Schweizerische Eidgenossen
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

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

Money Laundering Reporting Office Switzerland MROS

Annual Report 2021

May 2022

Money Laundering Reporting Office Switzerland MROS

Annual Report 2021

May 2022

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

In 2021, the Money Laundering Reporting Office (MROS) recorded an increase in the number of suspicious activity reports (SARs) received for the eighth consecutive year. The 5,964 new SARs, involving more than 10,000 business relationships, represent an increase of 12% compared to 2020. This trend once again underlines the need for MROS to continue with its current strategy, relying on greater digitalisation to perform its mandate.

Besides the increase in SARs received, the main trends emerging from the 2021 SARs were not very different from those seen in 2020: fraud remained the most frequently suspected predicate offence; once again, most of the SARs were submitted by the banking sector; and, for the second consecutive year, transaction monitoring was the greatest trigger for suspicion.

These trends can be explained in part by the large number of SARs – albeit fewer than in 2020 – received in connection with suspected fraud related to government-backed loans by financial institutions as a result of the COVID-19 pandemic.

The goAML system is now well established among financial intermediaries. Throughout 2021, MROS continued to devote significant effort to helping them learn to use the system, in particular to improving the quality of the data they transmit to MROS. MROS did this by checking the quality of the data from individual financial intermediaries and providing them with consistent feedback; more than 700 systematic shortcomings were thus corrected. This process is essential in order to ensure that MROS receives good quality data, without which the digital processing and analysis of SARs would be virtually impossible. This support for financial intermediaries will therefore continue in 2022. MROS must be able to provide prosecution authorities with correct and reliable data when it transmits information from SARs.

Last year also saw the entry into force of the amended Anti-Money Laundering Act (AMLA)[1] granting MROS extended competences in the area of cooperation with its foreign counterparts (the new Art. 11a para. 2bis AMLA). Implementing the new provision did not cause any particular difficulties and will make the anti-money laundering system in Switzerland more effective. The Egmont Group has taken note of this development and suspended the procedure opened against MROS for non-compliance with international standards. Further, in March 2021, a new amendment to the AMLA was adopted. It is expected to come into force in 2022 and will lead to changes for both financial intermediaries and MROS, which will be outlined in this report.

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 2022

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

[1] SR **955.0**

2. Main developments and challenges in 2021

Once again, MROS faced significant challenges in 2021. For the eighth consecutive year, the number of SARs rose sharply, by 12% compared to 2020. While this increase is lower than in the last three years, when it averaged around 30%, the long-term trend is clear: the number of SARs submitted to MROS in 2021 was over seven times higher than in 2013. This increase reflects an international trend, with many Financial Intelligence Units (FIUs) experiencing similar developments; it is a result of financial intermediaries' greater awareness of money laundering on the one hand, and the tightening of international standards on the other.
In order to meet the challenges posed by these developments, MROS continued in 2021 to implement the strategy it adopted in 2020.[2] On one hand, by taking advantage of the efficiency gains from the digitalised processing of SARs and, on the other hand, by further developing the criteria for the rapid sorting of SARs and for determining the type of analysis they require. This allows MROS to use its resources where they generate the most added value.

2.1 Positive evaluation of MROS by the Swiss Federal Audit Office

MROS was the subject of an audit by the Swiss Federal Audit Office (SFAO) in 2021.[3] To examine whether MROS is able to fulfil its legal duties, the SFAO conducted numerous interviews with MROS staff, with fedpol employees involved in MROS activities, with national and international partner authorities, and with financial intermediaries.
The audit yielded many positive findings. MROS' strategy strategy was found to be 'ambitious', 'comprehensibly formulated' and 'convincing', and its implementation in terms of goal achievement was rated as good. The SFAO also gave a positive rating to MROS' current structure and judged its processes to be suitable. It further noted the good cooperation with national and international authorities and called for this to be further strengthened. Its comments on the sorting and comprehensive analysis of SARs encourage MROS to continue the efforts of the last three years to improve efficiency, for example by automating certain steps in the processing of reports and by concentrating its resources on priority cases. The SFAO recommendations support these efforts.
In its report, the SFAO criticised that MROS had insufficient data on the money laundering judgements and rulings of the prosecution authorities, in particular when these decisions are linked to a SAR (Art. 29a para. 1 and 2 AMLA[4]). Despite repeated reminders by MROS,[5] this legal provision is still insufficiently applied

---

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

3 See Swiss Federal Audit Office (SFAO): *Audit of the fulfilment of tasks by the Money Laundering Reporting Office Switzerland*, March 2022.

4 SR **955.0**

5 See, for example, the *2009 MROS Annual Report*, p. 78, the *2012 MROS Annual Report*, p. 79, and the *2018 MROS Annual Report*, p. 22.

by the authorities concerned. Moreover, the data entry and processing of these decisions presents MROS with a considerable amount of work (see Chapter 2.4). Efforts should be made in the future to digitalise the processing of this information.

2.2 The use of the new legal provisions under Art. 11a 2bis AMLA

The amended AMLA came into force on 1 July 2021, giving MROS new competences under Art. 11a para. 2bis AMLA.[6] The new provisions allow MROS to request information from Swiss financial intermediaries on one or more transactions or on a business relationship reported by another FIU – for example through a spontaneous information or a request – even in the absence of a SAR. Implementation of this provision has not posed any particular problems.
MROS made use of its new competences between 1 July and 31 December 2021. While requests made under Art. 11a para. 2bis AMLA make financial intermediaries aware of potential risks on their books that they might not otherwise have detected, they also generate significant additional work for MROS and for the requested financial intermediaries. For this reason, and in addition to the applicable legal requirements, MROS limits such requests to cases where they are possible and necessary. In practice this can be difficult, but MROS works with the financial intermediaries to determine what information may be useful. Experience so far has been good, and up to now MROS has not received undue amounts of irrelevant information. These enquiries have also enabled financial intermediaries to fulfil their clarification obligations under Art. 6 para. 2 AMLA, which is triggered by such requests. However, the proportion of responses to an MROS request under Art. 11a AMLA in electronic form, although increasing, remains lower than for SARs, thus generating avoidable additional data entry work. MROS will therefore continue its efforts to encourage financial intermediaries to transmit the required information – particularly transaction data – digitally and in a suitable format whenever possible.

MROS has sometimes been approached by financial intermediaries who have received requests for information under Art. 11a AMLA and who wish to know whether the request sent to them was related to a request from a foreign FIU or to a SAR from a Swiss financial intermediary. MROS is not allowed to disclose to third parties any information that may reveal the existence or absence of a request from a foreign FIU because this would be contrary to the principles of the Egmont Group and to Art. 30 para. 1 AMLA, applied by reciprocity. For this reason, MROS uses similar forms for its information requests, regardless of whether they are made under Art. 11a para. 2 or Art. 11a para. 2bis AMLA.
The introduction of these new competences has strengthened the Swiss anti-money laundering system. The closer cooperation with foreign FIUs should also, in the long run, improve and facilitate international mutual assistance in criminal matters, with initial positive results already having been achieved. Finally, the Egmont Group, the operational exchange forum for FIUs, has acknowledged that the new legal provisions have come into force and has ended the proceedings against MROS for Switzerland's non-compliance with Recommendation 40 of the Financial Action Task Force (FATF) (see Chapter 7.1).

2.3 MROS activities in the Interdepartmental Coordinating Group on Combating Money Laundering and the Financing of Terrorism (CGMF)

The Interdepartmental Coordinating Group on Combating Money Laundering and the Financing of Terrorism (CGMF) was established by the Federal Council in 2013 as a permanent structure with a mandate to coordinate measures and policy related to fighting money laundering and terrorist financing. Under the aegis of the State Secretariat for International Finance (SIF), the CGMF implements FATF Recommendations 1 and 2 on national risk assessment as well as

[6] The new competences were outlined in last year's report. See *2020 MROS Annual Report*, p. 35.

FATF Recommendation 6 on freezing the assets of terrorist persons or organisations. MROS participates in the work of the CGMF and leads the subgroup on risk analysis, contributing to the updated national risk analysis in 2021 and to the publication of the subsequent report.[7] The sectoral analyses carried out within the framework of the CGMF's work make it possible to report on specific risks, trends and methods in the area of money laundering or terrorist financing. A report on risks in connection with the financing of proliferation is currently being prepared jointly with the State Secretariat for Economic Affairs (SECO).
On 17 November 2021, the Federal Council revised the CGMF mandate and appointed MROS, in cooperation with other offices, to evaluate possibilities for developing a public-private partnership project in Switzerland on financial information exchange in the course of 2022. A closer exchange between MROS and its partners – national and international authorities, international organisations and the private sector – aims at improving the identification of money laundering and terrorist financing trends and methods. It should also enable financial intermediaries to better detect suspicious transactions, to provide high-quality SARs and to take preventive action. The mandate of the Federal Council is a step in this direction.

2.4 Providing MROS with the decisions of the prosecution authorities (Art. 29a AMLA)

As mentioned in Chapter 2.1, the SFAO criticised that MROS had insufficient data on the decisions of the prosecution authorities in money laundering matters, in particular when these decisions are linked to a SAR (Art. 29a para. 1 and 2 AMLA).
Art. 29a AMLA was introduced on 1 February 2009 as part of the implementation of the recommendations of the FATF.[8] The article[9] stipulates that the prosecution authorities must provide MROS with judgments and rulings abandoning proceedings connected with Art. 260ter, Art. 260^{quinquies} para. 1, Art. 305bis and Art. 305ter para. 1 of the Swiss Criminal Code (SCC)[10], including the grounds therefor. On one hand, these judgments and rulings provide MROS with an up-to-date picture of the situation regarding money laundering and its predicate offences, organised crime and terrorist financing.[11] On the other hand, their subsequent analysis allows MROS to raise awareness among financial intermediaries in these areas (see Chapter 5.6).
In addition, the prosecution authorities are supposed to provide MROS under Art. 29a para. 2 AMLA with all decisions issued on the basis of a report by MROS. These can include decisions on opening an investigation (Art. 309 para. 3 CrimPC), on extending an investigation (Art. 311 para. 2 CrimPC) or on not proceeding with one (Art. 310 para. 1 CrimPC). This information allows MROS to stay up to date with the progress of proceedings and transmit further information concerning the same case to the public prosecutor's office if necessary. It also allows MROS to assess the quality of its work and keep the relevant statistics.[12] MROS therefore assumes that all decisions issued on the basis of a report it has filed must also be transmitted to MROS.
A statistical overview of the judgments and rulings sent to MROS under Art. 29a para. 2 AMLA is provided in Chapter 4.14 of this report. However, it is not just the strategic aspects or the aim to raise financial intermediaries' awareness that play a role in Art. 29a AMLA. The correct implementation of Art. 30 para. 5 AMLA and Art. 12 para. 2 of the Ordinance of 25 August 2004 on the

---

7 See CGMF: *Second national report on the evaluation of the risks of money laundering and terrorist financing in Switzerland*, October, 2021.

8 See FATF Recommendations: *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations*, March 2022; (BBl **2007** 6269).

9 The wording of paragraph 1 already existed in part in the version of Art. 29 AMLA in force until 1 February 2009 under the provisions on 'cooperation between domestic authorities'. However, it only applied to the cantonal law enforcement authorities.

10 SR **311.0**

11 BBl **2007** 6302

12 BBl **2007** 6302

Money Laundering Reporting Office (MROSO)[13] can also be complicated if MROS does not have information on ongoing criminal proceedings or if obtaining such information would result in a considerable amount of additional work. Under Art. 30 para. 5 AMLA (Cooperation with foreign reporting offices), MROS must obtain the prior consent of the relevant public prosecutor's office before passing on information to a third foreign authority about facts that are the subject of criminal proceedings in Switzerland. Similarly, under Art. 12 para. 2 MROSO (Cooperation with national authorities), MROS is obliged to refer a requesting authority to the Swiss authority if it appears that a prosecution authority is already conducting an investigation against persons mentioned in the request. In order to implement both provisions correctly, MROS relies on the prosecution authorities to provide it with the relevant judgments and rulings.

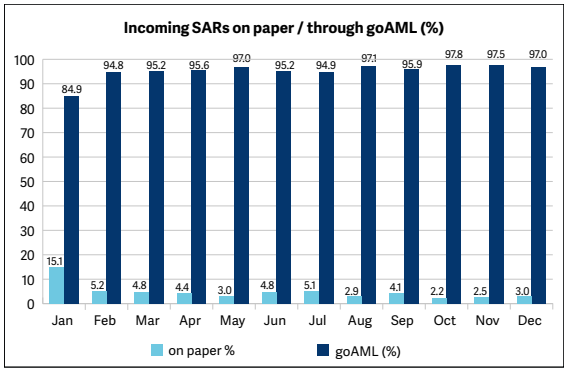
[13] SR **955.23**

3. GoAML information system

Just over two years ago, MROS introduced the goAML information system, a key element in the implementation of MROS's digitalisation strategy and in increasing the efficiency of MROS. The system has proven to be a secure and efficient means of communication between MROS and its counterparts. Not only is the number of SARs submitted to MROS via goAML steadily increasing (see Chapter 3.1), MROS also receives daily requests for administrative assistance and follow-up information on the further processing of reports submitted by MROS to the prosecution authorities via the system. However, further steps are needed to exploit the potential of the system in full. Thanks to the electronic transmission and processing of SARs, the use of paper and the time needed for scanning documents could be drastically reduced. It is also possible to work with the system at any time and from any location, which has been particularly important during the pandemic. Nonetheless, the effort required by MROS to maintain the system is still too high. The efforts to digitally and automatically process and prioritise incoming SARs as well as national and international requests for administrative assistance must be continued.
An important aspect in terms of increasing efficiency is improving the quality of data submitted to MROS. The number of incomplete or incorrect SARs that must subsequently be returned to financial intermediaries for rectification is still too high. The resulting avoidable work for MROS as well as for the financial intermediaries is considerable. In 2021, MROS carried out a systematic data quality check on the financial intermediaries that submit the most reports. 165 SARs were thoroughly checked and more than 700 recurring faults that negatively affect the quality of the data in goAML were identified. The results of this review were discussed with the financial intermediaries concerned and alternative solutions were examined. This review will be continued in 2022 and extended to other financial intermediaries.

3.1 Proportion of electronic SARs

The proportion of SARs submitted electronically was already very high at the end of 2020 (90%). It increased further in 2021, to 95%. MROS is pleased with this result, which has been achieved after only two years of the system coming into operation, and hopes this figure will continue to rise in the coming years. It is only when SARs are transmitted electronically that the full benefits of goAML can be realised (e.g. by automatically linking newly registered accounts, persons and companies with data already known to MROS). In contrast, SARs submitted on paper require much time and effort on the part of MROS to enter and scan. In addition, MROS employees have to manually link this information to the information already in the system, which is very time-consuming.



