are considered in the statistics.
- The increase in reports from the cantonal banks (from 5.3% in 2019 to 14.0% in 2020) is partly explained by the large number of SARs relating to COVID loans.

For comparison: 2011 to 2020[11] (in %)

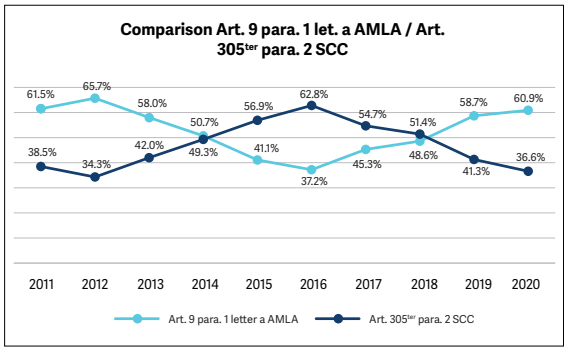
Type of bank[12]	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2020 in absolute numbers	Average 2011–2020
Cantonal bank	6.9	7.6	6.4	5.0	5.8	7.6	5.2	5.5	5.3	14.0	666	**6.9**
Major bank	28.7	29.3	28.9	31.7	35.3	31.1	26.3	26.7	28.2	34.1	1,629	**30.0**
Regional and savings bank	1.4	1.8	0.5	0.9	0.5	1.2	0.6	1.1	1.3	3.5	165	**1.3**
Raiffeisen bank	5.6	6.1	7.0	9.0	5.8	6.2	3.9	3.2	3.1	7.2	342	**5.7**
Stock exchange bank	14.4	12.1	10.2	10.6	14.0	12.4	12.7	20.8	25.1	10.7	513	**14.3**
Other bank	2.5	4.0	20.5	14.3	9.9	12.9	9.6	9.5	8.6	16.3	778	**10.8**
Private bank	2.4	5.7	4.6	2.6	1.8	2.3	1.7	1.9	1.3	0.2	8	**2.5**
Foreign-controlled bank	36.0	33.1	21.4	25.6	26.6	26.3	39.8	31.0	26.9	12.5	596	**27.9**
Branch of foreign bank	1.9	0.2	0.4	0.2	0.3	0.1	0.1	0.3	0.2	1.6	76	**0.5**
Bank with special business clientele	0.1	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0	**0.0**
Total	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**4,773**	**100.0**

[11] The absolute figures for 2011-2019 are published in the respective MROS annual reports for the corresponding years.

[12] The type of bank and the sequence of this table correspond to those of the Swiss National Bank. See the publication *Banks in Switzerland 2019*, p. 9.

4.6 The legal basis of SARs

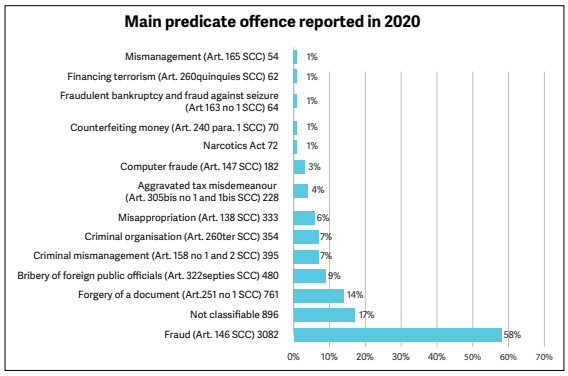
Of the 5,334 SARs received by MROS in 2020, 3,248 (60.9%) were submitted under Art. 9 AMLA (duty to report) and 1,952 (36.6%) under Art. 305ter para. 2 Swiss Criminal Code of 21 December 1937 (SCC)[13] (right to report). A further 129 SARs (2.4%) were submitted under Art. 9 para. 1 let. b AMLA and 2 under Art. 27 para. 4 AMLA.



The relative increase in SARs under Art. 9 para. 1 let. a AMLA observed since 2016 therefore continues. As the vast majority of SARs received by MROS are submitted by the banking sector, the trend is mainly an indicator of the behaviour of this sector. Nevertheless, there is a considerable difference between Swiss banks in terms of the number of SARs they submit under Art. 9 para. 1 let. a AMLA or Art. 305ter para. 2 SCC. The difference depends on the type of institution reporting and is illustrated in the table below.

4.7 Predicate offences

The chart below shows the main predicate offences that were suspected in the SARs submitted in 2020. In contrast to the situation up to 2019, the reporting financial intermediary may now indicate several possible predicate offences in each SAR. As a result, the proportion of predicate offences mentioned in the SARs, when added up, surpasses 100%. A comparison with previous years is therefore biased and is indicative only.



– The noticeable differences between 2020 and the previous years can partially be explained by the fact that financial intermediaries can now choose more than one predicate offence from a general list that has been updated and added to.

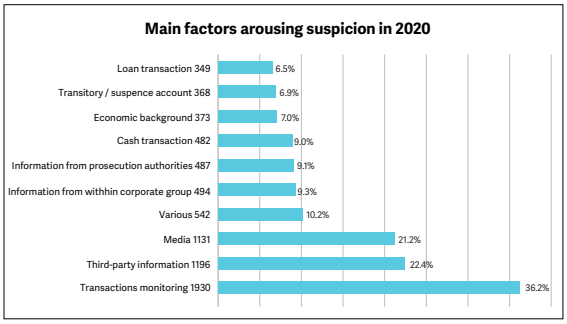
Type of bank	Art. 9 para. 1 let. a AMLA	in %	Art. 305ter para. 2 SCC	in %	Other	in %	Total	in %
Other bank	554	83.1	106	15.9	6	0.9	666	100.0
Foreign-controlled bank	790	48.5	829	50.8	10	0.6	1,629	100.0
Asset management bank	97	58.7	60	36.3	8	4.8	165	100.0
Branch of foreign bank	305	89.1	28	8.1	9	2.6	342	100.0
Major bank	230	44.8	250	48.7	33	6.4	513	100.0
Cantonal bank	663	85.2	101	12.9	14	1.8	778	100.0
Private bank	3	37.5	5	62.5	0	0.0	8	100.0
Raiffeisen bank	301	50.5	269	45.1	26	4.3	596	100.0
Regional and savings bank	12	15.7	64	84.2	0	0.0	76	100.0
Total	**2,955**	**61.9**	**1,712**	**35.8**	**106**	**2.2**	**4,773**	**100.0**

[13] SR **311.0**

– Nonetheless, 2020 saw an explosion in the number of SARs involving suspicions of fraud. In 2018 and 2019, fraud was mentioned as the predicate offence in 20% and 25% of SARs respectively. In 2020, this proportion rose to 58%, a development that can be explained in part by the large number of reports mentioning fraud in connection with COVID loans (see Chapter 5.1).
– The current reporting period saw a significant drop in the number of SARs involving corruption as the predicate offence. The bribery of foreign public officials was mentioned in 480 SARs (9%), the active bribery of Swiss public officials in 21 SARs (0.39%) and the passive bribery of Swiss public officials in 17 SARs (0.32%). These three categories, which appeared in previous reports as a single category, represented 24% of SARs in 2019 and 27% of SARs in 2018.
  It is difficult to interpret the reasons for such variations from one year to the next. The drop in SARs involving corruption can be partly explained by the fact that some complex international cases that in the last years influenced the Swiss financial center and triggered numerous SARs to MROS no longer generated many reports.

4.8 Factors arousing suspicion

The opposite diagram shows what sources triggered financial intermediaries' suspicions, prompting them to submit a SAR in 2020. As with predicate offences and in deviation from past practices, the new goAML system allows financial intermediaries to report more than one factor that aroused their suspicion. As a result, it is possible to calculate what proportion of SARs was triggered by what category of suspicion, but it is no longer possible to make an accurate comparison of these figures with those of previous years.



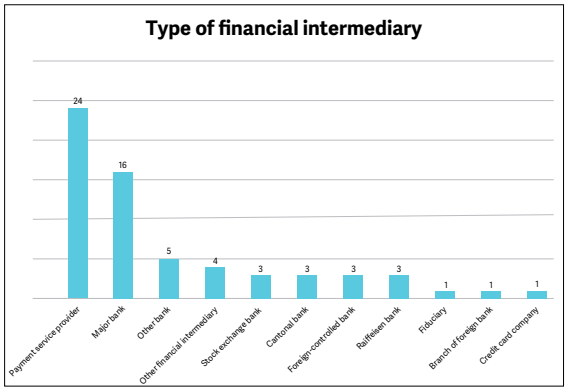
– A comparison of the above figures with previous years, where only one suspicion-arousing factor could be mentioned, is irrelevant.
– For the first time, in 2020, transaction monitoring was the category that aroused the most suspicion and triggered the most SARs (36.2% in 2020 compared with 31% in 2019 and 25% in 2018). This development is a confirmation that financial intermediaries are taking their duties of due diligence under Art. 6 para. 2 AMLA seriously with respect to clarifying the nature of business relationships and the purpose of transactions.
– Information from media reports, which in previous years was the most common factor arousing suspicion, featured less prominently in 2020 (21.2% of SARs compared with 35% in 2019 and 38% in 2018).

