Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

August 2021

National risk assessment (NRA)

Report on the national assessment of the risks of money laundering and terrorist financing in Switzerland

Report of the interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF)

Contents

Executive summary **4**

Introduction **6**

1. Recap of the main findings of the 2015 NRA report and subsequent sectoral studies. **7**

1.1. National risk assessment report published in 2015 (2015 NRA report) 7

1.2. Sectoral reports 9

1.2.1. Report on money laundering and terrorist financing risks in non-profit organisations (NPOs) 9

1.2.2. Money laundering risks in the case of legal entities 10

1.2.3. Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding 10

1.2.4. Report on the use of cash and the risks of it being misused for money laundering and terrorist financing in Switzerland 11

1.2.5. Bribery as a predicate offence to money laundering 12

1.2.6. Supervision of commodity trading activities from a money laundering perspective 13

1.2.7. Fraud and phishing for the purpose of fraudulent misuse of a data processing system as a predicate offence to money laundering 13

2. Trends in money laundering risk, 2015-2019 ..... **14**

2.1. Statistical comparison of the 2004-2014 and 2015-2019 periods 14

2.1.1. Number of reports received by MROS 15

2.1.2. Breakdown of the seven main predicate offences identified 15

2.1.3. Money laundering without the mention of a predicate offence 16

2.1.4. Involvement of a domiciliary company 16

2.1.5. Financial intermediaries making reports 16

2.1.6. Domicile of contracting parties 17

2.1.7. Amounts deposited on accounts reported to MROS on date of reporting 18

2.2. Impact of the main international money laundering incidents in Switzerland, 2015-2019 19

2.3. Conclusions from the statistical comparison 21

2.4. Predicate offences 23

2.4.1. Bribery 23

2.4.2. Fraud and computer fraud 24

2.4.3. Misappropriation and criminal mismanagement 25

2.4.4. Criminal organisation 25

2.4.5. Money laundering 26

2.4.6. Aggravated tax misdemeanour 26

2.4.7. Terrorist financing 26

2.5. Financial intermediaries 26

2.6. Evolution of risks in non-financial sectors 28

2.7. Action by prosecution and supervisory authorities 29
3. Legal and operational measures for limiting the sectoral risks identified since 2015 31
3.1. Federal Act for Implementing the Revised Financial Action Task Force Recommendations of 2012 32
3.2. Increasing the effectiveness of precious metals control 32
3.3. Changes with regard to bonded and open customs warehouses 33
3.4. Exchange of information on tax matters 34
3.5. Federal Decree on the Approval and Implementation of the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol and the Strengthening of Criminal Justice Instruments for combating Terrorism and Organised Crime 35
3.6. Revision of the Anti-Money Laundering Act and additional measures in connection with the FATF mutual evaluation 37
3.7. Consultation procedure on the Amendment of the Land Register Ordinance 38
3.8. Innovations in the area of virtual assets (VA) and virtual asset service providers (VASPs) 38
3.9. Federal Act on the Freezing and the Restitution of Illicit Assets held by Foreign Politically Exposed Persons (FIAA) 40
4. Changes in risks since 2015 41
4.1. Online casinos 41
4.2. Terrorist financing 43
4.3. Cryptocurrencies 46
5. Conclusion 49
Annex: Summary table of recommendations made in analysis reports published since 2015 and changes to the mechanisms to combat money laundering and terrorist financing adopted as a result 50
Bibliography 55

Executive summary

Understanding the money laundering and terrorist financing risks faced by a country is a key component of any strategy to mitigate them. The interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF) therefore decided to assess how these risks have evolved since the publication of the first national risk assessment in 2015 (now known as the 2015 NRA report).

That assessment has resulted in this report. It presents the trends of money laundering risk between 2015 and 2019. It reviews the legislative and regulatory measures adopted since then to improve Switzerland's anti-money laundering and counter terrorist financing framework. Finally, it identifies the new risks that have emerged, as well as the areas of activity and crime types for which the risks have changed substantially.

The first chapter presents how the risks were assessed in the 2015 NRA report and in the subsequent sectoral risk analysis reports, which have made it possible to gain a more in-depth knowledge of the risk of money laundering and terrorist financing in different areas (non-profit organisations, legal entities, cryptocurrencies and crowdfunding, cash, bribery, fraud, commodity trading). By summarising the various analyses, this report allows for a comparison of the money laundering and terrorist financing risk as identified in the report with the current situation in the Swiss financial centre.

In order to make this comparison, the second chapter examines the main money laundering and terrorist financing trends that emerge from the analysis of the suspicious activity reports (SARs) received by MROS, criminal proceedings and international mutual assistance procedures in the period from 2015 to 2019, and views them in the light of the risks identified in the 2015 report.

The analysis is based on the SARs received by MROS, information available to the judicial, police and customs authorities and that from the financial supervisory authorities, and highlights some noteworthy developments: the number of SARs sent to MROS has risen sharply; bribery has become the most frequently cited predicate offence, while fraud is less frequently cited than in the past; suspicions of money laundering reported to MROS without a specific predicate offence having been identified have increased in number; the business relationships indicated are more often established in the name of domiciliary companies; the assets reported are significantly higher and the SARs originate from the banking sector even more frequently than in the past. However, by comparing the results of the SAR analysis with the sources of the other authorities involved in combating money laundering, the report considers that these developments reflect a change in the behaviour of financial intermediaries, specifically banks, and the economic effects of several major international money laundering cases rather than a change in the money laundering risk facing the Swiss financial centre.

The period from 2015 to 2019 was marked by large-scale foreign corruption cases (Lava Jato in Brazil, 1MDB in Malaysia, PDVSA in Venezuela), major financial data leaks, such as the Panama Papers and the Paradise Papers, and several laundromat cases, i.e. schemes for the massive movement of funds of dubious origin from former USSR countries to Western Europe, often via Baltic banks. These three types of case had a huge impact on the Swiss financial centre during the period under review. It explains the statistical developments observed since 2015, but it reflects a bygone era rather than the current state of money laundering.

Apart from the cyclical variations caused by the impact in Switzerland of these international money laundering cases, the risk of money laundering has changed little since 2015. In terms of SARs, criminal proceedings initiated for money laundering and international mutual assistance procedures, Switzerland continues to be exposed primarily to the laundering of money from prior offences committed abroad. This can be explained by the country's extremely international financial centre. As a result, the financial intermediation sectors that are the most vulnerable to money laundering remain banks, asset managers, fiduciaries, lawyers and notaries, while in the non-financial sectors, commodity trading activities continue to carry a significant risk.

Despite variations in their rankings, the same predicate offences as in 2015 are still being reported today, i.e. bribery, fraud, misappropriation, criminal mismanagement, computer fraud and membership of a criminal organisation. The only significant change in terms of predicate offences is the appearance of aggravated tax misdemeanours among the main suspected predicate offences. As it did not become a predicate offence to money laundering until 2016, the development of the money laundering risk associated with it cannot be assessed precisely.

The third chapter presents the main measures adopted since 2015 to mitigate the risk of money laundering. It provides a summary of the various legislative and regulatory changes that were often adopted in response to the recommendations of risk assessment reports and help to address the shortcomings identified in the Swiss anti-money laundering framework.