The steady increase in the number of responses MROS receives to requests for information under Art. 11, para. 1, 2 and 2bis AMLA in electronic form (AIF/AIFT reports) is also encouraging: it rose from 68% at the end of 2020 to 85% at the end of 2021. MROS and the financial intermediaries should endeavour to increase this proportion further in the coming years.

3.2 Fully-automatic upload as an XML file

Of the SARs MROS received via goAML in 2021, more than 60% were transmitted fully automatically via an XML file, compared to 55% in 2020. It is encouraging that in 2021 several financial intermediaries took the decision to develop an IT solution that allows them to transfer their data to MROS automatically by downloading an XML file. Such a solution is also beneficial for information requests sent by MROS under Art. 11a AMLA, since the number of such requests is likely to increase as a result of Art. 11a 2bis AMLA which came into force on 1 July 2021. The significant initial investment made by financial intermediaries wishing to enable the automatic transmission of its data may save a significant amount of additional manual work later on.

3.3 Rejected SARs

When a financial intermediary submits information via goAML, specially trained MROS staff check whether the information submitted meets the legal requirements and the necessary technical criteria. If this is not the case, SARs and information submitted under Art. 11a AMLA are returned to the financial intermediary for correction. Compared with the previous year, the rejection rate for reports submitted to MROS has fallen from 41% (2020) to 24% (2021), but is still too high. In many cases the points raised by MROS do not require much effort on the part of the financial intermediaries to be corrected. However, MROS regularly receives SARs that do not meet the requirements of Art. 3 AMLA nor the technical criteria of goAML.
Before entering a report in goAML, it is essential to read the documents available on the MROS website (manuals, FAQs, fact sheets) and contact MROS if anything is unclear. This can save both financial intermediaries and MROS a great deal of time and effort. An analysis of rejected information showed that information uploaded via XML was rejected far less often than information entered manually: 68% of the information rejected in 2021 had been entered in goAML Web manually. MROS and UNODC, which provides the goAML software, will improve the goAML input masks to make them more intuitive and easier to use.

3.4 Contact with MROS/goAML hotline/ newsletter

The number of calls to the goAML hotline fell significantly in 2021 compared with the previous year. We take this as a sign that the system is user-friendly and works reliably most of the time. Maintenance on the system and brief outages in connection with this maintenance are announced in advance on the goAML website. Before calling the hotline, goAML users should familiarise themselves with the documents available on the MROS website,[14] where goAML manuals, FAQs and instructions on how to file a report via the system are available in four languages.
In 2021, MROS also sent out three newsletters to the financial intermediaries registered in goAML. In these newsletters, MROS addresses general topics related to goAML. It clarifies its practice

[14] See Information on the data processing system goAML at MROS

and deals with legal issues. The usefulness of these newsletters is proven and they will continue to be published in 2022.

3.5 The future of goAML/goAML 5

The goAML system is now used in around 60 countries. The UNODC, which developed the goAML software, continues to improve it. Topics such as virtual currencies, artificial intelligence or machine learning are part of these reflections. A great advantage of the system is the virtual community of goAML users, where countries that use goAML can join forces to jointly discuss necessary developments and improvements. In 2022, a new version of the software (goAML 5) will be released. The new version contains improvements in many areas and is expected to be introduced at MROS in 2023. It will require adaptations by financial intermediaries. MROS will ensure that these changes affect financial intermediaries as little as possible.

3.6 Training of authorities

During the course of 2021, the use of goAML became established not only among financial intermediaries, but also among Swiss prosecution and supervisory authorities. Besides requests for administrative assistance, an increasing number of judgments and rulings under Art. 29a AMLA are being transmitted to MROS via goAML. During the past year, MROS made great efforts to encourage other authorities to register with and use goAML. No fewer than 70 cantonal and federal authorities had responded positively to this call. MROS offered training sessions on how to familiarise themselves with the software, how to transmit administrative assistance requests and decisions under Art. 29a AMLA via the goAML internal messaging system (goAML message board) as well as how to enter administrative assistance requests using a specific type of report. Submitting requests according to report type brings to light the true benefits of goAML: besides reducing the time required by MROS staff to enter the data manually, goAML is able to compare and, if appropriate, link data. In this way, links to existing information can be identified quickly. Around 180 people took part in the 15 training sessions, and dozens of administrative assistance and spontaneous information requests have now been sent using one of the two newly-available channels, i.e. the goAML message board or the specific report type option.

4. Annual MROS statistics

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

4.1 Overview of MROS statistics 2021

Summary of reporting year 2021 (1 January – 31 December 2021)

SAR Reporting Volume	2021 Absolute	2021 Relative
Total number of SARs received	**5,964**	**100.0%**
Analysed SARs	4,884	81.9%
SARs still under analysis as of 31 December 2021	1080	18.1%
Type of financial intermediary		
Bank	5,369	90.0%
Payment service provider	150	2.5%
Other financial intermediary	126	2.1%
Credit card company	103	1.7%
Asset manager/Investment advisor	59	1.0%
Fiduciary	27	0.5%
Casino	32	0.5%
Insurance company	19	0.3%
Loan, leasing and factoring business	15	0.3%
Commodity and precious metal trader	32	0.5%
Attorney	5	0.1%
Trustees	6	0.1%
Currency exchange	7	0.1%
Securities trader	11	0.2%
Self-regulatory organisations (SROs)/FINMA/SFGB/Gespa	3	0.1%

The table above provides an overview of the SARs received by MROS in 2021, but not of all SARs processed in that year. At the end of 2020, 829 SARs were still pending: although they were processed during 2021, they do not appear in the table above (see Chapter 4.13). In addition, 1,080 SARs received in 2021 – and therefore counted in

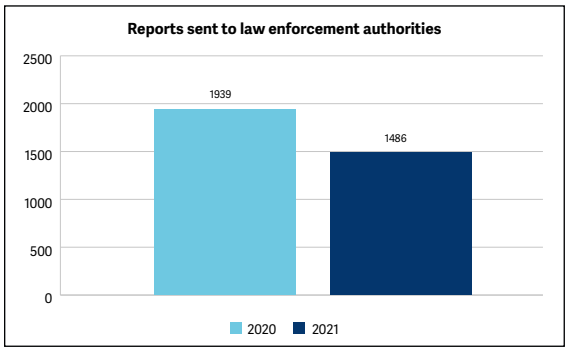
the table above – were still under analysis as of 31 December 2021.
For the second consecutive year and contrary to the practice until 2019, we have not given a quantitative indication of the balances of the reported business relationship's account, primarily because it may differ significantly from the reported suspicious assets. For example, a given client may have several accounts opened with a financial intermediary and totalling a very large sum of money but the SAR only relates to one single suspicious transaction. Moreover, the information provided by a financial intermediary about balances on reported accounts is not consistent and sometimes inaccurate, and their aggregation poses significant methodological problems (e.g. when loans have been granted).

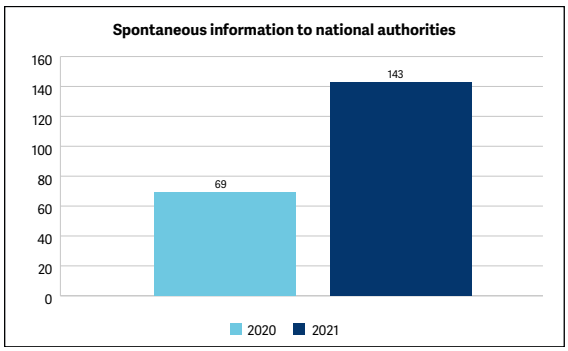
Notifications	1,486	100.0%
To the Office of the Attorney General of Switzerland	135	9.1%
To the cantonal prosecution authorities	1,351	90.9%

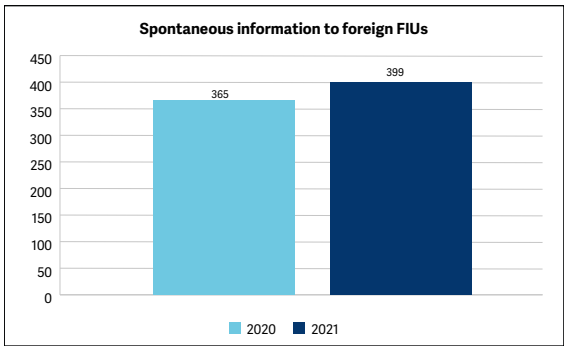
The table above shows the number of notifications made by MROS to the prosecution authorities in 2021. These notifications consist of reports drawn up by MROS on the basis of the information at its disposal, of which SARs are the main but not the only source. The information contained in a notification to the prosecution authorities may be drawn from different authorities and from several SARs, which may not all have been submitted in the same year (see Chapter 4.13). The number of notifications to the prosecution authorities in any given year is therefore not related to the number of SARs received in the same period.

4.2 General remarks

1. In 2021, MROS received 5,964 SARs, an increase of 12% compared to 2020 (5,334 SARs). This increase is about half the increase recorded in 2020 (25%) or 2019 (26%) compared to the previous year.
2. Although MROS received numerous SARs concerning the suspected misappropriation or fraudulent receipt of 'COVID loans' in 2021, the number of such SARs was less than half that of 2020.
3. The overwhelming majority of SARs once again came from the banking sector (90%), as in previous years.
4. MROS sent 1,486 notifications to the prosecution authorities in 2021, 23% fewer than in 2020 (1,939), which illustrates the importance of MROS as a filter. However, this figure should be seen in the context of the 143 spontaneous information reports sent by MROS to other Swiss authorities under Art. 29 AMLA (more than double the number sent in 2020) and the 399 spontaneous information reports sent to its foreign counterparts (a figure that also increased significantly in 2021). In addition to its role as a filter, MROS is increasingly sharing information with national and international authorities responsible for combating money laundering and terrorist financing.



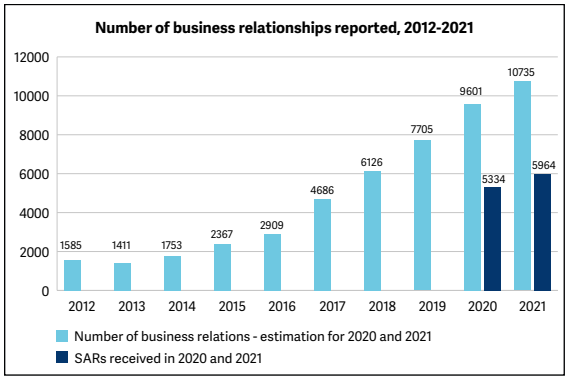




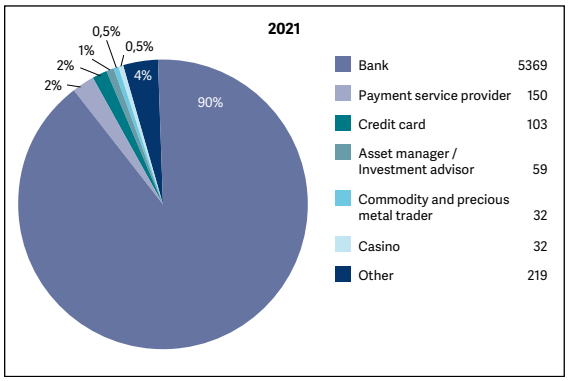
5. Despite the new legal competences granted to MROS in this area as of 1 July 2021, the number of requests for information from foreign FIUs did not increase significantly in 2021. However, these new competences allow MROS to reply in more depth to such requests than in the past. This is reflected in the number of requests based on Art. 11a para. 2 or 2bis AMLA addressed to Swiss financial intermediaries which increased by one third compared to the previous year.

4.3 Suspicious Activity Reports (SARs)

In 2021, MROS received 5,964 SARs, an increase of 12% compared to 2020 (5,334 SARs). This increase is about half the increase recorded in 2020 (25%) or 2019 (26%) compared to the previous year. As the method of counting SARs changed with the introduction of goAML, MROS has taken the number of SARs submitted in 2021 and multiplied this figure by 1.8, i.e. the average number of business relationships per SAR. This is necessary in order to compare the 2021 figures with previous years. The 5,964 SARs submitted in 2021 therefore correspond to 10,735 business relationships.



4.4 Origin of reports categorised by financial intermediary sector



- 90% of SARs were submitted by the banking sector.
- Compared with the previous year, the distribution of reporting by the various categories of financial intermediaries shows a high degree of stability. However, the small relative variation in certain financial intermediary categories compared with the total number of SARs makes it difficult to take into account the relative impact of occasional larger variations, as is the case for asset managers or insurance companies. However, these larger variations are not very significant because they are based on a small number of SARs in absolute terms.

For comparison: 2012 to 2021[15]

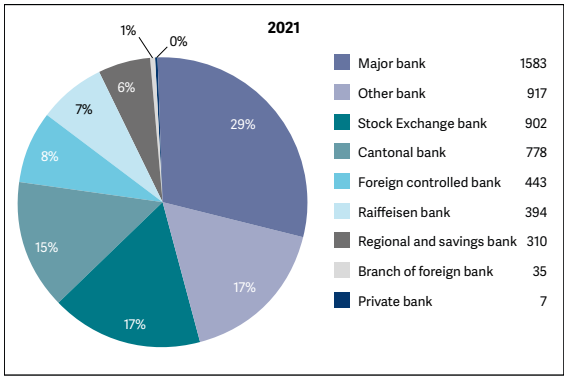
Financial intermediary category	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2021 in absolute numbers	Average 2012–2021
Bank	66.2	79.6	85.3	91.3	86.0	91.0	88.8	89.9	89.5	90	5,369	**85.8%**
Payment service provider	22.9	5.2	6.1	2.4	4.4	3.1	4.4	4.0	3.5	2.5	150	**5.9%**
Other financial intermediary[16]	0.3	0.1	0.2	0.2	0.7	0.4	2.3	0.6	2.3	2.1	126	**0.9%**
Credit card company	1.4	1.0	0.5	0.5	0.7	0.3	1.2	1.3	1.6	1.7	103	**1.0%**
Asset manager	3.1	5.2	2.3	1.9	2.2	1.9	1.0	0.9	0.8	1.0	59	**2.0%**
Casino	0.4	0.6	0.5	0.1	0.5	0.6	0.5	0.7	0.5	0.5	32	**0.5%**
Commodity and precious metal trader	0.2	0.7	0.2	0.3	0.1	0.2		0.3	0.2	0.5	32	**0.3%**
Fiduciary	4.1	4.9	2.8	2.0	1.5	1.1	0.7	0.8	0.6	0.5	27	**1.9%**
Insurance	0.6	1.3	0.6	0.5	3.1	0.5	0.6	0.3	0.4	0.3	19	**0.8%**
Loan, leasing and factoring business	0.1	0.3	0.2	0.3	0.3	0.3	0.3	0.3	0.4	0.3	15	**0.3%**
Securities trader	0.1	0.1	0.6	0.1	0.1	0.3	0.1	0.3	0.0	0.2	11	**0.2%**
Currency exchange									0.1	0.1	7	**0.1%**
Trust and loan companies									0.1	0.1	6	**0.0%**
Attorney	0.8	0.6	0.6	0.3	0.2	0.1	0.1	0.1	0.1	0.1	5	**0.3%**
Supervisory authority (FINMA/ESBK/Gespa)			0.1							0.1	3	**0.0%**
Foreign exchange trader		0.4			0.1			0.3	0.0		0	**0.2%**
SRO			0.1					0.1	0.0		0	**0.1%**
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**	**5,964**	**100%**

[15] The absolute figures for 2012–2020 are published in the respective MROS annual reports.