4.9 Terrorism financing

During the reporting year, 64 SARs were sent to MROS to report suspicions of terrorism financing and/or violation of the Federal Act of 12 December 2014 on the Proscription of Al-Qaeda, Islamic State and Associated Organisations[14] (i.e. 1.2% of the total number of SARs received). Since it is estimated that there are approximately 1.8 business relationships per SAR, these 64 SARs concern approximately 115 business relationships, roughly the same number as in 2019 (114). The 64 SARs are also linked to other predicate offences, such as membership in a criminal organisation (19 cases), fraud (7 cases) and bribery of foreign public officials (3 cases). In 10 cases, the predicate offences fall under the 'Various' category.

[14] SR **122**

The most frequent factors that financial intermediaries (particularly payment service providers) indicated as justifying their suspicions were transactions monitoring (33 cases), followed by media reports (20 cases), cash transactions (15 cases), third-party information (13 cases), and ties with high-risk countries (8 cases). In 12 cases, the reasons for suspicion fell under the 'Various' category.
Most of the terrorism-related SARs (34) were submitted by banks, followed by payment service providers (24 SARs). Only 6 SARs were sent by other types of financial intermediaries.



Of the 64 SARs concerning suspicions of terrorism, 47 did not lead to a notification by MROS, two were still being analysed by MROS at the end of the reporting year, and the information from the remaining 15 SARs was used to report 14 cases to the competent prosecuting authorities. Criminal proceedings were formally opened in three cases. One of these cases, however, related to human trafficking and not to violations of the Federal Act of 12 December 2014 on the Proscription of Al-Qaeda, Islamic State and Associated Organisations.

4.10 Organised crime

In 2020, MROS received 354 SARs indicating suspected links to a criminal organisation (i.e. 6.6% of the total number of SARs received). While it is not entirely possible to compare figures with those of previous years, for the reasons mentioned earlier, such a percentage indicates an increase compared to 2019, when such suspicions accounted for only 2.4% of the total number of SARs received.
During the reporting year, reports of suspected links to a criminal organisation also mentioned other potential predicate offences: bribery of foreign public officials (111 cases), fraud (72 cases), counterfeiting money (67 cases), forgery of documents (26 cases) and financing of terrorism (23 cases).

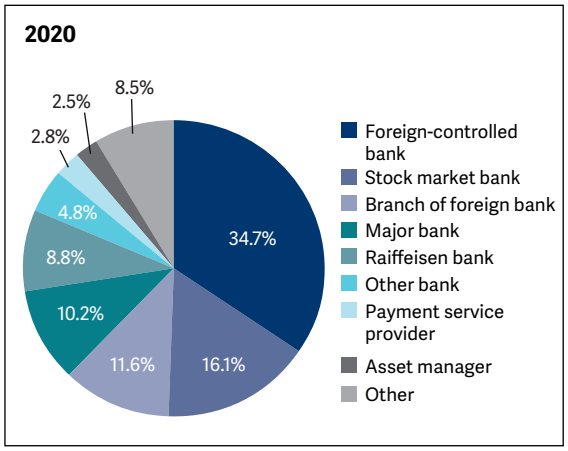
Other predicate offences most frequently mentioned in the SARs related to suspicion on membership in criminal organisations	Number of mentions	in %
Bribery of foreign public officials	111	31.4
Fraud	72	20.3
Counterfeiting money	67	18.9
Document forgery	26	7.3
Terrorism financing	23	6.5
Narcotics Act	20	5.6
Misappropriation	12	3.4
Criminal mismanagement	9	2.5
Extortion	5	1.4
Weapons Act	4	1.1
Theft	2	0.6
Misconduct in public office	2	0.6
Bribery of Swiss public officials/ bribery	1	0.3

During the reporting year, MROS received SARs that included mention of membership in a criminal organisation as reason to report. The reasons for suspicion in these cases were the following:

Main reasons for suspicion	Number of mentions	in %
Media	168	47.5
Transactions monitoring	115	32.5
Cash transaction	82	23.2
Various	76	21.5
Third-party information	42	11.9
Information from within a corporate group	28	7.9
Information from prosecution authorities	20	5.6
Opening of a business authorities	20	5.6
Opening of a business relationship	18	5.1
High-risk country	16	4.5

The vast majority of SARs relating to suspected links to a criminal organisation came from banks

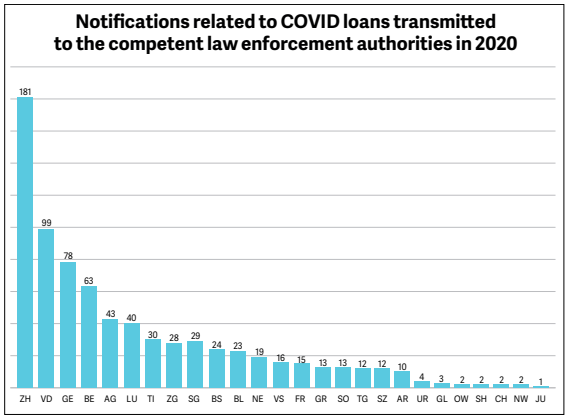
(88.7%), followed by payment service providers (2.82%), asset managers / investment advisors (2.54%) and insurance companies (2.26%). Among the banks, the main types that submitted these SARs were as follows:



256 out of these 354 SARs (73.2%) did not lead to a notification by MROS and 24 are still under analysis. The information provided in the remaining 74 SARs prompted MROS to transmit 46 reports to the competent criminal prosecution authorities. Of these, 8 reports led to no-proceedings orders, while the remaining 38 are still being processed by the competent prosecuting authorities.

4.11 COVID pandemic

The COVID pandemic that marked the year 2020 offered criminals several opportunities for unlawful gain, thus increasing the risks of money laundering. MROS statistics reflect the various types of suspected money laundering that emerged from the SARs sent to MROS during the reporting year (see Chapter 5.1 below), including the misappropriation or fraudulent use of loans granted by Swiss financial institutions under federal guarantee. Between 25 March 2020, when the Federal Council introduced these loans through an Ordinance[15] , and the end of 2020, MROS received 1,046 SARs falling under this category. The SARs related to 1,054 COVID loans granted by 43 different banks, totalling CHF 146,853,347.[16]
In 2020, MROS sent 764 notifications to the criminal prosecution authorities in relation to 914 SARs; 27 reports related to COVID loans were still being analysed at the end of the reporting year. The chart below lists the prosecution authorities that MROS notified and the number of notifications. The resulting reports gave rise to several hundred criminal investigations opened by prosecution authorities. This confirms the pivotal role that MROS played in this unexpected development, particularly considering the scale of the pandemic (see Chapter 5.1 below).



Legend

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

[15] SR **951.261**. This was replaced by the Federal Act of 18 December 2020 on Granting Loans and Guarantees in connection with the Coronavirus Pandemic (COVID-19 Loan Guarantees Act: SR **951.26**).

[16] See the corresponding statistics published on the MROS website: *COVID-19 bridging loans.*

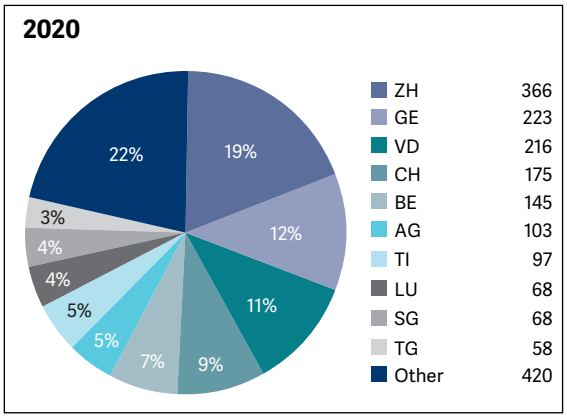
4.12 Notifications to the criminal prosecution authorities

In 2020, MROS submitted 1,939 notifications to the criminal prosecution authorities. Following amendment of the MROSO, MROS will no longer forward SARs directly to the prosecution authorities as it did in the past. In order to ensure the protection of sources – no indication will be made of the identity of the person and reporting entity as such submitting the SAR or information to the criminal prosecution authorities (see Art. 8 para. 1 MROSO).[17] The relevant information and its analysis by MROS are sent electronically to the appropriate public prosecutor's office. Moreover, the notifications transmitted to the criminal prosecution authorities may contain information from different sources or SARs (see Art. 1 para. 2 let. a-e MROSO). Although, in practice, MROS reports always contain information drawn mainly from the SAR submitted, this is no longer the standard rule. It will be the aggregate sum of the information obtained by MROS that will determine the outcome of SAR processing. As already announced in our 2019 Annual Report[18], the 'proportion of SARs forwarded to the prosecution authorities' is no longer a relevant statistic. Indeed, as MROS notifications may contain information from several different sources and SARs, which in some cases may have been received in different years, it is no longer possible to draw a direct comparison between SARs received in a given year.
MROS reports sent to criminal prosecution authorities in 2020 included information from

- 2,156 SARs received in 2020
- 179 business relationships reported in 2019
- 52 business relationships reported in 2018
- 12 business relationships reported in 2017
- 3 business relationships announced in 2016
- 1 business relationship reported in 2014
- 4 business relationships reported in 2011

The statistics on SARs received after 22 November 2019[19] (i.e. 2,235 cases) concern SARs that may relate to several business relationships. Figures for the period prior to that date correspond to only one business relationship.

Prosecution authorities concerned
The chart below shows the cantonal prosecution authorities that MROS sent the 1,939 reports to in 2020.