The final chapter describes the three areas where the risk seems to have changed since 2015, i.e. online casinos, which were not authorised in Switzerland until 2019; terrorist financing; and cryptocurrencies, whose rapid development and growing popularity are bringing new risks to the fore.

Introduction

Switzerland constantly assesses the risks associated with money laundering and terrorist financing in order to effectively combat these crimes. This work is carried out under the aegis of the interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF). Established by the Federal Council on 29 November 2013, the CGMF is a permanent group charged with coordinating Switzerland's anti-money laundering and counter terrorist financing policy. In accordance with recommendations 1 and 2 of the Financial Action Task Force (FATF), the CGMF conducts risk analyses to assess the money laundering and terrorist financing threats and vulnerabilities in order to identify and address possible gaps in the regulatory framework.[1]

Switzerland published its first national assessment report on money laundering and terrorist financing risks in 2015.[2] That report provided a comprehensive overview of the risk situation and was supplemented by a number of sectoral reports. The various reports made it possible to identify the main money laundering and terrorist financing risks to which the Swiss financial centre is exposed and proposed measures to mitigate them. Since criminal circles are constantly refining their money laundering and terrorist financing techniques, it is necessary to continually monitor and regularly update the comprehensive risk analysis and adapt the measures to combat these phenomena. This is the only way to assess the effectiveness of the Swiss system and to react to new threats.

Six years after the publication of the first national risk assessment, the latest report provides an updated overview of the money laundering and terrorist financing risks in Switzerland. Like the analysis published in 2015, this assessment is based primarily on the statistical analysis of the SARs received by the Money Laundering Reporting Office of Switzerland (MROS), supplemented by information from criminal proceedings, international mutual assistance procedures concerning money laundering and other anti-money laundering and counter terrorist financing authorities. The views of the private sector, especially the self-regulatory organisations (SROs), were likewise sought.

The analysis begins by presenting the main findings of the 2015 NRA report and of the sectoral risk analysis reports published after that. This presentation makes it possible, in the second chapter, to compare the risks identified since 2015 with the current risks as they emerge from the review of the SARs received by MROS between 2015 and 2019, criminal proceedings and international mutual assistance procedures initiated during this period and the information available to the financial market supervisory authorities. The third chapter presents the measures taken since 2015 to mitigate the risks identified. In that regard, it examines the implementation of the recommendations made in the NRA and sectoral risk analysis reports summarised in the first chapter. Finally, the last chapter identifies the sectors and types of crime that appear to carry a risk that changed significantly during the period under review.

[1] Financial Action Task Force (FATF), *National Money Laundering and Terrorist Financing Risk Assessment,* 2013, p. 6, National Money Laundering and Terrorist Financing Risk Assessment (fatf-gafi.org)
[2] CGMF, *Report on the national evaluation of the risks of money laundering and terrorist financing in Switzerland*, 2015, https://www.newsd.admin.ch/newsd/message/attachments/42276.pdf (2015 NRA report)

1. Recap of the main findings of the 2015 NRA report and subsequent sectoral studies

The publication of the first national risk assessment report in 2015 (2015 NRA report) allowed a general overview of the money laundering and terrorist financing risks in Switzerland to be drawn up. It was supplemented by various sectoral reports on the main threats, which explored the risks in greater detail. Aside from these analyses conducted under the aegis of the CGMF, other interdepartmental reports published since 2015 examined the money laundering risk in specific sectors. This chapter presents those analyses' findings and recommendations.

1.1. National risk assessment report published in 2015 (2015 NRA report)

Undertaken as part of the FATF mutual evaluation of Switzerland, the 2015 NRA report aimed to analyse and assess all of the money laundering and terrorist financing threats at national level, identify Switzerland's vulnerabilities in the area, i.e. the factors that enable the threats to materialise, and draw conclusions concerning the level of risk found after weighting those factors.

With regard to money laundering, the report states that the financial intermediaries that are the most exposed to money laundering risks are banks (especially universal banks and private wealth management banks – private banking), independent asset managers, fiduciaries, lawyers, notaries and money transmitters, although the level of risk may differ depending on the financial intermediary. For example, the analysis showed that banks are only exposed to a medium risk overall. This is because of the consolidated regulations that are rigorously applied by the sector and FINMA's direct risk-based supervision. However, the risk is heightened if we look solely at universal banks and wealth management banks. The same is true for asset managers, fiduciaries, lawyers and notaries. This is due to the complexity of their business relationships, which very often involve legal constructs, and higher risks related to the presence of politically exposed persons (PEPs). In the case of securities dealers, the risk is heightened primarily where trading is carried out for the account of clients and they are offered wealth management services and account management. The risks for money transmitters vary according to the countries receiving the transferred funds and because of the difficulty of performing checks on the auxiliary persons acting in the name and on behalf of the main financial intermediary. Payment transfer services generally entail a medium level of risk, but this may rise depending on the technology used and the degree of regulation in the service provider's place of domicile. Precious metals trading is generally associated with a medium level of risk, but this rises for cross-border trading in refined gold involving foundries, as well as for retail trade in scrap gold. Finally, a low risk of money laundering can be assumed for insurance companies, casinos and credit and leasing services. The report concludes that, as of 2015, a medium risk can be assumed for all sectors as a whole subject to the AMLA[3]. It notes that the existing legislative system and the associated measures are sufficient to control the vulnerabilities with regard to the threats present.

[3] *Federal Act of 10 October 1997 on Combating Money Laundering and Terrorist Financing*, (Anti-Money Laundering Act, AMLA, RS 955.0)

With regard to predicate offences to money laundering, the report uses a method that combines quantitative data with a qualitative approach to show which predicate offences pose the greatest threats to the Swiss financial sector. A particularly high risk of money laundering was identified in the case of acts of corruption abroad and membership of a criminal organisation, as these predicate offences are extremely complex and involve large sums of money, and it is difficult for the criminal prosecution authorities to provide evidence of felonies committed abroad. At the national level, the predicate offences concerned street crime in particular, including drug trafficking.

With respect to terrorist financing, the report states that there is a limited risk in Switzerland, especially in the area of financial intermediation. Nevertheless, the 2015 NRA report stresses that the risk of terrorist financing could rise rapidly if networks systematically used alternative financial transfer procedures that are not subject to the AMLA, namely the hawala system or cash transport. Furthermore, the investigations revealed that financial intermediaries, i.e. banks, money transmitters and credit service providers, were the most exposed. The sums of money involved are often small.

Aside from close national and international cooperation, it is necessary to raise the awareness of social players, especially NPOs, and use other available legal means in order to control the risk in the area of terrorist financing.