[16] The category 'other financial intermediary' includes virtual asset service providers (VASP). VASPs include crypto exchanges, wallet providers, financial service providers related to the issuance, offer and sale of virtual assets and other business models.

4.5 Types of banks

The diagram below shows the number of SARs submitted to MROS by type of bank.[17]



For comparison: 2012 to 2021[18]

Type of bank	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2021 in absolute numbers	Average 2012–2021
Cantonal bank	7.6%	6.4%	5.0%	5.8%	7.6%	5.2%	5.5%	5.3%	14.0%	14.5%	778	**7.7%**
Major bank	29.3%	28.9%	31.7%	35.3%	31.1%	26.3%	26.7%	28.2%	34.1%	29.5%	1,583	**30.1%**
Regional and savings bank	1.8%	0.5%	0.9%	0.5%	1.2%	0.6%	1.1%	1.3%	3.5%	5.8%	310	**1.7%**
Raiffeisen bank	6.1%	7.0%	9.0%	5.8%	6.2%	3.9%	3.2%	3.1%	7.2%	7.3%	394	**5.9%**
Stock exchange bank	12.1%	10.2%	10.6%	14.0%	12.4%	12.7%	20.8%	25.1%	10.7%	16.8%	902	**14.5%**
Other bank	4.0%	20.5%	14.3%	9.9%	12.9%	9.6%	9.5%	8.6%	16.3%	17.1%	917	**12.3%**
Private bank	5.7%	4.6%	2.6%	1.8%	2.3%	1.7%	1.9%	1.3%	0.2%	0.1%	7	**2.2%**
Foreign-controlled bank	33.1%	21.4%	25.6%	26.6%	26.3%	39.8%	31.0%	26.9%	12.5%	8.3%	443	**25.2%**
Branch of foreign bank	0.2%	0.4%	0.2%	0.3%	0.1%	0.1%	0.3%	0.2%	1.6%	0.7%	35	**0.4%**
Bank with special business clientele	0.0%	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**	**5,369**	**100.0**

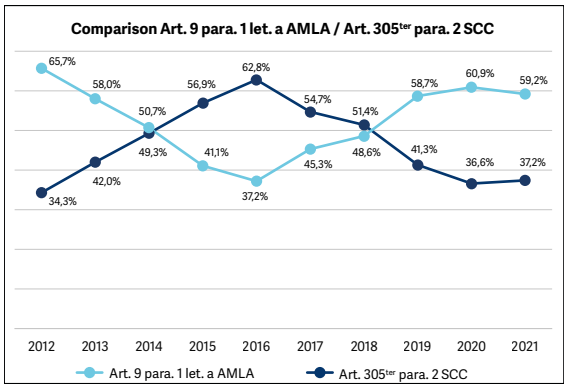
The table above does not show any significant changes compared with 2020.

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

[18] The absolute figures for 2012–2020 are published in the respective MROS annual reports.

4.6 The legal basis of SARs

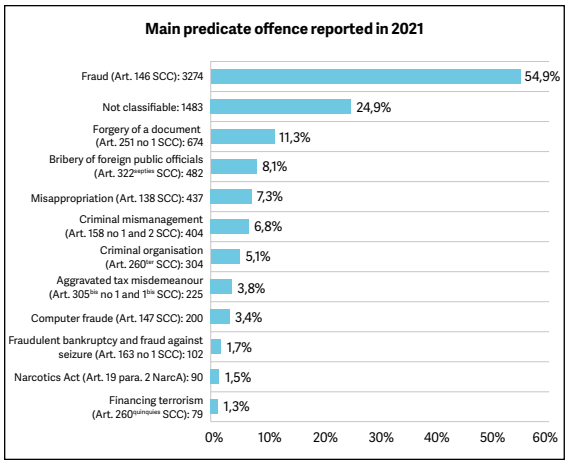
Of the 5,964 SARs received in 2021, 3,532 (59.2%) were submitted under Art. 9 para. 1 let. a AMLA (duty to report) and 2,230 (37.4%) under Art. 305ter para. 2 SCC[19] (right to report). A further 195 SARs (3.3%) were submitted under Art. 9 para. 1 let. b AMLA, while 4 SARs (0.07%) fell within the scope of the duty to report in accordance with Art. 9 para. 1 let. c AMLA and 3 SARs (0.05%) under Art. 16 para. 1 let. a AMLA.
As in 2020, no SARs were submitted under Art. 9 para. 1bis AMLA (duty of traders to report cash transactions).



The relative increase in SARs under Art. 9 para. 1 let. a AMLA observed since 2016 has not continued. As the vast majority of SARs received by MROS are submitted by banks, the trend is mainly an indicator of the behaviour of this sector. Nevertheless, there is a considerable difference between Swiss banks in terms of the number of SARs they submit under Art. 9 para. 1 let. a AMLA or Art. 305ter para. 2 SCC. This is illustrated in the table below.

4.7 Predicate offences

The chart below shows the main predicate offences that were suspected in the SARs submitted in 2021. Since 2020, the reporting financial intermediary may indicate several possible predicate offences in each SAR. As a result, the proportion of predicate offences mentioned in the SARs, when added up, exceeds 100%. A comparison with previous years is therefore indicative only.

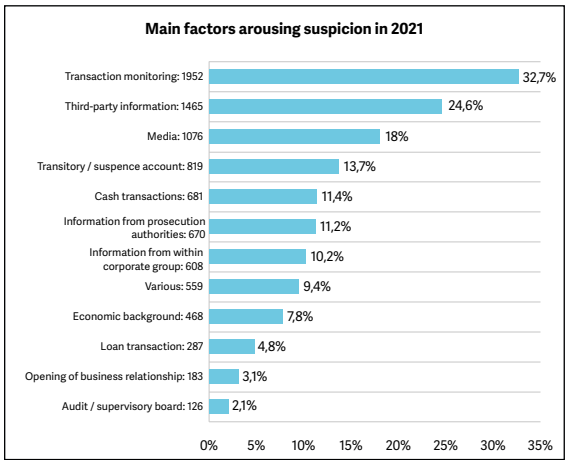


[19] SR **311.0**

– The above chart does not show much variation from 2020. The four most frequently suspected predicate offences (including 'not classifiable') remain the same, although there are differences over 2020 in absolute figures. The seven most frequently mentioned predicate offences also remain the same: although they appear in a slightly different order, their absolute figures do not change substantially.
– Fraud is the most frequently suspected predicate offence by far (in more than one out of two SARs), but slightly less often in 2021 (54.9%) compared with 2020 (58%). In 2021, as in 2020, this high proportion can be explained by the number of SARs submitted in connection with 'COVID loans' (see Chapter 4.11).
– One must be careful not to draw too precise conclusions about the nature of predicate offences in Switzerland from the chart since it only reflects the predicate offences suspected at the time the financial intermediary submitted the SAR. The analysis of the SAR carried out by MROS for its report to the prosecution authorities may establish other suspected predicate offences. In addition, the data presented here relates to SARs and does not take into account the value of assets or the number of business relationships or accounts reported per SAR. A more detailed analysis of predicate offences was carried out by the Interdepartmental Coordinating Group on Combating Money Laundering and the Financing of Terrorism (CGMF) in 2021, which we reported on.[20]

4.8 Factors causing suspicion

The chart below shows what sources triggered financial intermediaries' suspicions, prompting them to submit a SAR in 2021. As with predicate offences and in deviation from past practices, the new goAML system allows financial intermediaries to report more than one factor that caused 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.



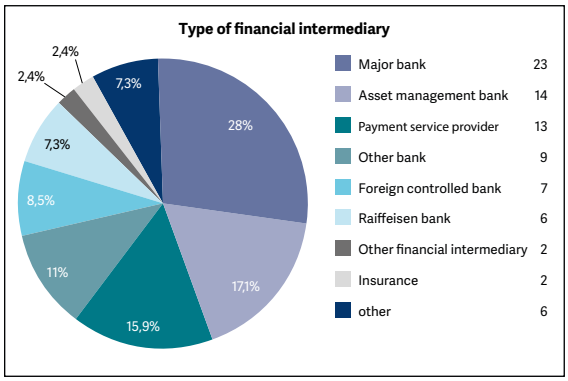
Type of bank	Art. 9 para. 1 let. a AMLA	in %	Art. 305ter para. 2 SCC	in %	Other	in %	Total
Cantonal bank	637	81.9%	133	17.1%	8	1.0%	778
Major bank	618	39.0%	952	60.1%	13	0.8%	1,583
Regional and savings bank	132	42.6%	171	55.2%	7	2.3%	310
Raiffeisen bank	339	86.0%	42	10.7%	13	3.3%	394
Stock exchange bank	529	58.6%	272	30.2%	101	11.2%	902
Other bank	713	77.8%	185	20.2%	19	2.1%	917
Private bank	0	0.0%	6	85.7%	1	14.3%	7
Foreign-controlled bank	236	53.3%	195	44.0%	12	2.7%	443
Branch of foreign bank	3	8.6%	32	91.4%	0	0.0%	35
Total	**3,207**	**59.7%**	**1,988**	**37.0%**	**174**	**3.2%**	**5,369**

[20] See Interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF): *Second national report on the evaluation of the risks of money laundering and terrorist financing in Switzerland*, October 2021, pp. 15-26.

– As in 2020, transaction monitoring was the category that aroused the most suspicion and triggered the most SARs (2021: 32.7%, 2020: 36.2%). The particularly high proportion of SARs triggered by transaction monitoring in 2021 is probably due, in part, to the large number of SARs submitted in connection with 'COVID loans' – as it was the case in 2020. Such SARs were submitted after transaction monitoring triggered financial intermediaries' suspicions that the loans were being misused.
– Information from third parties and information from media reports remain, as in 2020, in second and third place among the factors that triggered the most suspicion.

4.9 Terrorism financing

In 2021, 82 SARs were sent to MROS due to the suspicion of terrorism financing and/or violation of the Federal Act on the Proscription of 'Al-Qaeda', 'Islamic State' and Associated Organisations[21] (i.e. 1.4% of the total number of SARs received). These 82 SARs are also linked to other predicate offences, such as membership in a criminal organisation (24 cases), misappropriation (Art. 138 SCC) (6 cases) and bribery of foreign public officials (5 cases). Several cases also mention further predicate offences.
The most frequent suspicion triggers for financial intermediaries were transaction monitoring (32 cases), third-party information (22 cases), media reports (19 cases), cash transactions (16 cases) and information from within a corporate group (8 cases). Several cases also mention other suspicion triggers.
Most of the terrorism-related SARs were submitted by banks (62), followed by payment service providers (13 cases).[22]



Of the 82 terrorism-related SARs, 57 did not lead to a notification to the prosecution authorities by MROS while 10 were still being analysed at the end of 2021. The information from the remaining 15 SARs was used to submit 13 reports to the competent prosecution authorities: criminal proceedings were formally opened in 3 cases, in 1 case proceedings were abandoned and in 9 cases the decision of the prosecution authorities is pending or has not yet been communicated to MROS.

[21] SR **122**

[22] The categories "Other bank" and "Other financial intermediary" in the chart correspond to the categories in chapters 4.4 and 4.5. The category "other" refers to the remaining financial intermediaries, both banks and non-banks.

4.10 Organised crime

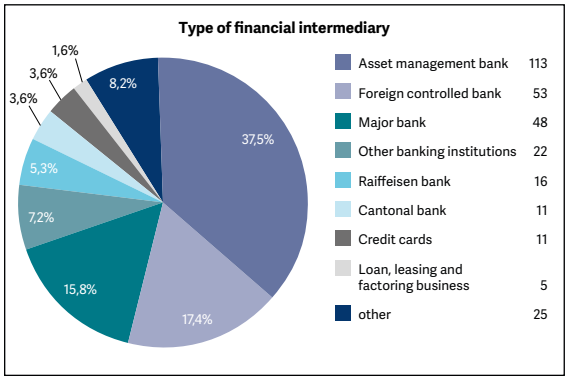
In 2021, MROS received 304 SARs indicating suspected links to a criminal organisation (i.e. 5.1% of total reporting volume).
During the reporting year, reports of suspected links to a criminal organisation also mentioned other potential predicate offences: fraud (115 cases), criminal mismanagement (66 cases), bribery of foreign public officials (40 cases), document forgery (30 cases) and misappropriation (24 cases).

Other predicate offences most frequently mentioned in the SARs related to suspicion on membership in criminal organisations	Number of mentions	in %
Fraud (Art. 146 SCC)	115	37.8
Criminal mismanagement (Art. 158 no 1 and 2 SCC)	66	21.7
Bribery of foreign public officials (Art. 322^{septies} SCC)	40	13.2
Document forgery (Art. 251 no 1 SCC)	30	9.9
Misappropriation (Art. 138 SCC)	24	7.9
Financing of terrorism (Art. 260^{quinquies} SCC)	22	7.2
Narcotics Act (Art. 19 para, 2 NarcA)	18	5.9
Aggravated tax misdemeanour (Art. 305bis no 1 and 1bis SCC)	12	3.9

In 2021, MROS received SARs concerning suspicion of membership in a criminal organisation with the following suspicion triggers:

Main reasons for suspicion	Number of mentions	in %
Media reports	119	39.1
Third-party information	59	19.4
Audit/Supervisory board	48	15.8
Transaction monitoring	47	15.5
Information from prosecution authorities	26	8.6
Opening of business relationship	26	8.6
Various	23	7.6
Cash transaction	22	7.2
Information from within a corporate group	17	5.6

The vast majority of SARs concerning suspected links to a criminal organisation came from the banking sector (87.5%), followed by credit card companies (3.6%). The main types of institutions that submitted these SARs were as follows:



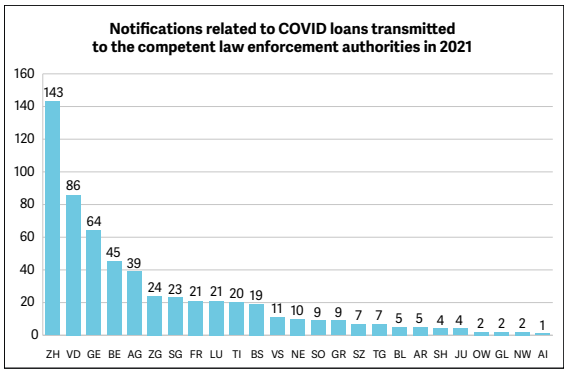
Of these 304 SARs, 234 (77%) did not lead to a notification to the prosecution authorities by MROS and 22 were still under analysis at the end of 2021. The information provided in 48 SARs prompted MROS to transmit 36 reports to the prosecution authorities. Of these, 4 led to no-proceedings orders, while the others are still being processed by the relevant prosecution authority.