For statistical reasons and due to change of method for counting SARs, comparison with previous years is not relevant. Since the goAML system was introduced, MROS reports now may contain information taken from several different SARs covering multiple business relationships. At the same time, the information sent to the prosecution authorities may also be taken from sources other than the SARs themselves.
For the first time, the Office of the Attorney General of Switzerland (OAG) was not the most frequent criminal prosecution authority that MROS sent reports to. The OAG received only 9% of the reports made in 2020, compared with 40% in 2019 and 49% in 2018. However, it is important to explain this decrease: in most cases, MROS reports to the OAG concern money laundering

[17] See also *Commentaries on partial revision of the Ordinance of 25 August 2004 on the Money Laundering Reporting Office Switzerland* (MROSO), 24 November 2019 (not available in English), pp. 9–10 and 16.

[18] *See Annual Report MROS 2019,* p. 9.

[19] From this date, MROS started entering incoming SARs in the goAML information system. Of the 179 SARs that MROS received in 2019 and subsequently reported to the criminal prosecution authorities in 2020, 76 were submitted through the goAML system. These 76 SARs related to 153 business relationships, bringing the total number of suspicious business relationships that gave rise to MROS reports in 2020 to 256.

associated with predicate offences committed abroad. They therefore present a higher degree of complexity and the information they contain is more frequently drawn from different SARs concerning several business relationships. In contrast, MROS reports to the cantonal prosecution authorities usually tend to relate only to a single SAR.
In 2020, the number of MROS reports sent to the canton of Zurich criminal prosecution authorities far exceeds the number of MROS reports sent to the canton of Geneva prosecution authorities (19% as opposed to 12%). In the past, MROS reports to the two cantons were roughly the same, and even slightly higher for Geneva than for Zurich.
Also, for the first time more MROS reports were sent to the criminal prosecution authorities of the cantons of Vaud, Bern and Aargau than those sent to the criminal prosecution authorities of the canton of Ticino.
Together, the seventeen other cantons received more MROS reports than Zurich (420 as opposed to 366). This contrasts with the situation up to 2019, when the seventeen or eighteen cantons with the lowest number of MROS reports rarely accounted for more than 15% of the total number of MROS reports.
In addition to the changes introduced by the goAML information system, which complicate comparisons with previous years, the variations observed are also due to the processing of the

For comparison: 2009–2018 (in %)

Authority	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2020 in absolute numbers	Average 2011–2020
ZH	19.7	14.4	18.4	12.4	13.5	12.0	10.2	12.8	14.3	18.9	366	14.7
GE	12.6	15.1	15.0	12.7	8.4	14.9	12.8	14.1	15.0	11.5	223	13.2
VD	4.7	2.1	2.4	2.5	2.6	3.1	1.8	4.3	5.5	11.1	216	4.0
CH	31.9	35.8	34.2	44.7	53.4	38.1	52.6	48.4	39.9	9.0	175	38.8
BE	3.2	3.8	1.6	4.6	1.8	3.0	1.6	1.8	3.3	7.5	145	3.2
AG	3.3	2.0	1.3	1.8	1.5	2.6	1.2	1.6	1.5	5.3	103	2.2
TI	8.5	13.6	12.5	7.3	6.5	6.0	6.0	3.3	3.3	5.0	97	7.2
SG	4.5	2.2	1.7	3.0	2.0	2.2	2.4	1.3	1.2	3.5	68	2.4
LU	0.6	1.1	1.5	1.8	1.0	1.4	1.4	0.8	1.8	3.5	68	1.5
TG	0.6	1.1	0.7	1.1	0.8	1.5	0.7	0.8	1.3	3.0	58	1.2
FR	0.7	1.2	0.5	0.2	0.6	0.6	1.4	1.6	1.5	2.7	53	1.1
VS	0.5	0.4	1.1	1.0	0.5	1.0	1.2	1.4	0.8	2.7	53	1.1
BS	3.4	2.7	2.2	1.2	1.3	3.3	2.0	0.9	0.9	2.6	50	2.0
ZG	1.3	0.6	1.2	1.3	1.5	1.2	0.6	1.9	1.9	2.5	49	1.4
NE	0.7	0.6	0.7	0.9	1.1	0.9	1.0	1.2	1.4	2.3	44	1.1
BL	0.5	1.3	0.8	0.5	1.5	1.5	1.2	0.8	2.9	2.1	41	1.3
SO	0.9	0.1	1.1	0.7	0.4	4.2	0.4	1.1	1.2	1.9	37	1.2
GR	0.5	0.5	0.9	1.0	0.6	0.3	0.5	0.3	0.4	1.5	29	0.7
SZ	0.6	0.6	0.6	0.2	0.5	0.8	0.5	0.3	0.4	1.0	20	0.6
AR	0.1	0.1	0.2	0.2	0.1	0.3	0.2	0.2	0.3	0.6	12	0.2
SH	0.5	0.4	0.6	0.3	0.1	0.5	0.3	0.1	0.3	0.5	10	0.4
UR	0.0	0.0	0.0	0.1	0.0	0.2	0.0	0.0	0.0	0.3	6	0.1
NW	0.3	0.0	0.4	0.1	0.1	0.0	0.0	0.7	0.2	0.3	5	0.2
JU	0.1	0.1	0.2	0.6	0.0	0.3	0.1	0.1	0.1	0.3	5	0.2
GL	0.0	0.0	0.1	0.0	0.0	0.1	0.1	0.2	0.0	0.2	3	0.1
OW	0.1	0.2	0.0	0.0	0.1	0.0	0.0	0.0	0.3	0.2	3	0.1
AI	0.1	0.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0	0.0
Total	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**100.0**	**0**	**100.0**

high number of SARs sent to MROS concerning suspicions related to COVID loans. This partly explains the lower rate of reporting to the OAG, which generally does not have the authority to deal with these types of cases. It also explains why more MROS reports were sent to the cantons of Vaud, Bern and Aargau than to Ticino.

4.13 Processing of SARs from 2016–2019 still under analysis

At the end of 2019, 6,095 business relationships reported to MROS between 2016 and 2019 were still under analysis (10 from 2016, 737 from 2017, 1,717 from 2018 and 3,631 from 2019). During the reporting year, MROS made a special effort to complete analysis of these cases. Most of them were not transmitted (94.5%), while 4.9% of them led to MROS notifications transmitted to the competent criminal prosecution authorities. At the end of 2020, only 37 of these SARs (0.6%) were still under analysis. The table below provides the details, broken down according to the year in which the business relationships were reported to MROS.

Receipt year	2016	2017	2018	2019	Total
Not transmitted	10	730	1,680	3,342	5,762
Notifications		6	34	256	296
SARs still under analysis		1	3	33	37
Total	**10**	**737**	**1,717**	**3,631**	**6,095**

4.14 Information sharing with foreign counterparts

MROS and its foreign counterparts, i.e. other FIUs, may share information through international administrative assistance channels for the purpose of investigating suspected cases of terrorism financing, money laundering and related predicate offences or organised crime. When MROS receives SARs involving foreign natural persons or legal entities, it is able to request information from its counterparts in the countries concerned. The information obtained is important for MROS's analyses, as most SARs received by MROS relate to foreign countries.

In 2020, MROS received 795 information requests from 95 countries, a slight decrease from the previous year (2019: 844 information requests from 103 countries). MROS processed 684 of these requests, i.e. 86%. The average processing time was 41 working days. In addition, MROS also responded to 173 information requests that had been sent to it in 2019.
In 2020, MROS processed a total of 5,212 (2,733 concerning legal entities and 2,479 concerning natural persons) information requests from foreign counterparts. Of that total, 4,169 of these information requests (2,155 concerning legal entities and 1,994 concerning natural persons) were received in 2020.
In some cases, a foreign counterpart will spontaneously provide MROS with information relating to a business relationship in Switzerland. Such information does not require a response from MROS. Likewise, MROS will occasionally also provide information to foreign counterparts that relates to a business relationship in their country. Since 2015, the number of spontaneous reports processed during the reporting year have been shown separately. In 2020, MROS received 504 spontaneous reports from 47 countries and sent 365 spontaneous reports to 76 foreign FIUs.
In 2020, MROS sent 126 information requests to 46 different foreign counterparts. These requests concerned 364 legal entities and 303 natural persons. On average, the FIUs contacted responded to requests within approximately 30 days.

4.15 Information sharing with national authorities

In addition to sharing information with its foreign counterparts, MROS also shares information with other Swiss authorities such as supervisory authorities or other authorities active in the fight against money laundering, predicate offences to money laundering, organised crime or the terrorism financing. MROS is authorised to share information with these authorities under Art. 29 AMLA. No statistics on this information sharing at national level have been published in previous MROS annual reports. However, both the content and volume of inquiries from national authori-

ties has increased to a point where it has had an impact on MROS workload.
In 2020, MROS was contacted 392 times by 26 Swiss authorities requesting information about specific natural persons and legal entities in the context of investigations of possible links to money laundering, organised crime or terrorism financing. In approximately 80% of the cases, these requests came from cantonal police authorities and Federal Judicial Police. These 392 information requests correspond to an increase of more than 200% compared with previous years: in 2018 as in 2019, the number of information requests from other Swiss authorities to MROS amounted to 117.
The role of MROS in relation to the other Swiss authorities involved in the fight against money laundering, predicate offences, organised crime and terrorism financing is not limited to responding to their information requests. As part of its analyses, MROS is also authorised to spontaneously provide information at its disposal to other Swiss authorities involved in the monitoring financial transactions and fighting money laundering, predicate offences to money laundering, organised crime or the terrorism financing. In 2020, MROS transmitted 69 spontaneous reports in this context. In addition, MROS may request information from other federal, cantonal and communal authorities for the purpose of conducting such analyses. These latter requests are not included in the above figures.