The report concludes that the legislative system in place at the time takes sufficient account of the risks of money laundering and terrorist financing. However, it states that greater use should be made of the instruments provided for by law in operational settings, which is why several measures are recommended in order to strengthen the system:

- Intensify dialogue with the private sector about risks.
- Continue the OAG's collection and analysis of data on money laundering and terrorist financing from the federal and cantonal criminal prosecution authorities, and compile consolidated statistics on the handling of such cases.
- The public and private players involved in combating money laundering and terrorist financing are to further develop and systematise the statistics, taking into consideration the quantitative methods used in this report.
- Perform risk analyses.
- Rapidly introduce the national real estate register accessible to the federal authorities as envisaged in the Federal Council dispatch of 16 April 2014, in order to reduce the vulnerabilities identified in the real estate sector.
- Enhance supervision and reduce the risk of foundations being used for money laundering and terrorist financing purposes by strengthening the Federal Supervisory Board for Foundations and providing it with additional resources.
- Put the Federal Council's strategy on customs warehouses into practice by implementing the recommendations of the Swiss Federal Audit Office and by establishing and applying a legal framework at ordinance level.
- Incorporate into the future bill and the corresponding dispatch for the attention of Parliament the proposals in the preliminary draft of the amendment to the Swiss Code of Obligations (law on companies limited by shares) concerning the accounting rules for raw materials extraction companies, which should lead to greater transparency, and extend these rules to the commodity trading sector as part of an internationally coordinated approach.

1.2. Sectoral reports

During its constituent sitting in February 2014, the CGMF decided to focus specifically on selected topics in addition to the general analysis of money laundering and terrorist financing risks (2015 NRA report). Since then, reports have been published on various topics relating to money laundering and terrorist financing. These reports are briefly explained below. These sectoral reports are supplemented by other Federal Council risk analysis reports (e.g. supervision of commodity trading activities from a money laundering perspective). They are additionally mentioned in this report, as they likewise analyse risks that contribute to the fight against money laundering and terrorist financing and are the result of interdepartmental discussions and work within the CGMF.

1.2.1. Report on money laundering and terrorist financing risks in non-profit organisations (NPOs)[4]

The CGMF's targeted analysis report on money laundering and terrorist financing risks at NPOs was prepared in summer 2017 under the auspices of the Federal Office of Police (fedpol). In particular, it examines the extent to which non-profit organisations (NPOs) can be misused for money laundering and terrorist financing purposes.

The report shows that the NPOs that are exposed to the greatest risk of being misused for terrorist financing purposes are those that operate in or near conflict zones, where state power is weakened or has collapsed, where terrorist groups are active or even exercise territorial rule.

Despite the fundamental appeal of NPOs for money laundering and terrorist financing, only a few cases of criminal acts by NPOs are known internationally, and such acts could be established by courts under the rule of law in even fewer cases. In summary, the analysis report thus concludes that the entire set of legal provisions on NPOs and the control mechanisms based on them are to be considered sufficient to effectively prevent and combat terrorist financing through NPOs. Nevertheless, for the sake of transparency and awareness-raising in the NPO sector, it seems appropriate to examine measures that facilitate the management of NPO-specific risks, especially those of fundraising associations. The following recommendations were made:

1. Extend the obligation to enter associations in the commercial register to include associations with a heightened terrorist financing risk, as well as the obligation to maintain a member list for registered associations.
2. Continue to consistently implement the provisions on combating money laundering and terrorist financing.
3. Raise awareness in the NPO sector: it is advisable to raise awareness of the risk of money laundering and terrorist financing throughout the NPO sector, as well as among the general public, financial intermediaries and the competent authorities. An initial measure could be the publication of a factsheet, for example.

[4] CGMF, *Report on money laundering and terrorist financing risks in non-profit organisations*, June 2017, nra-bericht-juni-2017-d (6).pdf

1.2.2. Money laundering risks in the case of legal entities[5]

The report on money laundering risks in the case of legal entities published in November 2017 examined the risk of money laundering and terrorist financing posed to the Swiss financial centre by commercial legal entities, essentially the various corporate forms. The report distinguishes between Swiss commercial legal entities that are directly subject to Swiss legislation and foreign companies that merely use financial services – and primarily banking services – in Switzerland. Furthermore, the report examines the difference between domiciliary companies and companies that have operating activities. The report additionally analyses the specific risk posed by the advisory activities of Swiss players (lawyers, notaries and fiduciaries) with regard to the establishment and management of foreign companies in particular.

With respect to the distinction between Swiss and foreign companies, the report concludes that foreign companies carry a significantly higher risk of money laundering. They are more frequently the subject of suspicious activity reports (SARS) and exacerbate the threat to the Swiss financial centre due to certain features: their business relationships involve more players, higher amounts of money, more domiciliary companies and more politically exposed persons. With regard to terrorist financing, it is noted that commercial legal entities constitute only a limited risk.

Among the various corporate forms, a high risk is posed mainly by companies limited by shares (including subsidiaries and branches) due to their involvement in international business and financial cycles, as do domiciliary companies because of their lack of transparency. In the establishment and management of such domiciliary companies, the focus is additionally on the role of lawyers, notaries and fiduciaries, who act in an advisory capacity when such companies are being established. Since the provision of such services *per se* is not subject to the AMLA, these activities are not subject to due diligence and reporting obligations under the Anti-Money Laundering Act either. Nevertheless, these service providers come under the AMLA as soon as they hold an executive body position in a domiciliary company or carry out financial transactions for third parties on a professional basis.

1.2.3. Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding[6]

In this report published in December 2018, the CGMF investigated two of the main uses of fintech: crypto assets and crowdfunding. The report first looks at the risks related to crypto assets before briefly addressing those related to online crowdfunding. The report notes that, to date, not one case of terrorist financing via crypto assets or online crowdfunding has been identified, and only a few cases of money laundering using these new technologies. Nonetheless, the report concludes that the risks stemming from these technologies and Switzerland's vulnerability in this area are considerable, and affect not just Switzerland, but every country. The main threat associated with cryptocurrencies is the anonymity of token transactions, and the fact that a large proportion of transactions are peer-to-peer, i.e. without a financial intermediary, which means that they are unregulated and unsupervised. This is compounded by the speed of transactions and their cross-border nature. The threat involves the criminal exploitation of cryptocurrency design flaws, investor fraud, especially in the context of initial coin offerings (ICOs), and the use of cryptocurrencies for ransomware payments. Moreover, the threat posed by cryptocurrencies also arises from their use for illegal purposes in criminal activity such as terrorist financing, money laundering originating from the sale of

[5] CGMF, *Money laundering risks in the case of legal entities*, November 2017, National Risk Assessment (NRA) - D (4).pdf

[6] CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, https://www.newsd.admin.ch/newsd/message/attachments/56167.pdf

illegal products and services, online phishing scams, as well as drug trafficking, especially in the hands of criminal organisations. With crowdfunding too, the main risk lies in anonymity, particularly on the part of the donors. Against this backdrop and in order to take the growing cryptocurrency risks into consideration, FINMA drew investors' attention to the risks associated with ICOs as early as 2017 and has since implemented technology-neutral regulations that take the FATF standards into account and govern cryptocurrency providers.

Moreover, crypto assets pose a technological challenge for the prosecution authorities. After all, crypto assets are generally cross-border in nature, making international mutual assistance requests or cooperation between police forces necessary to investigate the associated economic crimes.

In order to combat the risks associated with crypto assets, Switzerland, working within the FATF, is advocating greater harmonisation of national regulations. This is supplemented by regular training on cybercrime for the prosecution authorities and the creation of a national platform for judicial and police cooperation. In addition, the AMLA in Switzerland already covers a wide range of services that involve trading and transactions in crypto assets. The report therefore concludes that these efforts have resulted in a good regulatory system for combating the considerable risk posed by crypto assets. Despite this, it is not possible to eliminate all vulnerabilities – that would require an international solution, owing to the international nature of transactions.