4.11 COVID-19 pandemic

The various types of suspected money laundering cases emerging from the SARs sent to MROS in 2021 (see Chapter 4.1) included the misappropriation or fraudulent use of bridging loans granted by Swiss financial institutions under federal guarantee in connection with the COVID-19 pandemic, although the volume of these SARs was lower than in 2020. In 2021, MROS received 690 SARs (12% of total reporting volume) falling under this category (compared with 1,046 in 2020). The SARs related to 764 'COVID loans', granted by 31 different banks, totalling more than CHF 78 million. Since 2020, MROS has therefore received more than 1,700 SARs concerning COVID-related loans totalling almost CHF 230 million.[23]
In 2021, MROS sent 583 notifications to the prosecution authorities in relation to 675 SARs of

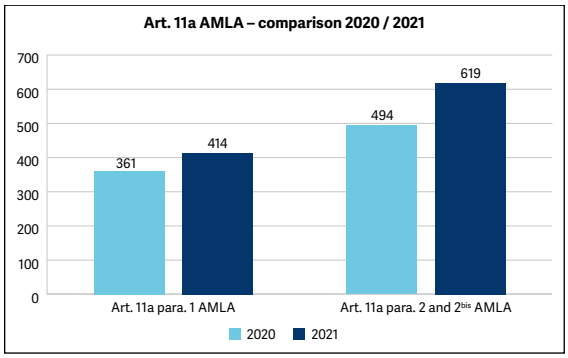
[23] See the corresponding statistics published on the MROS website: COVID-19 bridging loans.

this type; 138 were still under analysis at the end of the year.
The chart below lists the prosecution authorities that MROS notified and the number of notifications.

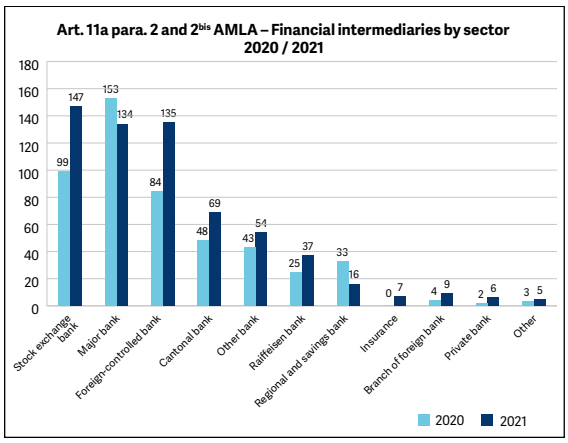


4.12 Requests for information under Art. 11a AMLA

Under Art. 11a para. 1 AMLA, MROS may formally request additional information from financial intermediaries that have submitted a SAR. Under Art. 11a para. 2 AMLA, MROS may also request further information from financial intermediaries that have not submitted a SAR, but that are involved in a transaction or business relationship related to a SAR (third-party financial intermediaries). The AMLA was expanded further on 1 July 2021 by introducing Art. 11a para. 2bis. The new provision obliges financial intermediaries involved in a transaction or business relationship reported by a foreign FIU to provide MROS at its request with all relevant information in their possession.
The number of requests to financial intermediaries under Art. 11a para. 1 AMLA increased slightly in 2021 over the previous year. The number of requests under Art. 11a para. 2 and 2bis AMLA to financial intermediaries who did not submit a SAR also increased. This is largely due to the introduction of the new Art. 11a para. 2bis AMLA.



There was no notable change in the category of financial intermediaries receiving a request for information under Art. 11a para. 2 and para. 1bis AMLA over 2020.

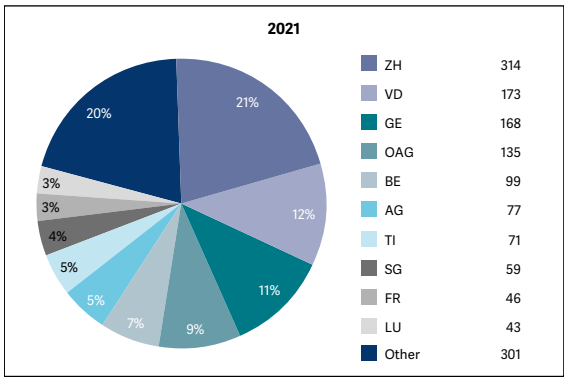


4.13 Notifications to the prosecution authorities

In 2021, MROS submitted 1,486 notifications to the prosecution authorities. This is 23% lower than in 2020 (1,939). As mentioned in our 2020 Annual Report, notifications can contain information from different sources and SARs, which in some cases have been received in different years. As a result, it is no longer possible to draw a direct comparison between the number of notifications made to the prosecution authorities and the number of SARs received in a given year. The 1,486 notifications to the prosecution authorities in 2021 contained information from

– 1,497 SARS received in 2021
– 304 SARs received in 2020
– 46 business relationships reported in 2019
– 18 business relationships reported in 2018
– 3 business relationships reported in 2017
– 2 business relationships reported in 2016

Prosecution authorities concerned
The chart below shows the cantonal prosecution authorities that MROS sent the 1,486 notifications to in 2021.



– As in 2020, the cantons of Zurich, Vaud and Geneva received the most notifications from MROS. The Office of the Attorney General of Switzerland (OAG) was in fourth position, as in 2020. The size of the financial sector in the various cantons has a significant influence on this distribution. In cases falling under cantonal jurisdiction, the place where the offence was committed generally determines which prosecution authority receives the notification from MROS. In the case of money laundering, the place of offence is generally the place where the suspicious business relationship was opened.
– In most cases, the notifications MROS sends to the OAG concern money laundering associated with predicate offences committed abroad. They therefore present a higher degree of complexity and the information they contain is more frequently drawn from different SARs. In contrast, notifications to the cantonal prosecution authorities tend to relate only to a single SAR.
– A comparison with years prior to 2020 is not meaningful: until 2020, each notification corresponded to one SAR concerning one business relationship. With the introduction of goAML, notifications may now involve several SARs concerning multiple business relationships. The information transmitted in these notifications may also have been drawn from sources other than SARs.

Legend

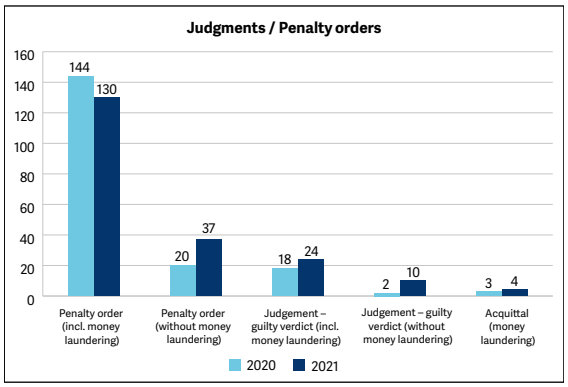
AG	Aargau	NW	Nidwalden
AI	Appenzel Inner Rhodes	OW	Obwalden
AR	Appenzel Outer Rhodes	SG	St. Gallen
BE	Bern	SH	Schaffhausen
BL	Basel-Landschaft	SO	Solothurn
BS	Basel-Stadt	SZ	Schwyz
OAG	Office of the Attorney General of Switzerland	TG	Thurgau
FR	Fribourg	TI	Ticino
GE	Geneva	UR	Uri
GL	Glarus	VD	Vaud
GR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

4.14 Decisions of the prosecution authorities

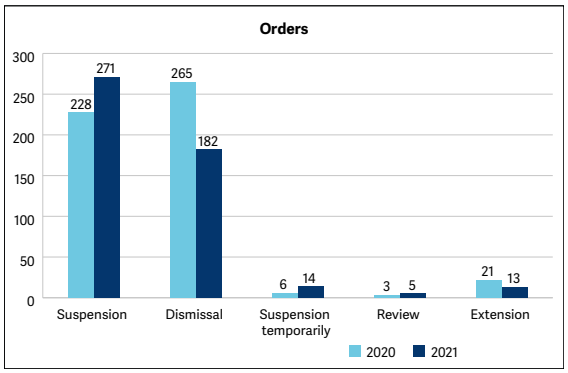
In 2021, MROS made an increased effort to obtain information under Art. 29a para. 2 AMLA on the status of notifications sent to the prosecution authorities and on judgments and rulings (Art. 29a para. 1 AMLA) in connection with Art. 260ter, 260^{quinquies} para. 1, 305bis and 305ter para. 1 SCC. In 2021, MROS received a total of 205 judgements and rulings in connection with notifications made by MROS during the year or before. It should be pointed out that MROS notifications to the prosecution authorities do not necessarily trigger the opening of new proceedings; sometimes they just contain information supporting proceedings that are already under way.

For comparison: 2012 – 2021

Authority	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2021 in absolute figures	Average 2012–2021
ZH	14.4%	18.4%	12.4%	13.5%	12.0%	10.2%	12.8%	14.3%	18.9%	21.1%	314	14.8%
VD	2.1%	2.4%	2.5%	2.6%	3.1%	1.8%	4.3%	5.5%	11.1%	11.6%	173	4.7%
GE	15.1%	15.0%	12.7%	8.4%	14.9%	12.8%	14.1%	15.0%	11.5%	11.3%	168	13.1%
OAG	35.8%	34.2%	44.7%	53.4%	38.1%	52.6%	48.4%	39.9%	9.0%	9.1%	135	36.5%
BE	3.8%	1.6%	4.6%	1.8%	3.0%	1.6%	1.8%	3.3%	7.5%	6.7%	99	3.6%
AG	2.0%	1.3%	1.8%	1.5%	2.6%	1.2%	1.6%	1.5%	5.3%	5.2%	77	2.4%
TI	13.6%	12.5%	7.3%	6.5%	6.0%	6.0%	3.3%	3.3%	5.0%	4.8%	71	6.8%
SG	2.2%	1.7%	3.0%	2.0%	2.2%	2.4%	1.3%	1.2%	3.5%	4.0%	59	2.4%
FR	1.2%	0.5%	0.2%	0.6%	0.6%	1.4%	1.6%	1.5%	2.7%	3.1%	46	1.3%
LU	1.1%	1.5%	1.8%	1.0%	1.4%	1.4%	0.8%	1.8%	3.5%	2.9%	43	1.7%
ZG	0.6%	1.2%	1.3%	1.5%	1.2%	0.6%	1.9%	1.9%	2.5%	2.6%	38	1.5%
VS	0.4%	1.1%	1.0%	0.5%	1.0%	1.2%	1.4%	0.8%	2.7%	2.4%	36	1.3%
BS	2.7%	2.2%	1.2%	1.3%	3.3%	2.0%	0.9%	0.9%	2.6%	2.3%	35	1.9%
TG	1.1%	0.7%	1.1%	0.8%	1.5%	0.7%	0.8%	1.3%	3.0%	2.1%	31	1.3%
SO	0.1%	1.1%	0.7%	0.4%	4.2%	0.4%	1.1%	1.2%	1.9%	2.0%	29	1.3%
NE	0.6%	0.7%	0.9%	1.1%	0.9%	1.0%	1.2%	1.4%	2.3%	1.9%	28	1.2%
BL	1.3%	0.8%	0.5%	1.5%	1.5%	1.2%	0.8%	2.9%	2.1%	1.7%	26	1.4%
SZ	0.6%	0.6%	0.2%	0.5%	0.8%	0.5%	0.3%	0.4%	1.0%	1.1%	16	0.6%
GR	0.5%	0.9%	1.0%	0.6%	0.3%	0.5%	0.3%	0.4%	1.5%	1.0%	15	0.7%
JU	0.1%	0.2%	0.6%	0.0%	0.3%	0.1%	0.1%	0.1%	0.3%	1.0%	15	0.3%
AR	0.1%	0.2%	0.2%	0.1%	0.3%	0.2%	0.2%	0.3%	0.6%	0.8%	12	0.3%
SH	0.4%	0.6%	0.3%	0.1%	0.5%	0.3%	0.1%	0.3%	0.5%	0.5%	7	0.4%
NW	0.0%	0.4%	0.1%	0.1%	0.0%	0.0%	0.7%	0.2%	0.3%	0.4%	6	0.2%
GL	0.0%	0.1%	0.0%	0.0%	0.1%	0.1%	0.2%	0.0%	0.2%	0.1%	2	0.1%
OW	0.2%	0.0%	0.0%	0.1%	0.0%	0.0%	0.0%	0.3%	0.2%	0.1%	2	0.1%
UR	0.0%	0.0%	0.1%	0.0%	0.2%	0.0%	0.0%	0.0%	0.3%	0.1%	2	0.1%
AI	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.1%	1	0.0%
Total	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**100.0%**	**1,486**	**100.0%**



In 2021, 182 no-proceedings orders and 271 ruling abandoning proceedings were issued in connection with MROS notifications. For the latter, it must be specified that these can also include cases that were partly abandoned (i.e. proceedings against one of several suspects or involving one of several offences were abandoned). Again, the MROS notifications, to which these decisions relate, were either made in 2021 or in previous years.



4.15 Sharing information with foreign FIUs

In the fight against terrorist financing, money laundering and its predicate offences as well as organised crime, MROS and its foreign partner authorities – the foreign Financial Intelligence Units (FIUs) – can exchange information via international administrative assistance. When MROS receives SARs involving foreign subjects, it is authorised to request information from its counterparts in the countries concerned. The information MROS obtains is important for its analyses, as a majority of SARs received by MROS have an international dimension.

In 2021, MROS sent 128 information requests to 52 different foreign FIUs.

In turn, it received 784 requests from 87 countries; this is the second consecutive year that this number has fallen (2020: 795 requests from 95 countries). This slight decrease is all the more remarkable given that MROS' extended competences to obtain information could have led to an increase in requests from foreign FIUs, prompted by the prospect of obtaining information MROS was not permitted to obtain prior to 1 July 2021 (see Chapter 2.2.).

Of the 784 requests for information it received in 2021, MROS processed 624 (86%). It also responded to 104 requests it had received in 2020. Although it is not apparent from the figures presented here, the substance of these responses is now more often supplemented with relevant financial information due to MROS' new competences. This means that processing information requests is now more complex and time-consuming than in the past.