5. Typologies – a selection of cases for raising awareness among financial intermediaries

The following typologies are not based on typical SARs from 2020, but on cases that are reported comparatively seldomly, with the exception of the SARs involving COVID (see Chapter 5.1). In 2020, for example, only 7.8% of the total number of SARs submitted to MROS involved criminal organisations and terrorism financing – two of several types of crime that are the focus of the FDJP's Crime Prevention Strategy 2020–2023. Those typologies show how the proceeds from suspected crime are laundered. The cases chosen reflect new trends in money laundering and illustrate the methods used. They also allow corresponding conclusions to be drawn. The typologies serve both as reference cases for research purposes and as important tools for raising financial intermediaries' awareness about what kinds of accounts, financial instruments and patterns of behaviour require greater attention based on the risks identified by MROS.

5.1 Cases involving the COVID pandemic

A major reason for the increase in reporting volume in 2020 was the increase in SARs involving the COVID pandemic: almost one third of the SARs submitted concerned this subject. The particular situation created by the pandemic has provided criminals with new opportunities for criminal activity and has hence increased the risk of money laundering. The global threat from money laundering, criminal organisations and terrorism financing has many facets[20]: with respect to COVID this threat includes the misappropriation of funds granted by the state or supranational bodies for fighting the pandemic, the rise in cybercrime as more people work from home, new scams involving the sale of health equipment, and the infiltration of illegal assets into economic sectors in financial difficulty. By way of prevention, MROS therefore informed Swiss financial intermediaries on 2 and 29 April 2020 – via goAML – of the risks arising from the pandemic, in particular involving COVID loans. The coronavirus-related SARs exposed three specific money laundering risks arising from the pandemic. The first concerns the misappropriation or misuse of loans granted to companies and guaranteed by the Swiss authorities. On 25 March 2020, the Federal Council adopted an emergency Ordinance on the granting of loans by credit institutions (banks) to companies on facilitated terms and guaranteed by the Confederation.[21] The Ordinance was replaced on 19 December by the Federal Act of 18 December 2020 on Granting Loans and Guarantees in connection with the Coronavirus Pandemic (COVID-19 Loan Guarantees Act).[22] The risk of these loans being misused is obvious. In the course of the year MROS received over 1,000 SARs involving more

[20] As early as spring 2020, several national and international organisations published analyses and warnings on this subject. For example, see the FATF analysis (www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html) published in May 2020 and updated in December.

[21] See footnote 15

[22] See footnote 15

than 1,100 loans[23] from financial intermediaries who had been alerted by the withdrawal or transfer to personal accounts of money granted under emergency assistance, by noticeably greater levels of turnover or by the use of loans in contravention of the terms prescribed by the Federal Ordinance. MROS made 800 notifications to law enforcement authorities, in particular for suspected fraud, document forgery and misappropriation. Several hundreds of criminal investigations were opened based on these notifications.

A further criminal activity that has been amplified by the pandemic are online scams involving 'phishing and social engineering'. Predicate offences of this kind are not intrinsically linked to COVID but have become more widespread owing to lockdown measures in numerous countries: these measures have driven many vulnerable people who would normally stay away from the internet into the arms of online scammers. A rise in such cases – evident in most countries – led to a slight increase in the number of SARs to MROS involving this type of fraud.

While the sums of money involved in such online scams are generally modest, this is not the case with the trade in health care products and protective equipment, which often generates millions of francs. Mass orders by state authorities and private companies at the outset of the pandemic for emergency equipment such as face masks, disinfectant and other protective equipment prompted cases of abuse and fraud. Some of the equipment sold was unusable, of poor quality, or overpriced. In some cases, the equipment did not even exist. The fear of catching coronavirus also prompted many people to procure their own material, often on the internet. A few dozen SARs involved fraudulent advertisements extolling the merits of particular medicines supposedly effective against infection, with the suspected fraud more often being committed abroad than in Switzerland. The main causes for suspicion were dubious sales contracts, the sudden change in the business field of a company that had not previously sold health care products or equipment, a suspicious increase in the number of middlemen between the supplier and the purchaser, press articles on companies charging inflated prices for equipment, and requests by aggrieved customers to their bank for a refund of the money paid.

Alleged money laundering in connection with selling health care equipment

A financial intermediary received three transfers from a third country for several tens of millions of francs through a business relationship opened in the name of a domiciliary company in a Pacific jurisdiction active in the field of asset management. The domiciliary company in question belonged to a European national active in the mining industry in a Gulf state. The funds represented the sale of 10 million medical masks ordered by a country and came from an account opened in the name of a government agency. The financial intermediary's client was supposedly acting as an intermediary between the country ordering the masks and the foreign suppliers. Some of the money paid into the account was transferred a short time later to various bank accounts opened in the country that acted as purchaser. The financial intermediary identified several inconsistencies between the information obtained from its client and the situation in the country in question, giving rise to doubt about the credibility of the transactions. The financial intermediary therefore suspected fraud or the mismanagement of public funds. Enquiries made by MROS revealed that, despite its unusual nature, the purchase in question had been duly authorised and that the masks ordered had indeed been delivered. The FIU of the country in which the masks had been ordered was informed about the unusual nature of the transaction.

Besides the above-mentioned examples of coronavirus-related risks, which were identified from the SARs submitted to MROS, other serious pandemic-related risks exist whose gravity was not reflected in the number of SARs. One risk in

[23] See the statistics on the MROS website: *COVID-19 bridging loans.*

particular involves criminal organisations that are taking advantage of the pandemic and its economic consequences to extend their influence, for example by buying up Swiss companies that have run into debt or by purchasing real estate from legal entities or natural persons that have become financially strapped during the crisis. While the growing risk of criminal organisations infiltrating the economy has been reported by several international bodies and documented in numerous investigations by journalists, MROS has only received two SARs relating to this subject. It should be noted, however, that some of the reported cases of loan fraud appear to have been committed by individuals cooperating with each other, or at least using the same modus operandi. At his stage, however, MROS has no indication that known criminal organisations are involved in such schemes.

COVID loan to a company owned by a member of a criminal organisation?
A financial intermediary noticed through an open business relationship with a company which was active in the field of vehicle maintenance and repair and which had applied for a COVID loan that a private loan had been repaid. This violates the provisions of Art. 2 para. 2 let. b COVID-19 Loan Guarantees Act. On conducting further enquiries, the financial intermediary came across media reports referring to the arrest of the owner of the company in a third country for belonging to a criminal organisation. The business relationship in question mainly showed cash transactions with third accounts opened in the country in which the company owner had been arrested. The sums involved amounted to several tens of thousands of francs.

5.2 Criminal organisations

Reports submitted to MROS involving criminal organisations show that most financial intermediaries are prompted to report their suspicions as a result of press reports or entries in private databases.
Often, the bank accounts of members of criminal organisations do not reveal any suspicious transactions or obvious patterns and are therefore not reported. There are probably various reasons why financial intermediaries have difficulty in identifying members of criminal organisations as defined in Art. 260ter SCC. Not only do these criminals move money around in cash, but transactions often remain below a certain threshold and are therefore inconspicuous. Moreover, the companies reported are frequently active in sectors where cash transactions are not unusual (e.g. catering or car workshops). However, also other sectors (e.g. intermediation in the real estate industry, construction sector) may be affected.

Cash transactions and membership in a criminal organisation
In 2020 a financial intermediary reported two credit card applications under the provisions of Art. 9 para. 1 let. b AMLA (attempted money laundering). The reports were based on an entry in the World Check database indicating that one of the applicants was a member of the criminal organisation 'Ndrangheta. The credit cards were supposed to be issued for the same company account – an ice-cream parlour. Both applicants resided in a Swiss canton, but the company was domiciled in a border canton.
The contents of the report led MROS to request further information under Art. 11a para. 2 and 3 AMLA on both persons' bank accounts and on the bank account of the company. As a result of this request, the financial intermediary from whom MROS had requested information also submitted a SAR based on publicly available information and the request from MROS.
The MROS analysis revealed the following about the bank accounts:
80% of the transactions comprised cash deposits of an unusually high frequency; the owners of the companies and the contracting parties were Italian nationals; and 80%

of the business conducted through the bank accounts comprised transactions to and from Italy. MROS also discovered that 60% of this business had links to Calabria or Naples. On analysing the ice-cream parlour's bank statements MROS further established that the company was probably not operative. According to the owner, the company had repositioned itself during the pandemic to become a restaurant.

As the case study above shows, there are elements that when considered cumulatively may indicate that a bank account is being used for illegal funds. In particular, the combination of cash transactions, non-operative companies and certain other risk factors (such as the links to Calabria in Italy in this case) can be an indication that accounts are possibly being used by members of criminal organisations and should therefore be investigated.

5.3 The financing of terrorism

The appeal of crypto currencies to finance terrorism

A financial intermediary provided its clients with a Crypto ATM service. The service enabled clients to make a deposit in Swiss francs at an ATM, which the financial intermediary subsequently exchanged for bitcoins. For this exchange, the financial intermediary cooperated with a south European trading platform for crypto currencies. The platform notified the financial intermediary that a transaction for BTC 0.00897707 (CHF 100) was made from Switzerland to a bitcoin address associated with Al Qaeda. The address was being investigated by a prosecution service in a third country.

The person who made the transaction and was the subject of the report to MROS was able to remain anonymous through using the Crypto ATM service, since just a contact record had to be indicated. However, MROS was able to identify this person: investigations revealed that four years previously the same person had attracted attention on social media for sharing violent jihadist propaganda.