1.2.4. Report on the use of cash and the risks of it being misused for money laundering and terrorist financing in Switzerland[7]

The CGMF's sectoral report examines the risks of cash being misused for money laundering and terrorist financing purposes in Switzerland, and takes account of the FATF's 2016 mutual evaluation report, which called on Switzerland to investigate the risks associated with the use of cash on its territory. The FATF justified this demand with the size of the Swiss financial centre and Switzerland's strong tradition of using cash.

In connection with the risk of cash being misused for money laundering and terrorist financing in Switzerland, the report, which was published in 2018, notes that repeated use of cash for criminal purposes is observable only for laundering the proceeds of drug trafficking and fraud, especially online fraud. Among financial intermediaries, it is money transmitters and casinos that are most affected by the risks associated with cash.

In order to reduce the risk of cash being used for money laundering and terrorist financing, the FATF recommends that thresholds be introduced for cash transactions, trading in precious metals and precious stones, exchanging currency and cashing in chips in a casino. If these thresholds are reached, financial intermediaries must exercise due diligence. Swiss legislation also contains such thresholds, following the entry into force of the Federal Act for Implementing the Revised FATF Recommendations of 1 July 2016. In addition, the revised AMLO-FINMA[8] and CDB[9] lowered the threshold for cash transactions from CHF 25,000 to CHF 15,000 with effect from 1 January 2020.

[7] CGMF, *Report on the national evaluation of the risks of money laundering and terrorist financing in Switzerland*, October 2018, https://www.newsd.admin.ch/newsd/message/attachments/55177.pdf

[8] *Ordinance of the Swiss Financial Market Supervisory Authority of 3 June 2015 on the Prevention of Money Laundering and the Financing of Terrorism*, (FINMA Anti-Money Laundering Ordinance, AMLO-FINMA, SR 955.033.0)

[9] Swiss Banking, *Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CDB 20)*, 2020, SBA_Agreement_CDB_2020_EN.pdf (swissbanking.ch)

The report concludes that cash carries a risk of money laundering and terrorist financing. However, owing to the preventive and repressive measures taken, and given the specificities of the Swiss financial centre with the strong international focus of its banking sector, this risk can be categorised as moderate.

1.2.5. Bribery as a predicate offence to money laundering[10]

Since 2015, bribery has replaced fraud as the most reported money laundering offence. Between 2008 and 2010, less than 10% of SARs to MROS concerned bribery, but in 2017 this had risen to over 23%. Bribery also accounted for 23% of predicate offences to money laundering in the cases dealt with by the OAG between 2010 and 2015. The increase in the figures demonstrates the considerable money laundering risk that bribery poses for the Swiss financial centre. The sectoral report published in April 2019 therefore discusses the money laundering risk posed to the Swiss financial centre by bribery.

The report reveals that the greatest threat stems from both active and, above all, passive corruption on the part of foreign officials in general and politically exposed persons (PEPs) in particular. For example, the report notes that a PEP is involved in over one third of business relationships that are reported on suspicion of bribery-related money laundering. According to the report, PEPs are also most frequently the subject of bribery-related SARs: more than half of the PEPs mentioned in the reports have featured in SARs involving bribery as a probable predicate offence. Domestic bribery associated with money laundering accounts for only 1% of all reports to MROS. It also emerges from the report that the involvement of legal entities – usually more than one and predominantly domiciliary companies – mainly registered in Central America or the Caribbean, is a defining characteristic of corruption-related money laundering systems. Swiss legal entities involved in suspected money laundering linked to foreign corruption are largely operating companies limited by shares that are often active in the areas of financial advice and financial management.

Assets from foreign corruption are rarely placed directly in Swiss bank accounts. They generally enter the legitimate financial system abroad and are then transferred onto Swiss accounts, from where they are moved to other countries. This makes it more difficult to identify the origin of the assets. However, the money can also be invested in Switzerland through the purchase of real estate, luxury goods or life insurance, for example. The stage in the money laundering process that involves the greatest risk for the Swiss financial centre is the layering stage, followed by the integration stage. The placement stage poses a slight, but non-negligible, risk.

The report shows that the predicate offence of bribery, in particular international corruption, poses an increased money laundering risk to the Swiss financial centre. All risk indicators point to this. The business relationships in SARs to MROS for probable bribery-related money laundering include above-average numbers of domiciliary companies (they account for 44.4% of the counterparties in the business relationships reported for suspicions of bribery, compared with 34.6% of the counterparties in all reported business relationships[11]), PEPs, high-risk countries, monetary amounts and participants. However, thanks to the effective Swiss legislation and the money laundering regulations, this increased risk is well controlled. Prosecution by the Swiss judicial authorities is effective and has resulted in a number of convictions. In addition, potentially relevant information on bribery-related money laundering is exchanged with foreign reporting offices, and FINMA ensures effective supervision of financial intermediaries. Moreover, the legal and institutional framework on combating the risk of money

[10] CGMF, *Corruption as a predicate offence to money laundering,* April 2019, 20190710_ber-korruption-geldwaescherei-d-final.pdf.download.pdf
[11] *Ibid*., p. 40

laundering in connection with the predicate offence of domestic or foreign bribery has been, and continues to be, regularly reinforced with new laws and bills.

1.2.6. Supervision of commodity trading activities from a money laundering perspective[12]

On 26 February 2020, the Federal Council published a report in response to the Seydoux-Christe postulate (17.4204). It assesses the extent to which banking controls in the area of commodity trade finance help to mitigate these risks.
The report notes that the Swiss financial centre is highly exposed to the risk of money laundering associated with commodity trading, through both its banks and the traders based in Switzerland. Nevertheless, it concludes that the authorities responsible for implementing anti-money laundering legislation have, to a very large extent, the legal basis and the means to prevent money laundering and the corruption inherent in it. It points out that combating corruption is essential to reduce the risk of money laundering in the Swiss financial system. Furthermore, it deems the banks' due diligence duties and their implementation to be appropriate overall. However, it considers that the effectiveness of the existing framework could be strengthened in a targeted manner and identifies five areas for action in this regard:

- Private sector implementation of anti-corruption initiatives
- Development and adoption of sector-specific guidelines on anti-money laundering due diligence
- Assessment of the scope of the duty to report suspicions
- International commitment to treating relationships with state-owned enterprises (SOEs) and companies that themselves have business relationships with SOEs as criteria for heightened risk
- Improvements to the anti-corruption mechanisms

1.2.7. Fraud and phishing for the purpose of fraudulent misuse of a data processing system as a predicate offence to money laundering[13]

In 2020, the CGMF published a report on fraud and phishing aimed at misusing data processing systems as a predicate offence to money laundering. The report was motivated by the fact that fraud and its digital counterpart, computer fraud, have consistently featured among the most often cited predicate offences in SARs to MROS since 2004 (between 2004 and 2014, it was the most often named predicate offence, accounting for 39.80% of reports; between 2015 and 2019, it was the second most often named predicate offence, accounting for 26.63%, but often for small amounts, since between 2009 and 2018, 67% of reports related to fraud and 79% of those related to computer fraud involved sums of less than CHF 10,000[14]).