Spontaneous information reports are reports provided by a foreign counterpart containing information with a link to Switzerland or, conversely, information from MROS sent to a foreign counterpart containing information with a link to a specific country. An FIU which receives a spontaneous information report is not required to provide any information in response. Since 2015, the number of spontaneous information reports processed in a given year is shown separately. In 2021, MROS received 527 spontaneous reports from 42 different countries. In turn, it sent 375 spontaneous information reports to 69 foreign FIUs.

4.16 Sharing information with national authorities

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

ing. MROS is authorised to share information with these authorities under Art. 29 AMLA. Since 2020, this form of information sharing has taken on new importance, both in terms of content and the heavy workload for MROS.
In 2021, MROS received 561 requests from 35 Swiss authorities for information on bank accounts, individuals and companies in the context of investigations into money laundering, organised crime and terrorist financing. In approximately 90% of the cases, these requests came from a cantonal police and the Federal Criminal Police. This is an increase in volume of 55% compared with the previous year (362 requests).
MROS also received 77 spontaneous information reports from Swiss authorities in 2021.
In turn, MROS forwarded 143 spontaneous information reports to other Swiss authorities active in the supervision of financial operations and combating money laundering and terrorism financing. MROS may also request information from other federal, cantonal or communal authorities; these requests are not listed in the figures above.

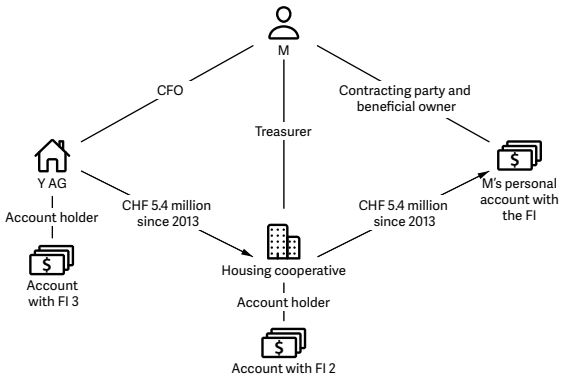
5. Typologies (a selection of cases to raise awareness among financial intermediaries)

The following five typologies (see Chapters 5.1-5.5) focus on the important role of financial intermediaries as the first line of defence in the Swiss anti-money laundering and combating the financing of terrorism system. These are exemplary cases (good practices) in which financial intermediaries have facilitated or even made possible an in-depth analysis by MROS thanks to the excellent quality of their SARs. These cases demonstrate, among other things, the importance of the clarifications carried out in accordance with Art. 6 AMLA ('Special due diligence obligations') before a SAR is filed and how these make it possible to fulfil the legal requirements that determine the content of a SAR (Art. 3 MROSO).
Financial intermediaries are the ones who know their clients best and their clarifications are crucial in order to be able to assess whether suspicions can be plausibilised and whether the requirements of the duty to report or the right to report are met. However, such clarifications do not end with the first indications of suspicion. The more complete and carefully documented the clarification documents are, the easier it is for MROS to carry out its analysis in a targeted and efficient manner.
The last typology presented below (see Chapter 5.6) is based on an analysis of selected judgements by prosecution authorities that were transmitted to MROS under Art. 29a para. 1 AMLA. It helps to raise financial intermediaries' awareness by showing the account types, customer profiles and behaviour patterns, and, in particular, the combination thereof, that require special attention on the part of financial intermediaries.

5.1 Suspected misappropriation of assets

Facts of the case
The client advisor working for the financial intermediary (FI) noted unusual incoming wire transfers to M's personal account from the account of a housing cooperative X.
Based on the client profile data that the FI has on file, client M is listed as the treasurer of the housing cooperative X. In addition, M is also mentioned as the CFO and member of the board of directors of a construction company Y AG.
Following transactional analysis, the FI determined that most of the incoming wire transfers into M's personal account came from housing cooperative X. The amounts paid into the account were unusally high and did not appear to correlate with any possible salary that the client might have received as remuneration for his position as treasurer. In total, the payments made to M's account from the housing cooperative X's account opened with another FI surpassed CHF 5 million.
The FI contacted the client to inquire about these transactions. The client explained that the incoming payments were commissions for construction projects carried out by the client. However, the FI was unable to ascertain why the client would receive funds from housing cooperative X in this capacity or how the incoming payments related to specific projects. The documentation provided by M to the FI during a meeting seemed to show that the funds paid out of the housing cooperative's accounts actually came from Y AG, of which M was the CFO. These funds were channelled through the account of

housing cooperative X. The FI was also unable to verify the authenticity of the said documentation. Moreover, the meeting did not enable further clarification of the economic background of these transactions.
This transactional pattern reinforced the FI's suspicions that funds credited to M's personal account could be the result of misappropriated assets by the client in his capacity as treasurer of housing cooperative X or in his capacity as CFO of company Y AG. The fact that the construction company Y AG had waived both ordinary and limited auditor supervision following a decision of the board of directors before the suspicious transactions began reinforced the FI's suspicion of a potential misappropriation of assets. The FI therefore submitted a corresponding SAR to MROS.



The identification and documentation provided by the FI in the presumed transactional diagram enabled MROS to formulate precise questions under Art. 11a para. 2 and 3 AMLA and to rapidly clarify this diagram.

Good practices of the reporting financial intermediary

– **The client advisor was attentive and detected suspicious transactions,** which allowed the compliance department to take over and carry out additional investigations. This highlights the importance of client advisors as the first line of defence in the financial intermediary's anti-money laundering system. Suspicious activities in their clients' business relationships must be detected and clarified in good time in order to be able to quickly take any necessary measures.
– **The precise documentation provided by the financial intermediary enabled MROS to seek targeted clarifications.** While new threads often emerge during an MROS analysis, complete and accurate documentation and evaluation by the financial intermediary is the starting point for an MROS analysis. When done properly, this can greatly enhance MROS's effectiveness.

5.2 Suspected human trafficking/forced prostitution

Facts of the case

A financial intermediary (FI) has a business relationship with a client who has indicated that she runs a beauty salon. The FI becomes suspicious because of the following transactional pattern: over the course of a single year, frequent cash deposits totalling over CHF 70,000 were paid into this account. The deposits were made by various female third parties in addition to the client herself. The FI's attention was drawn to the transactions because some of the funds were deposited into the account from one Swiss town and withdrawn several days later from another Swiss town, or in some cases from third countries in Europe. Transaction analysis and subsequent clarifications revealed that both the client and the female third parties involved had links to the prostitution industry.
In the case of a transit transaction to a third country in Europe, the FI's investigations revealed that the recipient was the client's alleged partner. The FI followed up on its investigations of this person and came across a relevant World-Check match. This linked the transaction recipient (the client's alleged partner) to organised crime and human trafficking activities.
The FI also noticed regular and frequent payments for advertising on adult entertainment platforms. The frequency of the advertising purchases suggested that the payments were made on behalf of several different people. In addition, the account showed rental payments for several rental properties, which was unusual given the client profile.

Finally, the client's behaviour as well as her incoherent and implausible statements prompted the FI to take an even closer look at the business relationship. The client stated that she ran a beauty salon and that the payments from female third parties mentioned at the beginning corresponded to payments for beauty treatments received. The client backed her statements with corresponding invoices. However, when the FI conducted an open source search, no beauty salon with the name indicated in connection with its client could be found. The FI also had doubts regarding the authenticity of the submitted invoices. For example, an unusual number of beauty care treatments seemed to have been provided to a single person at a time when the client was actually abroad; another example was that the presumed clients were charged different prices for identical treatments/services.

Good practices of the reporting financial intermediary

- **The financial intermediary noticed the suspicious transactions in a timely manner and immediately filed a SAR based on its clarifications.** A timely filing of SARs is essential for MROS to work efficiently. For one thing, it improves the chances of tracing or even freezing funds. At the same time, the information provided to MROS can also be a useful addition to investigative proceedings already underway in Switzerland or abroad.
- **Extensive open-source research was conducted.** Among other things, the persons involved and their presumed addresses were checked. In the process, the various persons involved were found to have links to the prostitution industry. In addition, the financial intermediary conducted a search on World Check for one of the money recipients, the client's alleged life partner, which yielded important information.
- **Avoiding the risk of tipping off the client. The financial intermediary discreetly contacted the client to inquire about all of these suspicious transactions. Inconsistent, incomplete or suspicious statements made by the client were documented and described.** Interviews with clients (if these can be done without the risk of tipping off the client) are an important aspect of the information that is conveyed in any SAR submitted to MROS. MROS does not have the authority to contact clients directly. Therefore, MROS must rely on the information that financial intermediaries are able to obtain. It is often the client behaviour, such as the coherence/correctness of statements, that provides indications which can be useful to MROS in analysing a SAR. However, it is important that the financial intermediary takes a critical view of such information and indications and provides MROS with all the elements at its disposal so that MROS can assess the reliability of the information and carry out any necessary checks. Financial intermediaries know their clients best and should use this advantage in their analyses.
- **A detailed transaction analysis was carried out and the main transactions were summarised precisely.** Among other things, clarifications were obtained regarding the counterparties. In addition, the invoices submitted by the client to justify the conspicuous payments were analysed in detail and examined for their plausibility in terms of content.
- **The documents/attachments submitted were complete and every suspicious event was fully documented.** No missing records had to be requested. Requests for additional information under Art. 11a para. 1 AMLA are time-consuming, both for MROS and for the reporting financial intermediary. According to Art. 3 para. 1 let. h MROSO, the reporting financial intermediary must ensure that the suspicions triggering the SAR are explained as precisely as possible and that all relevant documents are submitted.

Conclusion

Knowledge of the various characteristics and indicators of predicate offences to money laundering is an important prerequisite for an efficient compliance strategy. Different elements or combinations of elements indicate different predicate offences. For example, different indicators can be identified in cases of human trafficking than in cases of corruption or fraud. **In this specific case, the financial intermediary**

highlighted key indicators revealing activities involving human trafficking or forced prostitution. These indicators include the following:[24]

- Frequent cash deposits
- Deposits made to the account in town X with corresponding cash withdrawals in town Y (pass-through transactions)
- Transfers of relatively small amounts of money
- Large number of persons making deposits or withdrawals
- Outgoing international money transfers to persons and companies in countries where a disproportionate number of victims of trafficking come from
- Recurring and frequent payments for advertisements on adult entertainment platforms
- Frequent spending for different hotels/rental properties
- Expenditures that do not match the client's KYC profile
- Links to the prostitution industry

The business relationship was reported on the basis of a holistic approach. The different elements linked together are not necessarily suspicious if examined separately; a link to the prostitution industry, for example, is not in itself sufficient grounds for suspicion, since sex work is legal in Switzerland under certain conditions. However, in combination with other suspicious factors, such as World-Check hits in this case, certain elements can be indicative of an underlying predicate offence. The holistic approach adopted by the reporting financial intermediary made it possible to establish connections that would have remained undetected with a unilateral approach (focusing on isolated elements of the business relationship, such as individual transactions or KYC aspects).

5.3 Suspected professional money laundering

Facts of the case

The financial intermediary (FI) monitored the personal account of a lawyer who had ceased to be a member of the bar association several years earlier. The suspicions were raised after the FI found a number of incoming deposits that were then quickly transferred to other accounts in Switzerland and abroad. The client's account was therefore being used as a transit account, with the lawyer acting as an escrow agent. The FI contacted the client and found that he had marketed himself to third parties as a bar member, despite the fact that this had not been the case anymore for several years. Although the lawyer no longer practised law, he explained that he had retained some of his previous clientele for advice on legal matters. In particular, he made his account available to his clients. According to the former lawyer, one of his clients had been unable to carry out certain transactions because of anti-money laundering regulations. The lawyer provided the FI with several legal documents to support his claim. The FI carried out a background check on the lawyer's clients and found various news articles and other negative hits showing that one of the clients was allegedly subjected to criminal proceedings abroad.
Unable to dispel the suspicion that the lawyer had laundered money on behalf of his clients, the FI reported his personal account to MROS.

Good practices of the reporting financial intermediary

- **The financial intermediary used the client's profile as a frame of reference during research and clarification** when transactional analysis revealed various transactions from several third parties and determined that the client's account was being used as a transit account.
- **The financial intermediary conducted extensive background checks of counterparties.** This allowed the financial intermediary to identify negative information about these counterparties, which was then documented in detail.

[24] See FATF Report *Financial Flows from Human Trafficking*, July 2018, for more detailed explanations on indicators as well as case studies describing the detection of human trafficking and related predicate offences.

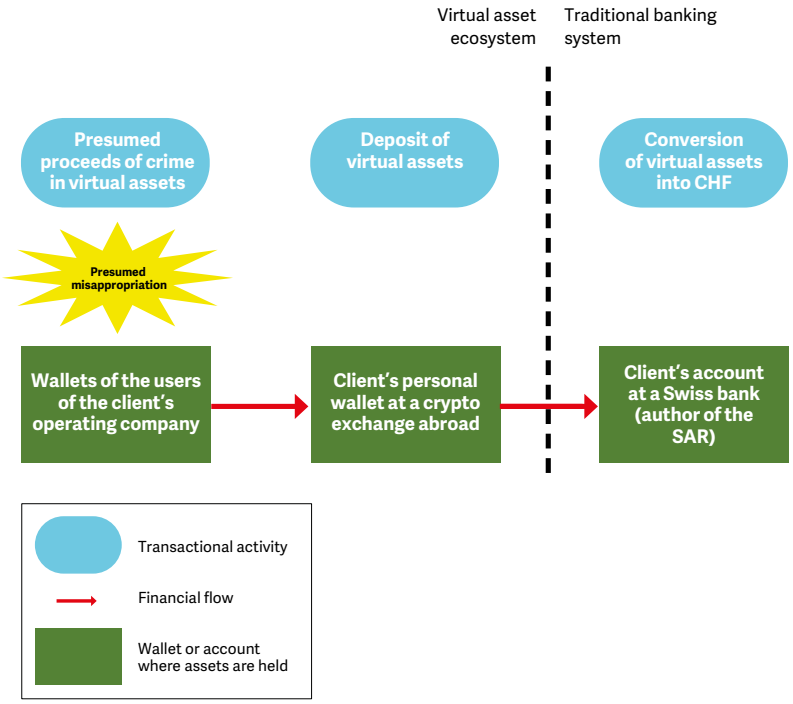
5.4 Suspected misappropriation of virtual assets

Facts of the case
Several clients of a financial intermediary (FI) from the banking sector ran a cryptocurrency exchange business via one of their operating companies. They appeared to have generated most of their wealth through this business as well as through early investments in cryptocurrencies.
After an urgent request from their clients that the FI considered unusual, the FI began to look more closely at the various accounts and called in the compliance department. In parallel to this incident, the FI noted recent unusual transactional behaviour on the accounts. In a short period of time, several hundred thousand Swiss francs were deposited via several wire transfers into the accounts of the clients in question. A significant portion of these funds originated from well-known cryptocurrency exchange platforms registered in various jurisdictions. Part of the deposits were therefore likely to result from the conversion or sale of crypto assets. Given the context, however, these transactions seemed suspicious and the FI sought clarifications. Following an analysis of the various transactions, the FI suspected that its clients may have misappropriated the funds from their clients/users of the cryptocurrency exchange platforms in question. Later, additional suspicious transactions, that reinforced this suspicion, were observed.
Overall, during its clarifications, the FI very quickly established the scope of its investigation including the origin of the cryptocurrency funds and verification of tax compliance. The clarifications carried out by the FI soon focused on technical aspects such as requesting screenshots of the clients' crypto exchange accounts as well as proof of origin of the cryptocurrencies on the exchanges in question. This was done in order to ultimately understand the paper trail. The FI also sought to obtain evidence of the existence of its clients' cryptocurrency holdings, whether held directly on a cryptocurrency exchange platform or in non-custodial wallets *(Private/Self-hosted/Unhosted/Non-custodial Wallet)*.
The scope of the investigation also included assessment of the legitimacy of the activities of the clients' company in the crypto assets sector. The FI's clarifications included, for example, ascertainment of whether the company had obtained the permits required for this activity in the various jurisdictions in question. The FI also critically examined the information published on the company's website.
Once all these clarifications had been obtained, the FI concluded that there was indeed a possible misappropriation of funds from the company's clients or users of the cryptocurrency exchange platforms in question. The FI therefore decided to submit a SAR regarding the business relationships of these various individuals to MROS.