Besides the said transaction, the MROS analysis showed a further 17 transactions for nearly CHF 3,000 to the same bitcoin address. A blockchain analysis tool revealed that the address belonged to the Al Qaeda Bitcoin Transfer Office.

This case is good example of how terrorist groups use new technologies for generating funds. Monitoring and tracing crypto transactions, and carrying out the relevant enquiries under Art. 6 para. 2 AMLA are one of the financial intermediary's key tasks. The case also shows that a single contact record enabled MROS to identify the relevant connections.

Focusing on the individuals who make transactions and receive funds instead of on the amounts transferred

A financial intermediary licensed in Switzerland received information from a foreign prosecution service via its parent company that certain persons were effecting transactions through the financial intermediary to finance terrorism. The work of MROS was significantly helped by the financial intermediary's well-documented analysis of the transactions and persons involved. The SAR also contained the names of the beneficiaries of the funds, which provided MROS with further clues. The analysis showed that two persons known to be associated with violent Islamic circles – one of whom was related to a Swiss foreign terrorist fighter – were transferring thousands of francs to two south European countries and an Asian country, where the brother of one of the two persons was taking receipt of the money. According to press reports, a further beneficiary had previously been in a conflict region and was convicted by a court after his return.

The above transaction pattern is typical for the two forms of terrorism financing identified by the FATF[24] – forms that have been evident for several years also in Switzerland and that often still go undetected. The first form involves the transfer of funds from a country to extremists – some of whom are known in the media – who either use the money in the receiving country for their living costs or transfer it on, possibly to fund attacks. The second form is the transfer of funds (which may be used to finance extremist attacks) via various countries with the aim of hiding the origin of the money. Switzerland is generally a starting point or stopover in this transaction chain. Such payments are very difficult to detect because the low value of the funds, which are transferred via the payment services sector or from retail accounts, does not arouse suspicion. The main reason for this is that transaction monitoring often focuses on the amount of money transferred. While this may be the right approach for identifying the flow of funds in the context of suspected money laundering activities, terrorism financing can be detected first and foremost by looking more closely at those who make the transactions and receive the funds.

5.4 Human trafficking

Smurfing, prostitution, high-risk countries and detailed information on beneficiaries

Within the space of two months a money services business reported five individual business relationships that showed overlaps in transaction patterns and demographic characteristics (e.g. age, sex, origin, profession) of the persons involved. The cases contained pointers to human trafficking (Art. 182 SCC) and/or encouraging prostitution (Art. 195 SCC).

The five female account holders had made multiple payments of identical amounts to various private individuals in a Caribbean and European country. Presumably the women had taken care to split the individual payments so as not to exceed CHF 5,000 – the amount over which financial intermediaries have a particular obligation of due diligence. There were also similarities with respect to the beneficiaries. The financial intermediary was therefore able to make a clear connection between the various business relationships. In one instance, a payment was made between the reported account holders which was then credited to the same Caribbean country.

Most of the female account holders were prostitutes or had connections to the red-light district. With a few exceptions, all the payments were made from the same branch office located close to a well-known red-light district in Switzerland. The reporting financial intermediary examined and followed the transaction patterns beyond the individual business relationships and discovered significant connections between business relationships that on the surface did not appear to be connected.

The fact that the financial intermediary was able to provide MROS with the names, dates of birth and addresses of all those involved enabled MROS to conduct in-depth and specific enquiries on the persons named in the report. The MROS enquiries confirmed the financial intermediary's suspicions. In particular, detailed information on the beneficiaries abroad allowed MROS to submit specific requests to the relevant foreign FIUs – a vitally important measure when dealing with transnational crime such as human trafficking. Two account holders provided addresses located in a red-light district. Two further addresses provided by the women turned out to be false, providing further evidence that the money transfers were possibly originated from a crime. The countries of origin of some of the account holders, together with other factors, were a further indication that the women were potentially human trafficking victims.

In its analysis the reporting financial intermediary referred to various indicators which according to the 2019 report of the Organization for Security and Co-operation in Europe (OSCE) 'Following

[24] See the FATF publication *Terrorist Financing Risk Assessment Guidance.*

the Money: Compendium of Resources and Step-by-step Guide to Financial Investigations Into Trafficking in Human Beings'[25] point to possible human trafficking activities. These indicators include:

- the use of addresses in known red-light districts or buildings where commercial sex work is known to occur;
- the use of straw persons;
- the use of institutions not belonging to the traditional financial system;
- transfers from different regions to the same persons in countries known to be a high risk for trafficking operations;
- structured transfers (smurfing);
- high and/or frequent expenditure inconsistent with the individual's personal use or stated business (money being used by a third party).

For the complete list of the indicators compiled by the OSCE Office of Special Representative and Co-coordinator for Combating Trafficking in Human Beings and resources for financial investigations, we refer to the said OSCE publication.

5.5 SARs involving Virtual Asset Service Providers (VASPs)

Phishing fraudsters who use Swiss crypto currency trading platforms to launder fraudulently acquired assets

A financial intermediary reported the business account of a Swiss crypto currency trading platform into which various banks had paid around CHF 30,000 of customers' money within a matter of a few days. The customers of these banks had been deceived through fake emails into disclosing their personal ebanking data, a scam known as 'phishing'. As a result, money had been withdrawn from their accounts by unknown third parties. The financial institutions whose customers had been affected by the phishing attack notified the reporting financial intermediary about the criminal origin of the funds. At the same time, the trading platform informed MROS that bitcoins had been purchased on its platform using the stolen money and provided MROS with the bitcoin addresses involved and the IP addresses of the persons who had commissioned the bitcoin purchases. The transactions had been carried out over an Application Programming Interface (API), a software interface made available by the trading platform for its customers on its website. The interface allows customers to conduct simplified and automated buying and selling transactions of up to CHF 5,000 per day without having to provide information on their identity when registering on the platform. For transactions via its API, the platform only required the customer to provide a source of funds account (which is generally under the control of the person authorised to make the transaction) and the crypto currency address to which the purchased crypto currencies were to be transferred. On completion of a purchasing order generated via the software interface, the customer received a reference number which they had to quote when making a bank transfer to the platform's business account. All purchasing orders were made for exactly or just under CHF 5,000 (so-called smurfing tactics) so that the trading platform was not obliged to request further Know-Your-Customer documentation from the person effecting the transaction.

Fraudulently acquired crypto assets laundered over a Swiss crypto currency trading platform

In 2019 a cyber attack was carried out on a foreign crypto currency trading platform. During the attack, crypto assets (F) to the sum of several millions of Swiss francs were stolen. The culprits were suspected of belonging to a group of hackers. To cover their tracks, they exchanged the stolen crypto funds for bitcoins. This method, known as 'chain hopping' (i.e. the exchange of crypto assets from one blockchain to another), makes it difficult to trace the funds, even

[25] See https://www.osce.org/cthb/438323.

using tracing software. The hackers chose global crypto currency trading platforms offering a simplified customer identification procedure that only required the customer to register their email address or telephone number, providing the funds to be exchanged did not exceed a certain value. They divided the stolen assets (F) into smaller amounts and sent them to numerous 'F' addresses (so-called hops) before depositing them for exchange on various trading platforms. This made it difficult to trace the origin of the funds and allowed the hackers to circumvent the trading platforms' early warning system because it was not obvious that the assets were derived from the hacking attack.
In this case, the hackers also misused the API software interface of a Swiss crypto currency trading platform, creating several accounts on the platform and changing the stolen assets (F) into bitcoins while taking care not to exceed the CHF 5,000 limit in order to avoid KYC requirements. The trading platform was now in possession of the stolen crypto assets (F) which, despite the hackers' efforts, were traced back to the cyber attack on the foreign trading platform using tracing software. However, the bitcoins which the crypto currency platform transferred to the hackers for exchange did not show any connection on the bitcoin blockchain to the attack on the foreign trading platform but only to the Swiss trading platform. Once the scam was discovered, the Swiss trading platform stopped further outgoing bitcoin transactions and reported the case to MROS.

More crypto currency trading platforms were hacked in 2019 than ever before.[26] Since crypto currencies such as bitcoin can be transferred across the globe relatively anonymously, the geographical location of the platform is irrelevant – the stolen currency can turn up in a different financial centre within a matter of seconds and be laundered there.
These two cases show how important 'smurfing' and the evasion of identification requirements[27] are with respect to VASPs. Preventing cases like this from occurring requires the use of software to trace transactions. Hackers, for their part, try to evade this 'early warning system' by transferring unlawfully obtained crypto assets to various digital currency addresses before they arrive at the target address. These digital currency addresses are merely used as a stopover (i.e. a 'hop') in the transaction chain: therefore to identify the origin of crypto funds, transactions must be able to be traced back over multiple 'hops'.
These examples illustrate once again how important tracing software is for crypto currency transactions. To enable MROS to conduct its own analyses, financial intermediaries must document the clarifications required under Art. 6 AMLA and the related analysis on tracing crypto transactions (Art. 3 para. 1 let. h MROSO).