The greatest vulnerabilities are considered to be the use of financial agents and foreign-domiciled legal entities. Furthermore, developments in information and communication technologies have provided a multitude of opportunities to internationalise predicate offences and the associated money laundering. In addition, the use of crypto assets for money laundering purposes could potentially constitute a huge vulnerability. Finally, the complexity of fraud as an offence, the timely seizure of assets and proving the predicate offence pose challenges for the prosecution authorities.

---

[12] Federal Council, *Supervision of commodity trading activities from a money laundering. Federal Council report in response to the Seydoux-Christe postulate (17.4204) of 14.12.2017*, 26 February 2020, https://www.parlament.ch/centers/eparl/curia/2017/20174204/Bericht%20BR%20F.pdf
[13] CGMF, *Fraud and phishing for the purpose of fraudulent misuse of a data processing system as a predicate offence to money laundering,* January 2020, NRA_Bericht_Betrug und Phishing.pdf
[14] *Ibid*., p. 20. For further discussion, see section 2.4.2

The report concludes that the risk posed to Switzerland by money laundering through fraud including computer fraud is, at most, moderate, based on the average financial losses concerned (see also section 3.2.4 in this regard). In addition, it appears that, thanks to a fundamentally effective system of defensive and combating measures, the consequences of fraud as a predicate offence to money laundering do not affect society, the financial sector or the services sector as a whole. Finally, anti-money laundering legislation can also have a preventive effect by making it possible to block certain suspicious payments.

The report's observations have given rise to the following recommendations for action:

- *Improve the factual basis*: The report shows that fraud as a phenomenon is only partially captured by the current data. Even if the complexities of fraud – and to a lesser extent computer fraud – are unlikely to ever be fully captured, improvements are possible. Regular independent and scientifically based surveys of victims, focusing specifically on fraud offences and covering both legal entities and private individuals, would provide a better overview. It would also be worth examining the question of whether and to what extent the losses and the predicate offence can be captured in the case of money laundering offences.
- *Continue awareness-raising activities*: Switzerland already has well established and professional prevention mechanisms. Yet fraudsters are constantly inventing new ways to fool their victims. It is therefore essential that the players in the area of prevention are kept informed of the latest modi operandi, and update and supplement their information to the public on an ongoing basis. In the area of cybercrime, the 2018 to 2022 national strategy for the protection of Switzerland against cyber-risks (NCS) already makes provision for the early detection of trends and technologies and the accumulation of know-how, as well as the expansion of awareness-raising activities. However, the expansion of awareness-raising to cover non-cyber types of fraud should also be examined.

2. Trends in money laundering risk, 2015-2019

This chapter discusses the main findings presented in 2015 and elaborated in subsequent reports, in light of the SARs submitted to MROS by Swiss financial intermediaries between 2015 and 2019, supplemented by a brief assessment of the risks associated with non-financial sectors, and by information from the prosecution and supervisory authorities. It analyses the main trends in money laundering and terrorist financing over the period, as reflected in the SARs, the information from the Federal Customs Administration (FCA), criminal proceedings and international mutual assistance procedures, and then compares the results with those from the 2015 report. This allows the persistent trends and breaks to be measured. The parallel presentation of the main statistics from the 2015 NRA report and those for the 2015-2019 period provides a summary, supplemented by a more detailed presentation of the risks of money laundering and terrorist financing associated with various predicate offences and different types of financial intermediary, plus a review of the typical risks for non-financial sectors.

2.1. Statistical comparison of the 2004-2014 and 2015-2019 periods

Seven main statistics taken from the 2015 NRA report were compared with the data from the 2015-2019 period: figures on the number of SARs received annually; predicate offences; money laundering for third parties; domiciliary companies; types of financial intermediaries reporting suspicions; domiciles of contracting parties; and the number of business relationships

reported. These statistics were selected because they involve most of the main indicators providing an idea of the scale of money laundering in Switzerland, and because a statistical comparison in this regard between the 2004-2014 and 2015-2019 periods is possible. Essentially, the results of this comparison, summarised below, show that the risks identified in 2015 are sometimes more or less pronounced, but that the overall picture has remained largely unchanged.

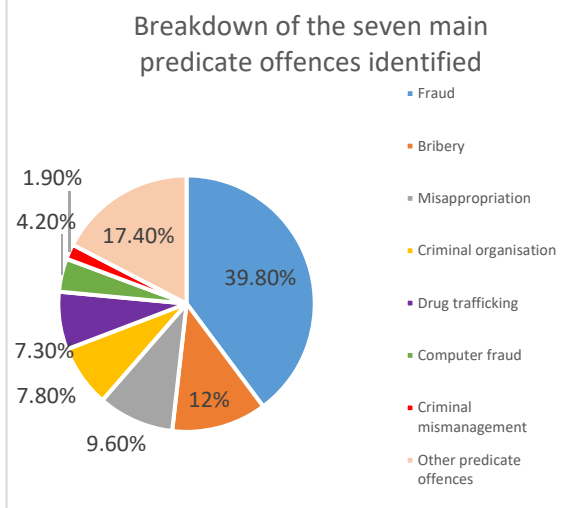
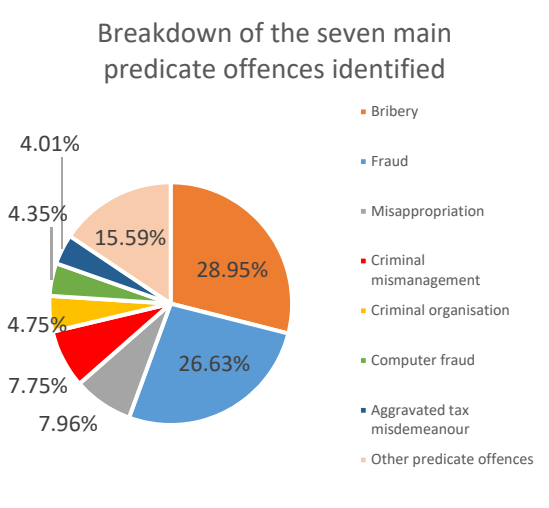
2.1.1. Number of reports received by MROS

There was, however, one significant change in the period covered by this report: between 2015 and 2019, MROS received 23,792 SARs. Thus, the annual average for these reports, which form the basis of the analysis in this chapter, has increased substantially compared to the 2004-2014 period, as shown in the table below:

	Total	Annual average
2004-2014	12,244	1,113.09
2015-2019	23,792	4,758.40

The number of SARs received by MROS was more than four times higher for the 2015-2019 period than for 2004-2014, and they now form a more representative database than hitherto. While their growth over the past five years does not reveal any fundamental change in the risk of money laundering and terrorist financing in Switzerland, it does show that the awareness of this risk among financial intermediaries has grown. We review the main possible reasons for this striking development below (see section 2.3).

2.1.2. Breakdown of the seven main predicate offences identified

2004-2014	2015-2019
	

The 2015 NRA report showed that four predicate offences – fraud, bribery, misappropriation and membership of a criminal organisation – were alone responsible for two thirds of the SARs received by MROS between 2004 and 2014. This finding remains valid for 2015 to 2019. However, three developments must be highlighted: bribery has ousted fraud in the list of the

four most frequent predicate offences; criminal mismanagement has replaced membership of a criminal organisation; and aggravated tax misdemeanour has entered the ranks of the main predicate offences of which people are suspected, while drug trafficking no longer features in the list.