Good practices of the reporting financial intermediary
– **Although the financial intermediary may be described as more of a 'traditional' financial intermediary, it demonstrated an excellent understanding of the risks inherent to the virtual assets sector.** Although the financial intermediary was unable to obtain all the clarifications requested, it collected and documented relevant and valuable information that facilitated MROS's analysis of the origin of the funds and the activity of the clients' company. These clarifications enabled MROS to send three requests for information to foreign FIUs and to obtain information related to, for example, the origin of the cryptocurrency funds at one of the platforms abroad or the legitimacy of the company mentioned above.

5.5 Possible case of indirect contamination

Facts of the case
The financial intermediary (FI) actively engages in the brokerage of cryptocurrencies and may be described as a virtual asset service provider (hereinafter VASP).
As part of a periodic review of transactions, one of the blockchain analysis tools used by the FI generated a high-risk alert in relation to various bitcoin transactions made on behalf of its clients.



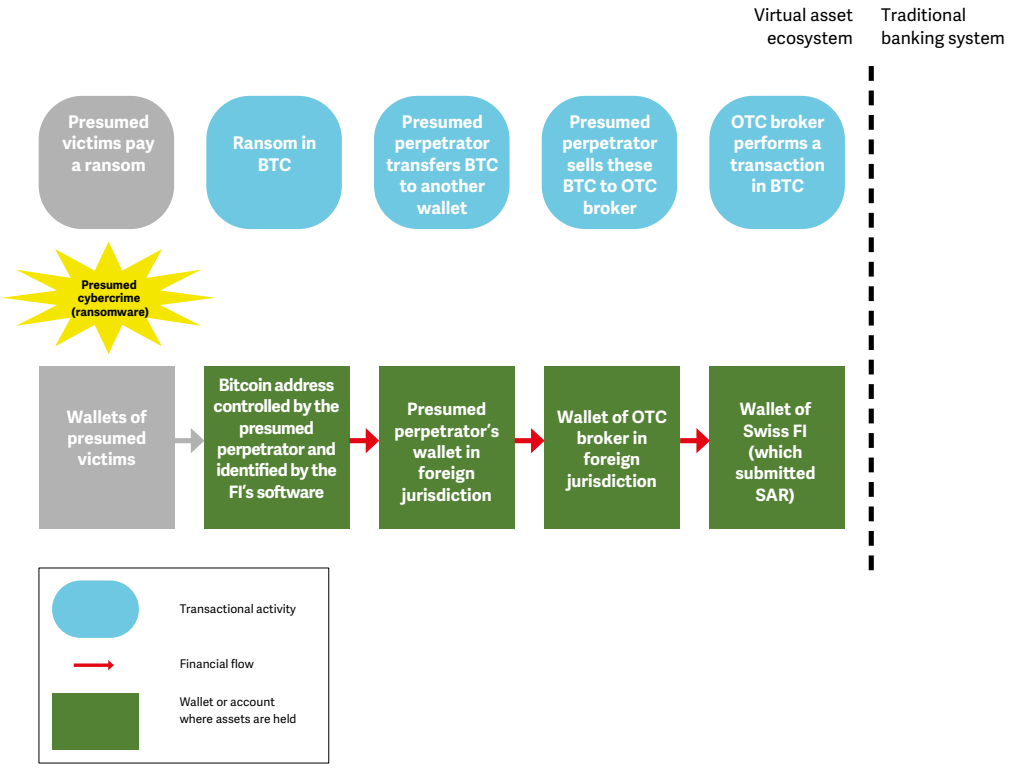
The alert generated by the blockchain analysis tool appeared to show an indirect link between these transactions and ransomware-type cybercrime.[25]

The suspicious transactions apparently took place in the context of the acquisition of several dozen bitcoins from a business partner abroad. The bitcoins were acquired on behalf of a client of the FI. The business partner in question is an OTC broker and therefore also a financial intermediary. As such, its virtual asset services are subject to due diligence requirements and the broker is registered with a supervisory authority.

The FI therefore initiated its clarification procedure, focussing its investigation on two areas: firstly, the FI contacted the OTC broker to find out whether it had already carried out clarifications on its side and what the outcome had been. Secondly, the FI performed an independent and critical analysis to understand why its blockchain analysis tool had generated the high-risk alert and whether this result alone could justify submitting a SAR to MROS. To this end, it carried out in-depth analysis of the source used by the blockchain analysis tool itself. The aim was therefore to determine whether a crime had actually been committed. In addition, the analysis included the use of different blockchain analysis tools to trace the same flow of transactions and compare the results.

Based on the analysis of the transactions and the further clarifications carried out, the FI came to the conclusion that a crime may have been committed and that there were possible connections to a client of his business partner abroad. At the end of its clarification process, the FI decided to report the case to MROS.

[25] Ransomware refers to malicious software (malware) that installs itself on the computer, encrypts data and/or blocks the computer. In most cases it is a so-called drive-by infection. If the victim visits a manipulated website from an insufficiently protected computer, the malware is installed. The criminals then demand a ransom for the data to be unencrypted or for the computer to be unlocked. Sometimes the malware also sends an apparently official notification, using police logos depending on the country, demanding that the victim pay a fine.



Good practices of the reporting financial intermediary

– **The financial intermediary did an excellent job of documenting the clarifications carried out with the foreign OTC broker and the blockchain analysis (submission of visual diagrams) and he critically questioned the sources used by one of its analysis software tools.** On this basis, MROS carried out additional analyses to assess whether it was appropriate to transmit the information gathered to a foreign FIU.

5.6 Selected findings from served judgments according to Art. 29a para. 1 AMLA

Human trafficking and procurement for prostitution:

In 2021, MROS received various unconnected judgments relating to human trafficking and procurement for prostitution. The victims, all women and transgender, came from two regions: Eastern Europe and Thailand. In both cases, the perpetrators and victims came from the same country. The trafficking organisations with victims from Eastern Europe and Thailand showed certain similarities, but there were also clear differences in their structure and modus operandi.

The characteristics related to Thai victims of human trafficking are described below:

The organisational aspects uncovered during investigations pointed to two 'organisations,' one in Thailand and one in Switzerland. In both cases, the perpetrators were predominantly female. These female perpetrators, or intermediaries, recruited the victims in Thailand. While the victims from Thailand knew that they were going to engage in prostitution, they had only received rudimentary information about the financial aspects and how to work off the debts (for facilitation services, travel and living expenses). Entry into Switzerland was achieved by means of visas organised in advance by the intermediaries. Often the victims were registered as alleged owners of companies, which allowed them to

apply for tourist visas for the Schengen area. In some cases, with the help of the Swiss 'organisation', forged EU passports were also arranged in order to obtain a type L residence permit in Switzerland.
Once in Switzerland, the victims were picked up by the female intermediaries and accompanied to the assigned brothels. Once arrived in Switzerland, the victims were always accompanied or under observation and thus socially isolated. In the case of entry by means of forged passports, the victims were also accompanied when going to the authorities (applying for visas, etc.), whereby the intermediaries sometimes waited outside the offices of the authorities.
For facilitation and travel, the victims had to pay back debts of about CHF 40,000 – 60,000 to the intermediaries. Furthermore, additional costs for board and lodging were constantly being added. It was clear from the judgments that the revenues generated by the victims were divided 50:50, with 50% of the revenues being used to repay the facilitation and travel costs and 50% being paid to the brothel operator. Accordingly, the victims were deprived of all income from their activities. Transactions were always carried out by the brothel operators or intermediaries.
It soon became clear to the victims that only a very small part, if any, of the revenues generated would be sent to their country of origin to support their families.
Despite the poor conditions, a key element in controlling the victims was, in addition to intimidation, the fact that the victims' contact persons were often older women. According to the statements referred to in the judgments, respect for the elderly, which is deeply ingrained in Thai mentality, led to strict obedience on the part of the victims.

The analysis of transaction behaviour in relation to business relationships held with Swiss financial intermediaries is based entirely on the reported judgements, as MROS did not receive any SARs in the cases analysed. The following typologies were identified in the analysed judgments:

- The victims did not have their own bank accounts. All accounts were held in the name of the perpetrators.
- According to the documents in the KYC records, the perpetrators were not indicated as involved in prostitution activities.
- The perpetrators were usually much older than the victims.
- The perpetrators' income from the accounts held in their names amounted to approximately CHF 60,000 and CHF 140,000 per year.
- Payments into the accounts of the perpetrators were made by third parties.
- The money paid into these accounts was then transferred to various intermediaries in Thailand to pay off the facilitation fees.
- In some cases, smaller amounts were also bank transferred from the perpetrator's accounts to the accounts of family members of the various victims.
- Other transactions were made via payment service providers to the intermediaries as well as to family members of the victims instead of bank transfers.

6. MROS practice

6.1 Revision of AMLA (SIF draft)

On 19 March 2021, the Swiss Parliament endorsed a reform of the Money Laundering Act (AMLA).[26] This led to the adaptation of five Federal Council ordinances[27] (including OMLTF[28] and MROSO[29]). At the time of writing, the date of entry into force of these amended legal instruments has not yet been formally fixed, but it is planned for 1 October 2022. These changes will involve adjustments to MROS practice in several respects. The main changes affecting both MROS and financial intermediaries and some of their practical implications are set out here.

6.1.1 Amendment of Art. 9 para. 1 let. c and 1^{quater} AMLA (definition of the term 'reasonable suspicion')

The Swiss Parliament introduced a definition of the notion of reasonable suspicion triggering the duty to report in Art. 9 para. 1^{quater} AMLA.[30] As the wording of the Act now makes clear, reasonable suspicion exists when the financial intermediary has one or more concrete indications that the assets held in the business relationship may meet the criteria of Art. 9 para. 1a AMLA and the additional clarifications carried out pursuant to Art. 6 AMLA do not dispel these suspicions. This definition is consistent with the approach that MROS and FINMA have adopted a long time ago[31] and which has been upheld repeatedly in case law.[32] With regard to the right to report, it is worth recalling that the Federal Council and the competent authorities consider the right to report to be an instrument of subsidiary importance to the duty to report.[33] This means that before making use of the right to report, the financial intermediary must always examine whether the duty to report is applicable, taking into account the definition of reasonable suspicion now established in the law. The financial intermediary may only make use of the right to report if there is no duty to report.
By including a definition of the notion of reasonable suspicion and removing the few remaining elements in the Act and corresponding ordinances that enabled MROS to treat reports differ-

---

26 SR **955.0**. The revision in question can be found here: BBl **2019** 5451 and here: BBl **2021** 668.

27 See FDF, Amendment of the Ordinance on Combating Money Laundering and Terrorist Financing: *Explanatory report on the consultative draft*, October 2021.

28 SR **955.01**

29 SR **955.23**

30 BBl **2021** 668

31 *2007 MROS Annual Report*, p. 3 and *2016 MROS Annual Report*, Chapter 4.1.2. See also as an example the *FINMA Annual Report for the year 2017*, April 2018, p. 31.

32 For an overview of this, see BBl **2019** 5477 as well as FSC 6B_686/2020 dated 11 Jan. 2021, c. 2.1.3 sq.

33 BBl **2019** 5451, Ch. 4.1.5.2.

ently (e.g. time limits on processing, see below), financial intermediaries will now have greater legal certainty. The revised Act should also help to harmonise financial intermediary practices when it comes to deciding whether to apply Art. 9 para. 1 AMLA or Art. 305ter para. 2 SCC as the legal basis for their SARs.
In keeping with current practice and the new wording of the revised Act, financial intermediaries will now always be required to carry out preliminary clarifications in accordance with Art. 6 para. 2 AMLA before submitting a SAR. This provision ensures the quality of SARs produced by financial intermediaries as well as the efficiency of the Swiss anti-money laundering system. In this respect, it is worth noting that any SAR sent to MROS must describe the suspicions on which it is based as precisely as possible, including account statements, detailed supporting documents showing the suspicious transactions as well as any links with other accounts. In addition, each SAR must also include documentation relating to the financial transactions, information regarding the required clarifications carried out as well as other supporting documents.[34] In accordance with Art. 4 para. 1 MROSO, MROS will only acknowledge receipt of a SAR if it contains all of the required information in accordance with Art. 3 para. 1 and Art. 3a para. 3 and 4 MROSO.