5.6 Video and online identification

In March 2016, the Swiss Financial Market Supervisory Authority FINMA published Circular 2016/7 on the due diligence obligations of financial intermediaries when establishing business relationships via digital channels. To take account of technological developments, the Circular on video and online identification was partially revised in 2018[28], and in 2020 FINMA proposed further amendments, which were subject to a consultation until 1 February 2021.[29] Most Swiss banking institutions now offer this option for establishing

[26] See *The 2020 State of Crypto Crime* published by Chainalysis in January 2020. In 2019 there were more incidents involving the hacking of crypto currency trading platforms than in any other year before that (Chainalysis counts 11 cases of hacking in 2019) although the volume of stolen assets was lower than in the previous years (2019: USD 282.6 million; 2018: USD 875.5 million; 2014: USD 483.1 million).

[27] However, under Art. 51a Anti-Money Laundering Ordinance-FINMA of 3 June 2015 (AMLO-FINMA, **SR 955.033.0**), which came into force on 1 January 2021, the limit for crypto currency transactions has been lowered from CHF 5,000 to CHF 1,000, thus implementing the interpretative note to recommendation 15 published by the FATF in mid-2019 with respect to VASPs. Those regulations were also adopted by SRO, whose members can also be providers of cryptocurrencies.

[28] See press release https://www.finma.ch/en/news/2018/07/20180717-mm-video-online-id/

[29] See press release https://www.finma.ch/en/news/2020/11/20201116-mm-online-identifizierung/

a business relationship. Some financial intermediaries, particularly those working in the virtual currency business, make systematic use of this option. The number of cases reported to MROS by financial intermediaries whose suspicions were raised during the process of identifying their customers when opening a digital business relationship is therefore increasing. Almost two-thirds of these cases relate to the use of crypto currencies. A major case announced recently concerned the online identification of potential investors in a case of 'initial coin offering'.[30]
Establishing business relationships through digital channels is not without risk. There are two main ways in which criminals wishing to establish a business relationship online to launder their dirty assets can proceed: they can use either forged or stolen identity documents.[31] Both methods feature frequently in the SARs submitted to MROS, although the use of forged documents predominates – probably because these are easier to identify than stolen ones.
In 2020 MROS received a SAR from a financial intermediary who offered potential customers the option of opening, online, an account by submitting copies of identity documents over the internet. The financial intermediary's suspicions were aroused by open source information accusing customers of defrauding investors in connection with launching technological innovations. While carrying out enquiries, MROS was able to establish that the identity card used by one of the main shareholders of one of the companies holding an account reported by the financial intermediary had been reported stolen three days before the account was opened. Precisely because the use of forged or stolen documents for opening a business relationship online makes it impossible to identify shareholders or the beneficial owners of a business relationship, it is particularly difficult to link suspicious assets to predicate money laundering offences. Cooperation between MROS and the police, and between MROS and foreign FIUs is vital, but the accuracy of information provided by the financial intermediary who submitted the SAR is decisive.

Breakdown of negotiations
A financial intermediary who engaged in trading virtual currency received three applications to open an account on its IT platform on the same day. The financial intermediary noticed that in all three cases the foreign identity document provided by the potential customers showed the same photograph but contained different names and dates of birth. The intermediary subsequently broke off negotiations and carried out further checks on the business relationships of recent clients, reporting its suspicions to MROS under Art. 9 para. 1 let. b AMLA (attempted money laundering). The checks turned up three further clients whose identity documents showed the same photograph. These business relationships were also reported to MROS, whose analysis identified the foreign accounts from which money had been transferred to the accounts held with the financial intermediary for the purpose of buying crypto currency. Based on the information received from the FIU of the foreign country concerned, MROS confirmed that the money transferred to purchase the crypto currency originated from scams committed abroad. Moreover, thanks to the information provided by the financial intermediary who submitted the SAR, MROS was able to provide its foreign counterpart with the IP addresses of the computers from which the transfers had been made. This allowed the foreign FIU concerned to report the perpetrators of the fraud and the subsequent money laundering attempt to the relevant criminal authorities.

In line with the FATF recommendations, several financial intermediaries have taken steps to reduce the risks arising from online identifica-

[30] A fund-raising method that works by issuing digital assets that can be exchanged for crypto money or fiat currency during the start-up phase of a project.

[31] See *Guidance on digital identity,* published in March 2020 by the FATF.

tion by moving away from manual checks by compliant officers and using instead computer programs to check document authenticity, which are more reliable.
On the other hand, MROS receives relatively few SARs following a breakdown in negotiations to open a business relationship. Using forged identity documents could, in our opinion, justify submitting a SAR under Art. 9 para. 1 let. b AMLA.

6. MROS practice

6.1 Transmitting information – not SARs

Following amendment of the MROSO, MROS will no longer forward SARs directly to the prosecution authorities as it did in the past. In order to ensure the protection of sources – no indication will be made of the identity of the person and reporting entity as such submitting the SAR or information to the criminal prosecution authorities (see Art. 8 para. 1 MROSO). The relevant information and its analysis by MROS are sent electronically to the appropriate public prosecutor's office. Moreover, the notifications transmitted to the criminal prosecution authorities may contain information from different sources or SARs (see Art. 1 para. 2 let. a-e MROSO). It will be the aggregate sum of the information obtained by MROS that will determine the outcome of SAR processing. As mentioned before (see Chapter 4.12 above), the 'proportion of SARs forwarded to the prosecution authorities' is no longer a relevant statistic.
The second point to be stressed is related to the first. Once the processing of information from a SAR has been completed, MROS informs the financial intermediaries in connection with Art. 23 para. 5 and para. 6 AMLA whether the information reported has been notified to prosecution authority or not. This information has only two practical functions: In the event of transmission, it obliges the financial intermediaries to freeze the assets of the reported business relationships in accordance with the provisions of Art. 10 AMLA. If the decision is made not to notify a criminal prosecution authority, it enables the financial intermediaries to decide on their own initiative whether to continue the reported business relationship in accordance with the provisions of Art. 30 AMLO-FINMA. As in the past, these decisions do not in any way allow conclusions to be drawn on the lawfulness of the assets stored in the reported business relationship. Decisions by MROS not to notify a case may well be taken after information has been passed on to counterpart FIUs or a national administrative authority, or because important information from the SAR has been reported without the transmission of all the information in the report being justified.

6.2 New powers in connection with Art. 11a para. 2bis AMLA

6.2.1 New Art. 11a para. 2bis AMLA

On 25 September 2020, the Swiss Parliament accepted the 'Federal Decree approving and implementing the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol and on the strengthening of penal standards against terrorism and organised crime'.[32] This decree amends the AMLA, in particular by introducing a new Art. 11a para. 2bis, worded as follows:

[32] BBl **2020** 7651, 7664.

"Where the analysis of information from a foreign counterpart shows that financial intermediaries within the meaning of this Act are involved or have been involved in a transaction or business relationship in connection with such information, the financial intermediaries concerned must provide all relevant information to the Reporting Office at the latter's request, provided that they are in possession of such information."

On 31 March 2021, the Federal Council decreed that these new provisions would come into force on 1 July 2021.[33]
As soon as it comes into force, this amendment to the AMLA will give MROS new powers in the fight against money laundering, predicate offences to money laundering, organised crime and the financing of terrorism. Since 1 November 2013, MROS has been able to request based on a transactional analysis additional information from Swiss financial intermediaries that is necessary for its analyses, in connection with third-party accounts with which transactions have been carried out since the reported business relationship. The legislator's aim was to provide MROS with additional means to deepen its analyses and, under certain conditions, to follow the 'paper trail'. Within a few years, this provision has become cardinal for MROS.
The use of requests for additional information under Art. 11a AMLA, coupled with the possibility for MROS to share information with its foreign counterparts and other national authorities, has indeed improved MROS's analyses and avoided overburdening the prosecuting authorities.
Until now, however, requests under Art. 11a AMLA have been limited to cases where MROS already had a SAR from a Swiss financial intermediary. Consequently, MROS could only make such requests when analysing information from counterpart FIUs to the extent that it was related to financial information reported to MROS by a Swiss financial intermediary. If such information revealed a connection to a SAR, MROS was able to respond. Otherwise, the Reporting Office could not provide financial information to the requesting FIU.
This shortcoming was criticised in the FATF's 2016 evaluation of Switzerland.[34] As a result, Switzerland was rated as only 'partially compliant' (an insufficient rating) with FATF Recommendation 40 ('Other forms of international cooperation') and the effectiveness achieved by Switzerland with respect to the international cooperation was deemed only 'moderate' (also an insufficient rating) for Immediate Outcome 2 ('International cooperation'). Addressing this significant deficiency was therefore one of the eight priority actions recommended for Switzerland by the assessors. The justification for corrective action was the highly internationalised Swiss financial market, among other things.
This unsatisfactory assessment outcome also triggered a compliance procedure against MROS within the Egmont Group, which is the operational exchange forum for FIUs. Under the rules governing implementation of Egmont Group principles, MROS is subject to a monitoring process and is required to report on the measures taken to address the deficiencies identified by the FATF assessment. If Switzerland's legal framework is not adapted within a certain timeframe to address these deficiencies, MROS risks being suspended from the Egmont Group. It should be recalled that foreign links are found in the majority of SARs received by MROS. In such cases, MROS needs to be able to gain access to the information available to Egmont Group FIUs. The new provisions of Art. 11a para. 2bis AMLA should bring MROS in line with international standards and put an end to the Egmont Group's monitoring process of MROS.
Under the new provisions of Art. 11a para. 2bis AMLA, MROS will in the future be able to request information from financial intermediaries on one or more transactions or business relationships reported by another FIU (e.g. through spontaneous information or a request made by a foreign counterpart) even when a Swiss financial intermediary has not submitted a SAR to MROS. Swiss financial intermediaries will also benefit

[33] See press release *Terrorismusbekämpfung: Bundesrat setzt verschärftes Strafrecht in Kraft,* (not available in English).