2.1.3. Money laundering without the mention of a predicate offence[15]

2004-2014	2015-2019
10%	15.42%

In 2015, the NRA report emphasised the number of business relationships reported to MROS because they were suspected of being involved in money laundering for third parties, despite it not being possible to identify a specific predicate offence (10%). A similar observation can be made for the 2015-2019 period, during which the trend actually accelerated – business relationships reported without a specific predicate offence being identified now make up 15% of reports received by MROS.

2.1.4. Involvement of a domiciliary company

	2004-2014	2015-2019
All predicate offences	17.10%	29.55%
Fraud	16.50%	16.63%
Bribery	38.10%	43.36%
Criminal organisation	22.60%	43.00%

Financial intermediaries and national and international anti-money laundering authorities have long been aware of the specific risks associated with the complexity of business relationships established in the name of domiciliary companies: the 2015 report had already emphasised it, and the AMLO-FINMA (Art. 13 lit. h) regards the involvement of domiciliary companies as an increased risk factor and imposes special due diligence obligations on financial intermediaries. Compared to the 2004-2014 period, the number of business relationships in the name of a domiciliary company that were reported to MROS almost doubled, from 17.10% to 29.55%.

2.1.5. Financial intermediaries making reports

Financial intermediaries	2004-2014	2015-2019
Banking sector	67.2%	89.5%
Money transmitters	21.2%	3.8%
Asset managers	2.6%	1.3%
Fiduciaries	4.2%	1.0%
Lawyers and notaries	1.0%	0.1%

[15] The charts showing the seven main predicate offences identified do not include reports to MROS regarding money laundering for third parties, since they are not recorded based on the total reports received, but only on the reports for which the possible predicate offences have been identified by financial intermediaries at the time of the report. The numbers given for money laundering for third parties, i.e. the cases extracted from the charts above, are calculated using the total figure for reports received by MROS during the period specified.

Casinos	0.5%	0.6%
Securities dealers	0.2%	0.2%
Other	3.1%	3.4%

The table above shows that the predominance of banks among the categories of intermediary reporting to MROS, which was already substantial for the 2004-2014 period, has strengthened further since then. However, this rise in the number of reports originating from the banking sector has not come at the expense of reports from other financial intermediaries. The only category to have seen a reduction in the average number of reports between 2015 and 2019 compared to 2004-2014 is lawyers and notaries. For all other types of financial intermediary, the number of reports was similar from one period to the next, despite occasional fluctuations. Thus, the rise in the number of reports received annually by MROS between 2015 and 2019 mainly reflects an increase in the number of reports by banks.

2.1.6. Domicile of contracting parties

	2004-2014		2015-2019	
	In Switzerland	Abroad	In Switzerland	Abroad
All predicate offences	44.00%	56.00%	39.60%	60.40%
Fraud	42.60%	57.40%	63.48%	36.52%
Misappropriation	37.90%	62.10%	33.14%	66.86%
Criminal mismanagement	28.20%	71.80%	37.47%	62.53%
Criminal organisation	20.90%	79.10%	29.22%	70.78%
Bribery	9.10%	90.90%	12.80%	87.20%

The table above shows that the percentage of business relationships involving a contracting party domiciled abroad rose only slightly in 2015-2019 (60%) compared to 2004-2014 (56%). This figure varies by less than 10% only if we focus on the main predicate offences suspected by the financial intermediaries submitting the reports, except for fraud, for which the trend is inverted. Whereas during 2004 to 2014, only 42.6% of contracting parties in business relationships reported to MROS for fraud were domiciled in Switzerland, for the 2015-2019 period this figure rises to 63.48%.

Between 2015 and 2019, the figure for beneficial owners domiciled in Switzerland in relationships reported to MROS is similar to that for contracting parties, at 39.9%. This appears to be a significant increase over the figure published in the 2015 NRA report, which stated that only 27% of beneficial owners in business relationships reported between 2004 and 2014 were domiciled in Switzerland (2015 NRA report, p. 33). In fact, this difference is the result of a change in the definition of "beneficial owner" introduced by the legislative reforms that entered into force on 1 January 2016. Up to that date, the beneficial owners of a business relationship established in the name of operating companies were the operating companies themselves, and MROS classified them accordingly. By contrast, the beneficial owners of business relationships established in the name of domiciliary companies were defined as people holding the equity of the company and had to be identified on Form A when the bank account was opened. Since the entry into force on 1 January 2016 of the amendments to the Federal Act on Money Laundering, which were contained in the Federal Act for Implementing the Revised Financial Action Task Force Recommendations of 2012 passed by Parliament on 12 December 2014, the beneficial owners of a legal entity performing an operational activity are defined as "the natural persons who ultimately control the legal entity in that they directly or indirectly, alone or in concert with third parties, hold at least 25 per cent of the capital or voting

rights in the legal entity or otherwise control it" (Art. 2*a* para.3 of the AMLA). Moreover, since 1 January 2016, when a business relationship is established with an operating company, its beneficial owners or those with a controlling interest must be identified by the financial intermediary using Form K. As a result, the variation in the figures for beneficial owners domiciled in Switzerland from one review period to the next shows that a large number of corporate vehicles suspected of involvement in money laundering schemes linked to crimes abroad are owned by individuals domiciled in Switzerland. Finally, it should be noted that, in an effort to simplify matters, the term "beneficial owner" as used in this report also encompasses controlling interests.

2.1.7. Amounts deposited on accounts reported to MROS on date of reporting

	2004-2014, closed accounts and assets on reporting date		**2015-2019, closed accounts and assets on reporting date**		**2015-2019, excluding closed accounts on reporting date**	
	Median value of amounts in CHF thousands	Average value of amounts in CHF millions	Median value of amounts in CHF thousands	Average value of amounts in CHF millions	Median value of amounts in CHF thousands	Average value of amounts in CHF millions
All predicate offences	0.97	1.67	0.06	2.54	6.51	4.71
Fraud	2.84	1.26	0.05	0.70	3.87	1.19
Bribery	70.68	3.99	0	4.89	676.59	9.83
Criminal organisation	18.52	1.49	0.04	1.61	79.47	3.11

MROS has information on the assets held by business relationships reported to it by financial intermediaries. The table above presents these amounts as median and average values. The "2004-2014" and "2015-2019" columns offer a comparison of these numbers for all the reports received during these two periods. They reveal the substantial growth in the average number of reports to MROS, irrespective of whether we look at all reports, where a rise was registered in the average number of reports per business relationship between 2004-2014 (CHF 1.67 million) and 2015-2019 (CHF 2.54 million), or the reports concerning membership of a criminal organisation, and above all bribery, for which the average figure per business relationship rose from CHF 3.993 million to CHF 4.89 million. By contrast, for fraud the average amount reported per business relationship fell from CHF 1.26 million in 2004-2014 to CHF 0.70 million in 2015-2019.