6.1.2 Abolition of MROS processing period (new wording of Art. 23 para. 5 AMLA) and notification of termination of business relationship (new Art. 9b para. 1 and 3 AMLA)

Currently, MROS has twenty days to decide whether or not to transmit a SAR that it has received under Art. 9 para. 1 AMLA to a prosecution authority (Art. 23 para. 5 AMLA). There is no time limit for SARs submitted under Art. 305ter para. 2 SCC. For several years, MROS has been unable to ensure compliance with this processing time limit, which is particularly insufficient for SARs that require in-depth analysis; lead to requests for information to foreign counterparts; or for which MROS sends requests for information to third party FIs under Art. 11a para. 2 AMLA. This leads to an unfortunate situation for both MROS and the FIs, especially as the current provisions of Art. 30 OMLTF-FINMA do not allow the financial intermediary to terminate the reported business relationship on its own initiative under Art. 305ter para. 2 SCC in the absence of notification from MROS on whether or not a SAR has been transmitted to prosecution authorities.
In order to address these difficulties, the Swiss Parliament chose to amend the AMLA. The new Art. 9b para. 1 AMLA provides for a period of forty working days after which financial intermediaries may terminate a business relationship that has been reported under certain conditions (paper trail) – irrespective of whether the SAR was submitted under Art. 9 para. 1 let. a AMLA or Art. 305ter para. 2 SCC – as long as MROS has not notified them in the meantime that the SAR has been transmitted to a prosecution authority. The possibility for financial intermediaries to decide at the end of this period whether they wish to continue a reported relationship or not is subject to the added requirement under the new Art. 9b para. 3 AMLA that financial intermediaries inform MROS 'without delay' of the termination of the reported business relationship and the date when this occurred. These amendments have important implications for MROS in a number of ways and will have practical consequences for financial intermediaries.
Firstly, it should be noted that these amendments effectively eliminate the legal time limit for processing and allow MROS to prioritise and process the SARs it receives according to its own internal criteria. As such, these amendments are an important element in the implementation of of MROS' strategy developed in 2020.[35]
Another important point should be stressed here. Until now, Art. 23 para. 6 AMLA required MROS to systematically inform the financial intermediaries of the outcome of their SAR, also in cases where a SAR was not transmitted to a prosecution authority. In the future, under the new wording of Art. 23 para. 5 AMLA, MROS will

[34] Art. 3 para. 1 let. h MROSO. For more information, see *2018 MROS Annual Report*, Chapter 4.1.

[35] For more information see *2020 MROS Annual Report*, p. 9.

only have to inform financial intermediaries if the information in a SAR is transmitted to a prosecution authority, and then only if the financial intermediary has not already terminated the business relationship reported under the new Art. 9b AMLA. The current wording of Art. 23 para. 6 AMLA was mainly justified by the fact that financial intermediaries had to wait for a decision from MROS before deciding on the possible termination of a reported business relationship. It was also based on the principle that MROS has a time limit for deciding whether or not to transmit a SAR. The removal of the time limit for processing and the provisions of the new Art. 9b para. 1 AMLA, which allow the financial intermediary to decide whether or not to continue a business relationship after 40 days, even in the absence of a decision by MROS, render these justifications obsolete.

Furthermore, the current situation in which MROS notifies financial intermediaries of its decision not to transmit information from a SAR is also unsatisfactory. Non-transmission decisions may be misinterpreted by financial intermediaries as a sign that the SAR was not justified or that the reported assets are of legitimate origin. They may influence the financial intermediary's assessment of whether or not to continue a reported business relationship. However, the fact that MROS decides not to transmit information from a SAR to a prosecution authority does not allow such conclusions to be drawn. It is often the case that MROS informs a counterpart in a third country of elements that may be of interest to it, for example because they are related to proceedings underway in that country. In such circumstances, the information in the SAR is not necessarily transmitted to a Swiss prosecution authority, but may be used instead as input for a possible request for international mutual assistance in criminal matters addressed to Switzerland. While in such a case the financial intermediary would indeed receive notification from MROS that the SAR was not transmitted (i.e. to a Swiss prosecution authority), no conclusions can be drawn as to the appropriateness of the SAR or legality of the reported assets. In other cases, several related SARs may reach MROS over a long period of time and only the more recent ones contain the elements that would justify transmitting the SAR to the prosecution authorities.[36] In such cases, the information of all relevant SARs is combined in a single report which might be transmitted to the competent authorities several months after MROS received and processed the first SAR.

It should be noted that Art. 8 para. 2 MROSO stipulates that MROS is free at any time to transmit information to a prosecution authority that previously might not have been transmitted (e.g. because new elements from another SAR or information from a national authority or a foreign counterpart justify it). In such cases, the financial intermediary that filed the first SAR will first receive notification that MROS did not transmit the SAR to a prosecution authority but then later would be notified that MROS has changed its initial decision.

As provided for in the new Art. 23 para. 5 AMLA, however, MROS will continue to notify financial intermediaries whenever information from a SAR has been transmitted to a prosecution authority. The main reason for this notification is the 5-day obligation to freeze assets under Art. 10 para. 1 and 2 AMLA. On the other hand, it makes little sense, from this point of view, to inform a financial intermediary of a transmission if it is unable to freeze the client's assets because the reported business relationship has been closed.

For these reasons, and in accordance with the new articles mentioned above, MROS will in the future only report its decisions if the SAR was transmitted to a prosecution authority and only if the financial intermediary has not terminated the reported business relationship under the new Art. 9b AMLA. MROS will also not respond to any requests from financial intermediaries to find out whether MROS has decided not to transmit the SAR, either before or after the expiry of the time limit provided for in the new Art. 9b para. 1 AMLA. As in the past, MROS will sometimes have to transmit information from a SAR to a prosecution authority after the time limit set out in the new Art. 9b para. 1 AMLA has elapsed. This might occur, for example, in the cases mentioned above;

[36] Within the meaning of Art. 23 para. 4 AMLA.

where analysis has taken longer than expected, or because MROS subsequently receives additional information justifying a decision to transmit the SAR to the prosecution authority. In such cases, the provisions of the new Art. 9b para. 3 AMLA will enable MROS to notify the relevant prosecution authority of the possible closure of a reported business relationship, if this has occurred after the SAR was submitted pursuant to the new Art. 9b para. 1 AMLA. It is therefore useful for MROS to know the destination of any significant assets remaining in the business relationship at the time of their closure, so that it can provide this information to the prosecution authorities. MROS will therefore expect financial intermediaries who report the termination of a reported business relationship under the new Art. 9b para. 3 AMLA to provide the relevant information collected under Art. 9b para. 2 AMLA (paper trail).

6.1.3 Practical questions associated with the implementation of the new provisions in Art. 9b and Art. 23 para. 5 AMLA

The effective application of the new provisions outlined above raises several practical issues.
A first question concerns the manner in which financial intermediaries will be required to inform MROS that they have terminated a business relationship pursuant to Art. 9b para. 3 AMLA. In practice, these notifications will have to be made in writing and will formally be considered a new form of notification – the content of which will be specified in the MROSO. They may be sent in electronic form or, for financial intermediaries not registered in goAML, by post, using an official form. The goAML manual published by MROS[37] will be updated by the time the new provisions come into force. This manual will describe the technical details for notifications to be sent in electronic form (e.g. how to indicate the reference number of the initial SAR, the procedure to follow when only part of the business relationship has been terminated, etc.). A copy of the documents proving the termination of the business relationship should be attached to the notification. If applicable, it should also provide information enabling MROS to determine the main destination(s) of the assets remaining in the business relationship at the time of its termination (details of significant transactions, account statements, etc.). By providing such information in full, the financial intermediary avoids having to deal with any subsequent request for information from MROS under Art. 11a AMLA.
A second question has to do with the point in time at which MROS should be notified. In some cases, a lot of time may pass between the moment when the financial intermediary decides to terminate a business relationship and the moment when the relationship is actually terminated. The wording of Art. 9b para. 3 AMLA ('inform MROS when the relationship is terminated' rather than 'inform MROS when the decision to terminate has been reached'; 'the date on which it [the termination] took place') clearly shows that MROS should be notified the moment when a business relationship has been effectively terminated. Furthermore, as long as assets remain in the reported accounts, the financial intermediary is in a position to freeze the remaining assets under Art. 10 para. 1 AMLA and must therefore be informed if MROS decides to transmit the SAR to the prosecution authorities.
A third question concerns the scope of Art. 9b AMLA, in particular in cases where the client – not the reporting financial intermediary – decides to terminate the business relationship. Following the line of reasoning outlined above, it makes little sense for a distinction to be drawn between client-driven or financial intermediary-driven termination. In neither case are any assets left to be blocked on the business relationship. However, under the new Art. 23 para. 5 AMLA, MROS is required to inform the financial intermediary if it decides to transmit the SAR to the prosecution authorities. The only exception is in cases where the business relationship has been terminated at the initiative of the financial intermediary. In the future, financial intermediaries will therefore not be required to submit a notification under Art. 9 b para. 3 AMLA to MROS in cases where a business relationship was terminated at the re-

[37] See *goAML Web – User's Manual.*

quest of a client. In such circumstances, financial intermediaries would continue to receive asset freeze requests that they would no longer be able to carry out.
Still on the subject of the scope of Art. 9b AMLA, financial intermediaries may also be uncertain as to whether a termination of a business relationship must be reported if it occurs much later than the 40-day period provided for in the new Art. 9b para. 1 AMLA, and for reasons unrelated to the suspicions that triggered the SAR (e.g. due to a policy change made by the financial intermediary). Neither the law nor the ordinances set any limits here: the scope of the law prevents the financial intermediary from terminating a reported business relationship of its own accord for 40 days, regardless of the reason for the termination, and then allows it to do so, regardless of the reason. Therefore, financial intermediaries will in any case have to notify MROS if they terminate a business relationship under Art. 9b para. 3 AMLA as long as MROS has not yet notified them of its decision to transmit their SAR to a prosecution authority. This requirement to inform MROS of the termination of a business relationship applies regardless of the reason or the date. However, the provisions of Art. 34 para. 4 AMLA that require financial intermediaries to destroy the data relating to a SAR after a period of five years from the date of submission of the SAR limit the duty to notify under Art. 9b para. 3 AMLA. Consequently, there will be no notification within the meaning of the new Art. 9b AMLA after the expiry of 5 years from the date on which MROS acknowledged receipt of the corresponding SAR. In the event of serious or repeated violations on the part of financial intermediaries, MROS may inform the competent supervisory authorities, supervisory bodies or self-regulatory organisations (SROs) pursuant to Art. 29 para. 1 AMLA, or the new Art. 29b AMLA concerning the sharing of information with SROs and supervisory bodies. This reporting by MROS is similar to what happens, for example, when a financial intermediary fails to comply with requests for information made pursuant to Art. 11a AMLA.[38]
A fourth question concerns whether MROS will continue the current practice of informing a reporting financial intermediary when its SAR has been transmitted to a prosecution authority even in cases where the business relationship ended prior to submission of the SAR to MROS. From the standpoint of enabling the financial intermediary to freeze the assets in question, the business relationship no longer exists and therefore informing the financial intermediary of the outcome of MROS analysis makes little sense. However, the law is clear: the only exception set out in Art. 23 para. 5 AMLA is the case provided for in Art. 9b AMLA where the business relationship is terminated after the SAR has been submitted. In such cases, MROS will continue to notify financial intermediaries when it decides to transmit a SAR to the prosecution authorities.

6.1.4 Other amendments in brief

The revised AMLA adopted on 19 March 2021 also affects MROS in other respects. There are no specific issues associated with the implementation of the new provisions. We refer to the information that has already been published on this subject[39] and limit ourselves to a brief mention here. The Central Office for Precious Metals Control (OPMC) has now been named a supervisory authority within the meaning of the AMLA. The same principles apply to the relationship between the OPMC and MROS in the context of the implementation of the AMLA as to the cooperation between MROS and the other supervisory authorities (FINMA, FGB, intercantonal authority), namely with regard to the exchange of information between authorities (Art. 29 para. 1 AMLA). Furthermore, the conditions under which prosecution authorities may use foreign information transmitted by MROS, if the use is subject to certain conditions, are now regulated by law (Art. 29a para. 2bis AMLA). In the future, authorised supervisory bodies and recognised

[38] BBl **2012** 6974

[39] BBl **2019** 5499; FDF, Amendment of the Ordinance on Combating Money Laundering and Terrorist Financing; *Explanatory report on the consultative draft*, October 2021.

self-regulatory organisations (SROs) will also be able to exchange all information required for AMLA implementation with MROS directly within the framework of national cooperation (Art. 29b para. 1 AMLA).

6.2 Financial intermediary questions regarding the duty to keep records

According to Art. 7 para. 3 AMLA, a financial intermediary must retain supporting documents for at least ten years after the business relationship has been terminated or after the transaction has taken place[40]. In the past, financial intermediaries have asked MROS two questions regarding this provision:

– What is meant by 'records' within the meaning of Art. 7 para. 3 AMLA?
– In the event of a SAR or a request under Art. 11a AMLA, must records that are older than 10 years also be disclosed?

In the context of this year's annual report, MROS would like to clarify the following:

a. Records within the meaning of Art. 7 para. 3 AMLA

MROS considers records within the meaning of Art. 7 para. 3 AMLA as comprising all documents that enable verification of compliance with the obligations set out in the AMLA[41] and its implementing ordinances as well as with the rules of SRO. In addition to conventional records, such as identification documents, documents enabling determination of the beneficial owner or information regarding the transactions carried out using the account(s) in question, records may also include 'internal investigation reports and the underlying structured documentation on extensive bank records and compliance forms'.[42] In practice, the absence of records or failure to maintain records could result in a situation where the information that needs to be provided to MROS pursuant to Art. 23 para. 2 AMLA in conjunction with Art. 1 para. 2 MROSO will not be available, thereby preventing MROS from being able to effectively analyse SARs and carry out analyses of the reported facts.
If during SAR processing it becomes apparent that a financial intermediary has not fulfilled its safekeeping obligations, MROS is free to inform FINMA, the SFGB or Gespa, and in the future also the OPMC or competent self-regulatory organisations (SROs) and supervisory organisations (see Chapter 6.1.4) of the apparent violation in accordance with Art. 29 para. 1 AMLA or Art. 29b para. 1 AMLA. The investigation of AMLA-related infringements and applicable penalties is not the responsibility of MROS but rather that of the relevant supervisory authorities and bodies.

b. Retention and availability of records under Art. 7 para. 3 AMLA

From MROS's perspective, the obligation to retain records per se does not raise any significant questions in practice. However, there are cases where financial intermediaries have information that is older than ten years. Based on the AMLA, there is no obligation to delete information after expiry of this period. Both in connection with SARs and in connection with MROS enquiries made under Art. 11a AMLA, MROS assumes that the financial intermediary must provide all available information. This also follows from the wording of Art. 11a para. 1 and 2 AMLA, which stipulates that all available information must be provided (principle of availability). Availability refers to 'all parts of the financial intermediary's business that are subject to Swiss jurisdiction'.[43] Just for the sake of completeness, it should be noted that recordkeeping obligations may also arise when a business relationship is taken over by another financial intermediary.
In addition, the obligation to delete records relating to SARs set out in Art. 34 para. 4 AMLA is also discussed, as this is regularly mentioned in connection with the obligation to retain under Art. 7 para. 3 AMLA. Art. 34 para. 1 AMLA stipulates that both the SAR and all related documents

---

40 The formulation 'at least' *(mindestens während 10 Jahren)* only appears in the German version.

41 Thomas Müller, in: *Stämpflis Handkommentar zum Geldwäschereigesetz*, 1st Edition 2017, N 1 regarding Art. 7 AMLA.

42 Federal Supreme Court judgment no 1B_85/2016 dated 20 September 2016, E. 6.4.

43 BBl **2012** 6961

must be destroyed five years after the SAR has been submitted. This obligation now also applies to documents that were sent to MROS by virtue of Art. 11a AMLA.[44]
Irrespective of the controversy surrounding whether the five-year period laid out in Art. 34 para. 4 AMLA is the result of a parliamentary error[45] or not[46], it should be noted that the time limit in Art. 34 AMLA refers only to the documents contained in a separate data file. These are therefore documents that have already been submitted to MROS following a SAR or a request for information in accordance with Art. 11a AMLA. Thus, it is not the original documents within the meaning of Art. 7 para. 3 AMLA that are destroyed, but rather only the copies of these documents, which – according to Art. 34 para. 1 AMLA – must be kept separately from the originals.