[34] See *mer-suisse-2016.pdf (fatf-gafi.org).*

from this extension of MROS powers, as MROS will now be able to draw their attention to potential risks on their books that have been ignored so far, thereby increasing the level of security in Switzerland. This improvement in the exchange of information ('financial intelligence') between FIUs will support international mutual assistance and prosecution in criminal matters.

6.2.2 Sharing information with foreign counterparts

International administrative assistance between MROS and its foreign counterparts is regulated by Art. 30–31 AMLA. MROS will therefore continue to share the financial information under the revised Art. 11a para. 2bis AMLA with its foreign counterparts under the same conditions as previously. The Federal Council has had the opportunity to express its views on this matter on several occasions.[35] Before sharing information with a foreign FIU, MROS must first make sure that the requirements of Art. 30 AMLA have been met. These include adherence to the principles of speciality, reciprocity and respect for official secrecy. Requests for information by foreign counterparts must then satisfy the requirements of Art. 31 AMLA. For example, MROS does not accept applications which clearly have no connection with Switzerland ('fishing expeditions'). Nor does it respond to requests that seek to circumvent the international mutual assistance channel in criminal matters. Finally, MROS does not provide information in cases where national interests or Swiss security and public order could be compromised. The information obtained may only be used by the requesting FIU in the context of its analyses relating to money laundering, its predicate offences, organised crime and the financing of terrorism. With the prior consent of MROS, information sent to a foreign FIU may also be passed on to other authorities in the same country. MROS verifies the conditions of Art. 30 para. 4 and 5 AMLA. It should be remembered that the information transmitted can only be used for intelligence gathering purposes and not as evidence, and is only presented in the form of a report (Art. 30 para. 3 AMLA).

6.2.3 Initial practical questions on application of the new Art. 11a para. 2bis AMLA

Entry into force of this new legal provision raises some practical implementation issues for financial intermediaries, which are worth noting here. The rules that financial intermediaries need to adhere to when receiving a request for information based on the new Art. 11a para. 2bis and 3 AMLA are identical to the tried and tested rules that have applied since 2013 for requests based on Art. 11a AMLA.[36] When requesting additional information, MROS uses specially adjusted forms according to Art. 11a para. 1 and para. 2 AMLA respectively. Each form contains a list of the requested documents/information. MROS selects the ones that are relevant to the corresponding legal basis (Art. 11a para. 1 or Art. 11a para. 2 or 2bis AMLA). The content of the form used for applications based on Art. 11a para. 2bis AMLA will be identical to the one used for information requests based on Art. 11a para. 2 AMLA. Intermediaries registered in goAML will receive such information requests through this system and will be asked to use this same channel on the basis of the practice documented in the goAML web manual addressed to them.[37]
It should be recalled that information requests must not result in automatic reporting of suspicions to MROS. The financial intermediary receiving such a request must respond to it. However, it cannot ignore the fact that it is a request from an authority based on suspicions of money laundering, predicate offences to money laundering, organised crime or the financing of terrorism. The

---

[35] See, for example, the Federal Council Dispatch of 14 September 2018 on the federal decree approving and implementing the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol and on improving criminal code provisions against terrorism and organised crime, BBl **2018**, 6541 et seqq. and the Federal Council Dispatch of 27 June 2012 on amendment of the Anti-Money Laundering Act', BBl **2012** 6449, 6487 et seqq.

[36] For more details, see the *MROS Annual Report 2013,* pp. 56 et seqq

[37] See *goAML web manual,* pp. 22 and 47.

financial intermediary must therefore carry out additional clarifications in accordance with Art. 6 AMLA and, in the case of simple or well-founded suspicions, report the case to MROS. If no such suspicion materialises, the financial intermediary will simply provide the information requested by MROS under the aforementioned provision and document these clarifications (see Art. 7 AMLA and Art. 31 AMLO-FINMA).
As was the case previously, a financial intermediary that decides to report a business relationship referred to in an MROS request for information may do so by attaching the required documents and the requested information to its SAR, as long as this is done by the deadline set for responding to the MROS request. This deadline is decided by MROS in accordance with Art. 11a para. 3 AMLA. The contacted financial intermediary will provide MROS with the information at its disposal. As the Federal Council has stated, under Art. 11a AMLA, 'all information in the possession of business entities, provided that these entities fall under Swiss jurisdiction, or information that can be acquired are considered available'.[38]

6.3 Disclosure orders issued by prosecution authorities and duty to report

Do financial intermediaries need to submit a SAR as soon as a prosecuting authority has issued a seizure order? This question is repeatedly put to MROS by financial intermediaries and/or other interested parties.
This issue was already addressed by MROS over ten years ago,[39] and confirmed by the 2018 case law of the Federal Supreme Court.
The Federal Council Dispatch on adoption of the AMLA clarifies the meaning and purpose of the AMLA:
"The main target of this fight is organised crime. It is therefore not only a question of detecting and confiscating the funds in question, but above all of establishing and keeping documents (paper trail) and communicating information (duty to report) enabling those guilty of money laundering to be identified and criminally prosecuted."[40]

AMLA provisions are thus primarily intended to achieve two objectives: the general repression of the offence of money laundering and the criminal prosecution of those accused of this offence. While the freezing and seizure of potentially incriminated assets is certainly an objective, it is not an exclusive or overriding concern. It should therefore be stressed that the objectives of the AMLA are not mutually exclusive. Achievement of the first objective does not necessarily imply achievement of the second. In other words, the two aforementioned objectives are separate goals and must be achieved, certainly as far as possible, in a coordinated manner.
As early as 2007, MROS included the purpose of the AMLA into its administrative practice concerning the obligation to notify financial intermediaries if it received a disclosure and/or seizure order. At the time, MROS stressed that this matter was not to be definitively decided. It must be assessed on a case-by-case basis, taking into account the results of the additional clarifications that the financial intermediary is required to undertake in such cases in accordance with Art. 6 para. 2 AMLA in conjunction with Art. 15 et seqq. of AMLO-FINMA: 'Basically, a disclosure and/or seizure order always sets off an obligation to conduct special inquiries under Art. 6 AMLA. [41]
Financial intermediaries are required to submit a SAR to MROS if the clarifications that they carry out in the wake of a disclosure and/or seizure order bring additional suspicious details to light, both in terms of transactions and the business relationship itself, provided that these details are conclusive enough to form a well-founded

---

38 BBl **2018** 6469, 6543.

39 See Chapter 5.5 'Disclosure orders from law enforcement authorities and mandatory reporting' in the *MROS Annual Report 2007* p. 88 ff. and Chapter 4.1 of the *MROS Annual Report 2017* (p. 57) where the practice published in 2007 was confirmed. See also the MROS practice published at the same place: *Publications of the Money Laundering Reporting Office (MROS).*

40 BBl **1996** III 1057, 1072.

41 See *MROS Annual Report 2007,* p. 84.

suspicion within the meaning of Art. 9 para. 1 let. a AMLA.
This would be the case, for example, if the financial intermediary's clarifications reveal business relationships other than those covered by the disclosure and/or seizure order received. The financial intermediary may come across persons mentioned in the order who are involved as holders, beneficial owners, authorised signatories, controlling owners or principals and beneficiaries of domestic or international transfers. The financial intermediary must achieve the same result and submit a SAR if the transactional analysis of the business relationship affected by the disclosure and/or seizure order indicates the existence of suspicious transactions outside the period of time indicated by the prosecuting authority. We remind, moreover, that the financial intermediary is not bound by the factual circumstances, generally succinct, indicated by the criminal prosecution authority responsible for the disclosure and/or seizure order.
In other words, financial intermediaries are also required to submit a SAR under Art. 9 para. 1 let. a AMLA if the following conditions are met: if the further clarifications under Art. 6 para. 2 AMLA in conjunction with Art. 15 et seqq. AMLO-FINMA reveal additional or new suspicious details in relation to the same or other persons mentioned in the disclosure and/or seizure order; or about persons involved in the business relationship whose assets are subject to seizure; or about persons in other business relationships; and if the details uncovered substantiate a well-founded suspicion. In such cases, the financial intermediary has to submit with the SAR the disclosure and/or seizure order concerned (art. 3 para 1 let. h MROSO).[42] MROS verifies the information and works with the competent criminal prosecution authorities to assess the information received and then decides whether to send the information reported to the competent authorities. In 2020, for example, 9.1% of the financial intermediaries that submitted a SAR to MROS stated that the 'information from the criminal prosecution authorities' had been the reason for suspicion. In most cases, this information is transmitted by MROS to the relevant prosecuting authorities because it can provide additional information that can be useful in the conduct of ongoing criminal proceedings.
On the other hand, if the financial intermediary's duty of clarification does not reveal anything other than what the prosecuting authority has requested in the disclosure and/or seizure order, then the financial intermediary may decide not to submit an additional SAR to MROS. Such a SAR would constitute an unnecessary duplication of effort.
This also applies to a third-party financial intermediary (asset manager / investment advidsor, trustee, etc.) who has been notified by a bank of the existence of a duty to hand over items or assets under Art. 265 Criminal Procedure Code of 5 October 2007 [43] (after the expiry of a possible prohibition to notify), or – under the conditions of Art. 10a para. 3 AMLA – of the fact that a SAR under Art. 9 AMLA has been submitted.
According to the case law of the Federal Supreme Court[44], the duty to report does not end with a case being referred to a prosecuting authority: it 'lasts as long as the assets can be discovered and confiscated'.[45] The opening of an investigation does not yet mean that the conditions for a seizure of incriminated assets have been met. On the other hand, the SAR submitted by the financial intermediary to MROS under Art. 9 AMLA and 3 MROSO can very quickly lead to the temporary freezing of assets on the basis of Art. 10 AMLA. Financial intermediaries are under a specific obligation to report suspicious activity irrespective of possible criminal proceedings. However, when the financial intermediary receives a disclosure and/or seizure order, it undertakes, through proper application of the special duties of due diligence under Art. 6 para. 2 AMLA

---

42 See also *MROS Annual Report 2017* (p. 57) as well as *Commentaries on partial revision of the Ordinance of 25 August 2004 on the Money Laundering Reporting Office Switzerland (MROSO),* 24 November 2019 (not available in English), p. 14 note 37.