In contrast to the average value, the median value declines significantly between the 2004-2014 period and the 2015-2019 period, reflecting the large number of business relationships reported to MROS between 2015 and 2019 following their dissolution or when they had a zero balance. Moreover, in the case of bribery, the number is higher than for business relationships that were still active at the time of reporting, which explains why the median value for assets reported on suspicion of bribery during the 2015-2019 period is zero. Conversely, the size of the assets reported to MROS between 2015 and 2019 presents a more favourable picture when only those business relationships that are still active at the time of reporting to MROS are included. As regards this figure, the average amount per business relationship for the 2015-2019 period is CHF 4.71 million. It rises to CHF 9.93 million for reports concerning bribery, while for reports of fraud it remains lower than the average amount for active and dissolved business relationships reported to MROS between 2004 and 2014 in connection with suspected fraud.

2.2. Impact of the main international money laundering incidents in Switzerland, 2015-2019

Compared to the 2004-2014 period, the dominant feature of the 2015-2019 period is the increase in the number of reports received by MROS, the growing number of business relationships established in the name of a domiciliary company, the rise in the amounts reported to MROS and, to a lesser extent, the greater number of reports concerning money laundering that cannot be linked to a clearly identified predicate offence. Nonetheless, a comparison between the statistics for the two periods also reveals the persistence of the same main predicate offences despite the predominance of bribery, the largely unchanged number of foreign-domiciled contracting parties to the business relationships reported, and the growing predominance of banks among the financial intermediation sectors submitting reports. In order to accurately assess the magnitude of these persistent factors and their development, it should be borne in mind that the reports received in the 2015-2019 period and used to make the comparison reflect the level of suspicion on the part of financial intermediaries. Yet these years were marked by several large international financial scandals which had major repercussions for Switzerland. Their particularities have thus shaped the morphology of the corpus constituted by the SARs. These major scandals mainly fall into three categories.

Firstly, since the launch in 2014 of the Brazilian police investigation under operation "Lava Jato", there have been several bribery scandals abroad, of which Petrobras/Lava Jato in Brazil, 1MDB in Malaysia and PDVSA in Venezuela are the main examples. Characterised by the payment and receipt of bribes during the fraudulent awarding of public contracts, especially in the areas of construction and raw materials extraction and marketing, the misappropriation of company/state institution assets by their directors, or the siphoning-off of sovereign assets with the complicity of corrupt politicians, these scandals had profound repercussions in Switzerland. Indeed, in many cases, the criminals used Swiss bank accounts to channel their ill-gotten gains with the aim of multiplying the transactions and thereby obscuring the paper trail. They also used reputable Swiss asset management services to place their illegally acquired funds with Swiss banks and asset managers, often after multiple transfers between different bank accounts opened in different jurisdictions.

Secondly, the last few years have also been characterised by several large data leaks, such as the Panama Papers in 2016 or the Paradise Papers in 2017. International consortia of journalists used the leaked information to uncover several cases of bribery and misappropriation of funds. But more generally, they revealed the desire by beneficial owners to anonymise the assets involved by using domiciliary companies in particular, hence the emergence of doubt as to the legality of their origins. However, in many cases, these domiciliary companies have bank accounts in Switzerland.

Thirdly, the 2015-2019 period was marked by the revelation of several apparent cases of money laundering on a grand scale, known as "laundromats": Azerbaijani laundromat, Russian/Moldovan laundromat, Troika Laundromat, Danske Bank, ABLV, etc. These cases, which occasionally overlap, share a number of characteristics. They involve the transfer of huge sums between former Soviet states and various jurisdictions – including Switzerland – via banks in Baltic countries. These transfers often pass through transitory accounts open in the name of domiciliary companies, often in the English-speaking world, whose declared beneficial owners are frequently pseudonyms[16]. The sums of money involved are considerable. According to the Organized Crimes and Corruption Reporting Project (OCCRP), at least USD 2.9 billion was transferred out of Azerbaijan in the context of the Azerbaijani laundromat; the funds transferred out of Russia as part of the Russian laundromat amounted

[16] Transparency International UK, *Hiding in plain sight. How UK companies are used to launder corrupt wealth*, November 2017, HidingInPlainSight_WEB3.pdf (transparency.org.uk)

to USD 20.8 billion; and those under the Troika laundromat to EUR 26.3 billion, while the dubious amounts that transited via the Estonian office of Danske Bank and the Latvian bank ABLV came to EUR 200 billion and EUR 100 billion respectively[17]. The Swiss financial centre has proved to be particularly exposed to these laundromat affairs. During the period concerned, transactions between Switzerland and the banks involved in these affairs amounted to tens of billions of Swiss francs and involve a number of Swiss financial intermediaries. During these affairs, they operated accounts for, above all, domiciliary companies; more often than not, they were used as transitory accounts. These accounts were frequently closed out once the transactions had been completed.

During the 2015-2019 period, Swiss financial intermediaries submitted numerous reports to MROS in connection with these three types of scandal. These heavily shaped the corpus upon which the statistics presented above were based, so that they help to explain the resulting developments.

First and foremost, these affairs serve to partly explain the rise in the number of reports to MROS. Once these cases became public, financial intermediaries carried out systematic checks to see whether their clientele included anyone who might be involved in such affairs. It can be estimated that around 20% of the reports received by MROS between 2015 and 2019 were linked to one of the three main types of international financial scandal.

The increase in the number of business relationships established in the name of domiciliary companies observed during the 2015-2019 period likewise reflects the cases that have come to light in recent years. As a matter of fact, this type of corporate vehicle is at the heart of the revelations surrounding the Panama Papers and Paradise Papers, and it is systematically used in laundromat affairs. Moreover, as domiciliary companies are frequently used in the context of tax-optimising asset management, and as the assets originating from the bribery scandals mentioned above are often under management in Switzerland, the owners of the accounts opened to manage these assets are generally domiciliary companies. Thus, given the number of reports received regarding these various affairs, it is not surprising to observe a growing number of business relationships being established in the name of domiciliary companies during the 2015-2019 period compared to the previous period.

Similarly, it is no surprise that during the 2015-2019 period, we can observe an increase in the reports submitted to MROS regarding bribery, due to the ramifications in Switzerland of the bribery scandals that have emerged in recent years. Although less pronounced, the growth in SARs to MROS without an identifiable associated predicate offence is also to a certain extent the result of the laundromat affairs. One of the main features of these laundromats is the fact that it is difficult to identify the origin of the funds, owing to the multiplicity and rapidity of transactions between offshore corporate accounts, for which potentially dubious but formally correct lending contracts or commercial invoices are frequently used as justification. As a result, the reports to MROS relating to laundromats generally involve suspicions of money laundering, without a potential predicate offence being identifiable. The public naming of the main Baltic banking institutions involved in these laundromat affairs prompted Swiss financial intermediaries to review all the transactions conducted with them, and to uncover after the fact some dubious transactions that had not been identified at the time of the transfer instruction, such as transfers whose payment reason was the purchase of over 100 lawnmowers for personal use, or some 300 bathtubs for a private property.