6.3 Money laundering and terrorist financing risks in connection with virtual assets

In 2021, MROS examined the extent to which risks of money laundering and terrorist financing (AML/CFT risks) arise in connection with virtual assets (e.g. cryptocurrencies or virtual currencies). The last in-depth risk analysis of the virtual asset sector in Switzerland was carried out by the Interdepartmental Coordinating Group on Combating Money Laundering and the Financing of Terrorism (CGMF)[47]. In its report published back in 2018, the threats and vulnerabilities associated with the use of virtual assets for the purposes of money laundering and terrorist financing in Switzerland were already considered to be 'substantial'. Since then, both the global daily trading volume in virtual assets, the range of uses for them and the sheer number of users have increased many times over. This has created a need for more in-depth analysis of AML/CFT risks in this area. This was necessary not only for Swiss financial intermediaries who increasingly offer services in the field of virtual assets (VASP), but also for those who do not offer such services, since the business relationships they manage may also include transactions linked to such providers.
The growth of the virtual asset sector has also increasingly brought it into the focus of national and international AML/CFT regulations. With the implementation of the virtual asset-specific recommendations adopted by the Financial Action Task Force (FATF) in June 2019 (the Travel Rule for Crypto Assets in particular), financial flows between accounts of financial intermediaries with VASP activities must be made more transparent. At the same time, the standard of control ensuring compliance with due diligence obligations for centralised virtual asset services must be aligned with the one applying to SWIFT payment services.[48] However, the FATF noted in July 2021 that the level of implementation of these recommendations varies widely from country to country.[49]
In Switzerland, FINMA already confirmed in August 2019 that existing provisions (namely Art. 10 AMLO-FINMA) regarding the information to be provided for payment orders, must be interpreted in a technology-neutral manner and thus also ap-

---

44 BBl **2021** 668

45 See Werner de Capitani, in: *Kommentar – Einziehung – Organisiertes Verbrechen – Geldwäscherei*, Volume II, 2002, Art. 34 N 1; Corsin Derungs, Eliane Gmünder in: Stämpflis Handkommentar zum Geldwäschereigesetz, 1st edition 2017, 23f on Art. 34 with reference to other provisions. **Note:** the Federal Council Dispatch adopted in 1996 (BBl **1996** III 1129) also provided for a time limit of only five years to be established in Art. 7 para. 3 AMLA. When the time limit for Art. 7 para. 3 AMLA was increased to ten years following parliamentary discussions in 1997, it was neglected to also adjust the time limit in Art. 34 para. 4 AMLA accordingly.

46 See Stiliano Ordolli, in: Daniel Thelesklaf, et al. (Ed.), *GwG-Kommentar. Schweizerisches Geldwäschereigesetz mit weiteren Erlassen*, Zurich, Orell Füssli, 3rd edition 2019, Art. 34 N 10. More information can also be found in BBl **2021** 668: The five-year period has not been increased to ten years even with the current draft of the AMLA, which seems to indicate that there has been no error on the part of the Swiss Parliament.

47 See CGMF report, *National Risk Assessment (NRA): Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018.

48 See FATF: *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations*, March 2022, pp. 76–77.

49 See FATF: *Second 12-Month Review of Revised FATF Standards – Virtual Assets and VASPs*, July 2021, p. 17.

ply to virtual asset transactions.[50] With the Federal Act on the Adaptation of Federal Legislation to Developments in Distributed Ledger Technology (DLT Act) and the associated implementing ordinance, further amendments aimed at mitigating money laundering risks in the virtual asset sector came into force on 1 August 2021.[51]

Despite the increased attention and undisputed growth of the virtual asset sector, many countries, including Switzerland, have very little information regarding the actual use of virtual assets. In particular, there seems to be no consensus at present on which metrics can be used by individual countries to analyse economic activities and financial flows in the virtual asset sector, which is essentially global. As a result, there are no reliable figures that could shed light on the frequency and size of virtual asset-related financial flows within and through the Swiss financial sector. This lack of information increases the risk that unexpected developments will remain undetected for a longer period of time and expose the Swiss financial sector both economically and politically.

An analysis of the SARs received shows that the majority of SARs relating to virtual assets come from financial intermediaries who do not themselves carry out VASP activities, but whose suspicions relate to business relationships involving transactions with VASPs, which are generally based abroad. Additionally, only a small minority of Swiss financial intermediaries with VASP activities submitted SARs to MROS. However, due to the lack of data mentioned earlier, it is difficult to determine whether this is due to the low level of business activity of the corresponding financial intermediaries, the absence of money laundering risks, or a lack of awareness of money laundering risks and the associated due diligence and reporting obligations. SARs related to virtual assets generally reveal strong international links in terms of financial flows, reported counterparties, as well as suspected predicate offenses, which cover a broad spectrum beyond cybercrime-related offenses. The analysis of SARs also showed that the reporting financial intermediaries that engage in VASP activities mainly stated that it was contacts from prosecution authorities or third-party banks that prompted the SARs. Only on very few occasions were tracing tools mentioned as the trigger for reporting to MROS.

Financial intermediaries can bring considerable added value to MROS if they submit a SAR together with analyses already carried out using tracing tools. As things currently stand, however, financial intermediaries do not use tracing tools in a uniform manner (especially with regard to the number of hops investigated). The transparency of blockchains offers opportunities for real-time monitoring of virtual asset-related financial flows that are not yet adequately taken into account and that cannot be observed via the traditional methods of monitoring payments traffic. In addition to tracing tools, digital information can be linked to people and events in the analogue world, creating unprecedented opportunities for in-depth analysis. In this way, the use of tracing tools enables MROS to quickly provide important information to Swiss prosecution authorities and foreign partner authorities, thus facilitating their investigations and proceedings (see Chapter 5.5).

Both authorities and financial intermediaries need to keep up with the pace of technological advances and continuously review and adapt their assessments, verifications and investigative tools so that virtual assets do not become a safe haven for criminals and terrorists. This is particularly true in the case of existing gaps in the monitoring of virtual asset financial flows (e.g. privacy coins) as well as in the context of certain areas of crime that are not easy to identify even with tracing tools.

---

50 See *FINMA Guidance 02/2019.*

51 See Federal Act of 25 September 2020 on the Adaptation of Federal Legislation in Response to Advances in Distributed Ledger Technology, (BBl **2020** 7801); Ordinance of 18 June 2021 on Adaptation of Federal Legislation in Response to Advances in Distributed Ledger Technology, (AS **2021** 400).

7. International cooperation in the fight against money laundering

7.1 Egmont Group

MROS is a member of the Egmont Group, a network of 167 financial intelligence units (FIUs) specialised in detecting and combating money laundering, its predicate offenses and terrorist financing. The Egmont Group can be considered as an international forum of operationally independent FIUs. Since the revision of the FATF Recommendations in 2012, membership in the Egmont Group is a clear prerequisite for an adequate anti-money laundering and counter-terrorism system.

The Egmont Group pursues the following objectives:

- Create the conditions required for the systematic exchange of information worldwide;
- Help to improve the efficiency of FIUs through training strategies and staff exchange programmes;
- Facilitate the sharing of information between FIUs worldwide under secure conditions, using state-of-the-art technologies such as stand-alone Internet connections.
- Encourage the operational independence of FIUs;
- Support the establishment of centralised hotlines.

In general, COVID-19 restrictions severely limited Egmont Group activity in 2021 and made international collaboration difficult, as all meetings had to be conducted online. Thus, the two main meetings of the Egmont Group, the Working Group Meetings scheduled for February 2021 and the Egmont Plenary scheduled for June and July, were also held online.

The Working Group Meetings that took place in February focused mainly on the various projects carried out by individual working groups. A key topic was the 'Trade-Based Money Laundering (TBML) Project', which is jointly pursued by the FATF and the Egmont Group, under the lead of FIU Germany. The TBML project is intended to produce a list of indicators of trade-based money laundering risks as well as an e-catalogue of Virtual Asset Service Providers (VASPs). This topic is becoming increasingly important in the fight against money laundering. A new project on 'Corruption and Asset Recovery' was also proposed to address, among other things, corruption during the COVID-19 pandemic and corruption related to organised crime.

In its 2020 annual report, MROS already reported on the non-compliance proceedings brought against MROS by the Egmont Group for a lack of adequate powers in international cooperation.[52] These proceedings were discussed at the meetings of the Egmont Group's Membership, Support and Compliance Working Group (MSCWG). As MROS was given new competences in connection with Art. 11a para. 2bis AMLA in July 2021 (see Chapter 2.2), the Egmont Group dropped its proceedings against MROS in December 2021.

[52] See *2020 MROS Annual Report,* Chapter 6.2.1.

7.2 GAFI/FATF

The Financial Action Task Force (FATF) is an intergovernmental organisation established by the G7 at a ministerial meeting in Paris in July 1989. The FATF is the leading international organisation in the international fight against money laundering and terrorist financing. It sets the standards of the measures to combat these crimes and periodically evaluates the implementation of its recommendations in the individual member states, which are required to implement the FATF recommendations. The results of the evaluations and the corresponding justifications are compiled and published as a report for each State.

The fourth round of evaluations, which is currently underway, will examine the level of compliance (technical compliance) and effectiveness of implementation (effectiveness) of the FATF recommendations.

Switzerland participates in various FATF working groups: the Policy Development Group (PDG), which is responsible for aspects relating to regulations and guidelines; the Evaluations and Compliance Group (ECG), which is responsible for monitoring and ensuring the consistency of the mutual evaluations and the subsequent process (follow-up process); the International Co-operation Review Group (ICRG); and the Global Network Coordination Group (GNCG). Within the framework of the FATF, MROS, as a member of the Swiss delegation, participates in the meetings of the Risk Trends and Methods Group (RTMG), the working group responsible for analysing money laundering risks, the means used for this purpose and the observable trends in this area. The aim is to identify and analyse recurring patterns and characteristics of offences related to money laundering and terrorist financing on the basis of concrete cases, in order to combat these offences more effectively. The reports published by the FATF in 2021 in the category 'Methods and Trend' deal with the criminal prosecution of financial flows from environmental crime, right-wing extremist terrorism and trade-based money laundering (TBML).[53]

The FATF recently revised its standards to require countries and their financial sectors to identify, adequately assess, and mitigate their proliferation financing risks (any support for the development and transfer of weapons of mass destruction). In this regard, guidelines were published in June 2021 (Guidance on Proliferation Financing Risk Assessment and Mitigation[54]). Among other things, this document contains an updated list of indicators of possible illegal activity as well as non-implementation or circumvention of sanctions applied to counter proliferation financing. Assessing and mitigating risks in this area requires close cooperation between the public and private sectors. The FATF will continue its efforts in this regard.

Several new projects are also underway at the FATF, including those on human smuggling and illicit trafficking in art or cultural goods. At the Joint Experts Meeting (JEM) in December 2021, it was stated that the art and antiquities trade is a high-risk sector for money laundering and terrorist financing. Markets are poorly regulated and prices of individual objects are subjectively set and difficult to compare. Easily accessible social media platforms play a key role in illicit trade. This situation benefits, among others, terrorist organisations, which aim to smuggle stolen cultural goods into the legal market in this way. According to MROS estimates, Switzerland could also be exposed to considerable risks due to the importance of its art market.

7.3 Europol Financial Intelligence Public Private Partnership (EFIPPP)

In September 2019, MROS became a member of the public-private partnership in the fight against money laundering and terrorist financing organised by Europol. This partnership, called 'The Europol Financial Intelligence Public Private Partnership' (EFIPPP), is part of Europol's new European Financial and Economic Crime Centre

[53] See FATF Methods and Trends.

[54] See *Guidance on Proliferation Financing Risk Assessment and Mitigation*, June 2021.

(EFECC).[55] The EFIPPP consists of representatives of various authorities, including financial intelligence units (FIUs), law enforcement agencies and customs offices, on the one hand, and representatives of the private sector on the other. In particular, private-sector delegates represent internationally prominent banks, including Swiss financial intermediaries. Other European or international institutions – such as the FATF – or representatives of the academic world also take part in this partnership, holding observer status. The plenary sessions of this partnership take place four times a year at Europol's offices in The Hague. The main objective is to intensify the exchange of strategic, non-operational information between the public and private sector. A number of relevant topics relating to efforts to counter money laundering and terrorism financing are discussed at the sessions.

Currently, the EFIPPP has established the following working group structure:

- Threats & Typologies Working Group
  - Terrorist Financing & Proliferation Financing work stream
  - Crypto Assets work stream
  - Business Email Compromise work stream
  - Mule Accounts work stream
  - Investment Fraud work stream
  - Virtual IBANS work stream
- Innovation Working Group
- Legal Gateway Working Group

EFIPPP also allows its various participants to exchange views on the development (and/or creation) of national public-private partnerships in the context of the fight against money laundering and terrorism financing. Since 2020, MROS has attended several working group sessions. This participation has allowed it to determine whether certain trends identified by members of the partnership could pose a threat to Switzerland. MROS was also able to report on its own findings as to whether or not similar trends exist in Switzerland. A variety of topics were discussed in this regard, such as the change in money laundering risks caused by the pandemic, the risks associated with the use of virtual IBANs or the use of cryptocurrencies in money laundering schemes.

Over time, the information available to MROS through its participation in the EFIPPP could also be shared with Swiss financial intermediaries, possibly within the framework of a similar Swiss partnership (for more information see Chapter 2.3).

The EFIPPP plenary session was held from 1 to 2 December 2021. On this occasion, MROS presented the results of the last seminar in Lausanne, organised by the Directorate of Public International Law (DDIP) of the Federal Department of Foreign Affairs, in collaboration with the International Centre for Asset Recovery and with the support of the Stolen Asset Recovery Initiative (World Bank/UNODC). Participants at this seminar explored the potential for cooperation between public and private stakeholders in the area of asset recovery.

Swiss Financial Market Supervisory Authority (FINMA)

[55] See the website of the European Financial and Economic Crime Centre – EFECC | Europol (europa.eu).