43 SR **312.0**

44 See DTF 144 IV 391, points 3.1 and 3.3–3.4; DTF 142 IV 276, point 5.4.2

45 See DTF 144 IV 391, point 3.1

in connection with Art. 15 et seqq. AMLO-FINMA, to discover all potentially incriminating assets still on its books or in connection with business relationships that have now been closed and to identify any other suspicious details. As long as this activity has not been completed, the financial intermediary is not in a position to rule out the existence of a well-founded suspicion.
A SAR submitted to MROS under Art. 9 para. 1 AMLA, followed by a report from MROS to a prosecuting authority under Art. 23 para. 4 AMLA and the resulting *ex lege* freezing of assets (Art. 10 AMLA), is thus the only possible means of ensuring the discovery of these assets so that the competent prosecuting authority can issue a new disclosure and/or seizure order, paving the way for forfeiture if necessary. This SAR also makes it possible to identify and criminally prosecute any other persons guilty of money laundering.

6.4 Receipt of SARs by MROS

MROS also regularly receives submissions that do not satisfy the criteria of a SAR under the AMLA or the Federal Act 18 December 2015 on the Freezing and the Restitution of Illicit Assets held by Foreign Politically Exposed Persons (FIAA)[46] due to a lack of factual and local jurisdiction, and therefore cannot process them.
Those submitting a SAR may be natural or legal persons that are not subject to the AMLA, or institutions that are subject to the AMLA but do not act as financial intermediaries within the meaning of Art. 2 AMLA or as persons and institutions within the meaning of Art. 7 FIAA in the context of the reported facts.
MROS is the only office in Switzerland authorised to receive and process SARs from financial intermediaries, dealers, authorities and organisations under the AMLA in relation to suspicion of money laundering, predicate offences, membership of a criminal organisation and terrorism financing. MROS decides whether the reported information will be transmitted to a prosecution authority (Art. 23 para. 4 AMLA). In addition, MROS receives information from persons and institutions under Art. 7 para. 1 and 2 AMLA and sends the information received to the Federal Department of Foreign Affairs (FDFA) and the Federal Office of Justice (FOJ) (Art. 7 para. 6 AMLA).
If MROS does not accept a SAR due to a lack of factual and local jurisdiction, the information contained therein cannot be processed by MROS and sent to a prosecution authority within the meaning of Art. 23 para. 4 AMLA.
Under the principle of speciality, MROS can only receive and process SARs if it has authority over the subject matter and location.
All other persons (natural or legal) who are not subject to the AMLA and FIAA and who have such suspicions are therefore required to report such matters directly to the prosecution authorities. Usually, criminal complaints are made to the police at the place of residence of the person making the report.
In 2020, MROS received 140 letters from citizens and 8 submissions designated as SARs under Art. 9 AMLA or Art. 305ter SCC, for which it lacked substantive and/or local authority.
Upon receipt of a submission, MROS examines whether it falls in its area of authority *ex officio*. However, it can only summarily examine whether the reporting entity is subject to the AMLA or not. This is particularly because by law MROS does not have the power to decide on the substance of whether or not the reporting entity is subject to the AMLA. This task is largely the responsibility of FINMA, which is also indirectly responsible for SROs and SOs and the entities supervised by them. FINMA also publishes on its website the names of institutions that have a certain form of authorisation.[47] According to Art. 12 AMLA, the responsibility for monitoring compliance with AMLA obligations is shared by FINMA, the Federal Gaming Board (FGB), the intercantonal supervisory and enforcement authority under Art. 105 Gambling Act of 29 Sep-

[46] SR **196.1**

[47] See https://www.finma.ch/en/finma-public/authorised-institutions-individuals-and-products/ and https://www.finma.ch/en/authorisation/self-regulatory-organisations-sros/sro-member-search/

tember 2017[48], i.e. the Swiss Gambling Supervisory Authority (Gespa), or the recognised SROs and authorised SOs. Corresponding information is also published on their respective websites. MROS may also share information with FINMA, the FGB or the Gespa in this regard (see Art. 29 para. 1 AMLA in conjunction with Art. 7 para. 1 let. d MROSO).
When drafting a SAR or registering in the goAML system, information must be provided about the authority or organisation that supervises the financial intermediary pursuant to Art. 12 AMLA or Art. 43a Financial Market Supervision Act of 22 June 2007[49] (see Art. 3 para. 1 let. b MROSO). Also, only summary examination is carried out to determine whether an entity that lacks an official licence in the narrower sense has acted as a financial intermediary, which would place the area of activity beyond the scope of the AMLA as a whole since no official licencing procedure took place. Here too, however, information can be shared with the supervisory authorities under the conditions of Art. 29 para. 1 AMLA.

48 SR **935.51**

49 SR **956.1**

7. Links

7.1 Switzerland

7.1.1 MROS

www.fedpol.admin.ch
Federal Office of Police (fedpol)

www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/geldwaescherei.html
Money Laundering Reporting Office Switzerland (MROS)

www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/geldwaescherei/meldung.html
Information on goAML

7.1.2 Supervisory authorities

www.finma.ch
Swiss Financial Market Supervisory Authority (FINMA)

www.esbk.admin.ch
Federal Gaming Commission (ESBK)

www.gespa.ch
Intercantonal Gaming Supervisory Authority (Gespa)

7.1.3 National associations and organisations

www.swissbanking.org
Swiss Bankers Association

www.abps.ch
Swiss Private Bankers Association

www.afbs.ch
Association of Foreign Banks in Switzerland

www.svv.ch
Swiss Insurance Association (SVV)

www.vsv-asg.ch
Verband Schweizerischer Vermögensverwalter / Swiss Association of Wealth Managers (VSV)

www.sfama.ch
Swiss Funds & Asset Management Association (SFAMA)

www.svig.org
Swiss Association of Investment Companies (SAIC)

7.1.4 Self-regulatory organisations

https://www.aoos.ch/
Schweizerische Aktiengesellschaft für Aufsicht (AOOS)

www.arif.ch
Association Romande des Intermédiaires Financières (ARIF)

http://so-fit.ch/
Organisme de Surveillance pour Intermédiaire Financiers & Trustees (SOFIT)

www.oadfct.ch
Organismo di Autodisciplina dei Fiduciari del Cantone Ticino (OAD FCT)

www.polyreg.ch
PolyReg General Self-regulatory Association

www.sro-sav-snv.ch
Self-regulatory Organization of the Swiss Bar Association and the Swiss Notaries Association (SAVSNV)

www.leasingverband.ch
Association of Swiss Leasing Companies (SLV)

www.sro-treuhandsuisse.ch
SRO Treuhand Suisse

www.vqf.ch
Verein zur Qualitätssicherung von Finanzdienstleistungen
(VQF)

www.sro-svv.ch
Self-regulatory Organisation of the Swiss Insurance Association (SRO SIA)

7.1.5 Supervisory organisations

https://www.aoos.ch/
Schweizerische Aktiengesellschaft für Aufsicht (AOOS)

http://www.fincontrol.ch/
FINcontrol Suisse Ltd

https://osif.ch/
Supervisory Body for Financial Institutes (OSIF)

http://so-fit.ch/
Organisme de Surveillance pour Intermédiaire Financiers & Trustees (SOFIT)

https://osfin.ch/fr/
Organisation de Surveillance Financière (OSFIN)

7.1.6 Further links

www.ezv.admin.ch
Federal Customs Administration

www.snb.ch
Swiss National Bank

www.bundesanwaltschaft.ch
Office of the Attorney General of Switzerland

https://www.seco.admin.ch/seco/en/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/sanktionen-embargos.html
State Secretariat for Economic Affairs (economic sanctions under the Embargo Act)

www.estv.admin.ch
Federal Tax Administration (FTA)

https://www.vbs.admin.ch/de/vbs/organisation/verwaltungseinheiten/nachrichtendienst.html
Federal Intelligence Service (FIS)

www.bstger.ch
Federal Criminal Court

7.2 International

7.2.1 Foreign FIUs

https://www.egmontgroup.org/en/membership/list
List of all Egmont members, partially with link to the website of the corresponding country

7.2.2 International organisations

www.fatf-gafi.org
Financial Action Task Force on Money Laundering (FATF)

www.unodc.org
United Nations Office on Drugs and Crime (UNODC)

www.egmontgroup.org
Egmont Group

www.cfatf-gafic.org
Caribbean Financial Action Task Force (CFATF)

7.2.3 Further links

www.interpol.int
Interpol

www.europol.europa.eu
Europol