[17] Organized Crimes and Corruption Reporting Project (OCCRP), *The Russian Laundromat exposed*, 20 March 2017, The Russian Laundromat Exposed – OCCRP; idem, *The Troika Laundromat*, 4 March 2019, The Troika Laundromat – OCCRP; idem, *The Azerbaijani Laundromat*, 4 September 2017, The Azerbaijani Laundromat – OCCRP

These major financial crime cases also determined the volume and configuration of the corpus of reports on which the statistics presented above were based. It is still difficult to ascertain the extent to which the changes wrought by these large international cases on the statistics for reports received between 2015 and 2019 could persist in the coming years. It should be noted that, essentially, they do not reflect the current state of money laundering risk in Switzerland as these cases, although reported between 2015 and 2019, concerned criminal activities that had begun much earlier. The large number of already dissolved business relationships reported to MROS between 2015 and 2019 shows that they are involved in presumed money laundering activities identified after the fact, and that they reflect a state of money laundering that has already changed.

However, it would be wrong to think that all the developments revealed by the statistical comparison of the 2004-2014 and 2015-2019 periods can be attributed to these various scandals. For example, they had only a very marginal impact on the increase in average amounts deposited as part of reported business relationships at the time of their reporting to MROS. In addition, the figures presented above show that there are large areas of continuity between the two periods. Thus, the conclusion should be drawn that the differences arising out of the statistical comparison between the 2004-2014 and 2015-2019 periods are explained by factors other than these major cases of international financial crime.

2.3. Conclusions from the statistical comparison

The main conclusion that can be drawn from the statistical comparison presented in section 2.1 concerns the stability of the figure for foreign domiciliation of contracting parties in the reported business relationships, which rose by only 4% between the two review periods, from 56% to 60%. This percentage illustrates the fact that, just as in the 2004-2014 period, the main risk to which Switzerland is exposed is that of being used as a location for laundering the assets acquired from financial crimes committed abroad. Thus, among the business relationships reported to MROS between July 2015 and 2019[18], the suspected predicate offence was committed in Switzerland in only 22.3% of cases and these reports accounted for only 4.3% of the assets deposited in connection with business relationships. But the discrepancy between the numbers for predicate offences committed in Switzerland and those for domiciliation of beneficial owners and contracting parties also shows that Swiss-resident individuals and Swiss-registered companies help to launder the proceeds of crimes committed in other countries.

This greater risk of assets from crimes committed abroad being laundered in Switzerland, which was already highlighted in the 2015 NRA report, can be explained by the heavily international focus of the Swiss financial centre and, in particular, its dominant position in cross-border asset management and, to a lesser extent, commodity trading.

As explained in more detail below, this gives rise to a risk of money laundering that weighs disproportionately on the different types of financial intermediaries, but primarily banks; the statistical comparison above suggests that banks have changed their behaviour since 2015. Despite the deluge of reports they prompted, the scandals of 2015-2019 do not, on their own, explain the rise in reports received by MROS during that period. It can also be explained by banks' greater awareness of money laundering risk. Having learned their lesson from these major international money laundering cases, which had significant ramifications in Switzerland,

[18] The indicator for the location in which the presumed predicate offence was committed was not added to the MROS database until July 2015. As a result, information on this subject is available only for the period between 1 July 2015 and 21 November 2019, when MROS changed the system for submitting reports.

these banks are monitoring their clients more closely and multiplying their checks in this regard. Moreover, since 2015 various legislative and regulatory amendments have brought in new due diligence obligations; these have led financial intermediaries, and especially banks, to multiply their internal checks, which have revealed numerous suspect cases. In addition, Swiss banking institutions have become more cautious as regards money laundering, due to the checks carried out by FINMA and the sanctions it has occasionally imposed, and to the criminal proceedings in Switzerland and abroad involving banking institutions. Finally, jurisprudence has evolved since 2015. In various rulings, the Federal Criminal Court and then the Federal Supreme Court have held that a well-founded suspicion leading to an obligation to report a business relationship to MROS exists as soon as the additional clarifications undertaken by a financial intermediary do not make it possible to disprove the hypothesis that the assets involved might be the result of criminal activity. The Federal Supreme Court therefore set a low threshold for considering money laundering suspicions as well-founded, establishing the same practice as that used by a number of financial intermediaries. In the last revision of the AMLA, this jurisprudence was also explicitly anchored in law.

These various elements, which are hard to quantify in isolation, explain the rise in the number of reports to MROS. Between 2015 and 2019, more banking institutions submitted SARs to MROS, despite the fact that the number of banks licensed by FINMA has declined each year since 2015[19]. Between 2004 and 2014, SARs from the banking sector were made by 184 different institutions, while those received from this sector between 2015 and 2019 were submitted to MROS by 232 banks. In addition, between 2015 and 2019, eleven banks made at least 2% of all reports from the sector, whereas between 2004 and 2014, the figure was only five. Finally, internal audits and transaction monitoring increasingly result in suspicions being reported to MROS by the banking sector. It should also be noted that this heightened awareness and the associated rise in reports are not exclusive to Switzerland, but rather are in line with an international trend. Several foreign financial centres comparable to Switzerland have witnessed a similar development over the last decade[20]. A similar trend is not, however, discernible for fiduciaries, and is moderate for asset managers, despite the fact that they have been impacted almost as much as the banks by the cases that have made the latter more cautious, and the fact that all of these players are involved in asset management, a sector that is exposed to a higher level of risk, as already emphasised in 2015. The annual average for SARs to MROS from lawyers and notaries was lower during the period under review than in the earlier period.

It is difficult to assess whether the growth in reports from the banking sector should be interpreted as an increase or decrease in the risk of money laundering. On the one hand, by reporting more suspicions to MROS, Swiss banks are helping to raise the probability that money laundering will be punished and, hence, that the risk posed to the Swiss financial centre will decline. On the other hand, the rise in reports from the banking sector could also suggest that it is uncovering more reportable cases than in the past. However, these hypotheses appear to be contradicted by the fact that over 40% of business relationships reported by banks between 2015 and 2019 had already been dissolved at the time of reporting. This figure demonstrates that the growth in reports reflects a picture of money laundering in Switzerland which has already partly evolved. Thus, it does not show increased risk, but rather improved

[19] The number declined from 266 in 2015 to 246 in 2019. Swiss National Bank, *Banks in Switzerland*, 2019, p. 6, Swiss National Bank (SNB) – Banks in Switzerland (snb.ch)

[20] For example, in the United Kingdom the number of SARs increased by 20% between 2019 and 2020, and by 70% between 2011 and 2019. See HM Treasury and Home Office, *National risk assessment of money laundering and terrorist financing*, 2020, p. 11, NRA_2020_v1.2_FOR_PUBLICATION.pdf (publishing.service.gov.uk) In Luxembourg, they rose from 10,959 in 2015 to 51,930 in 2019 (Financial Intelligence Unit of the Duchy of Luxembourg, *Annual report 2019*, p. 11, Annual report 2019 (public.lu). In France, SARs received by TRACFIN rose by 25% between 2018 and 2019 (TRACFIN, *Annual report 2019*, p. 10, web-ra-analyse-tracfin-19-20-v26_0.pdf (economie.gouv.fr). In Liechtenstein, they went up by nearly 40% between 2015 and 2019 (Financial Intelligence Unit (FIU) of the Principality of Liechtenstein, *2019 annual report*, p. 15, a202783_fiu_jahresbericht_2019_de_Einzelseiten.indd (llv.li).

detection of pre-existing risks after the fact. Yet, precisely because it reflects a risk that has already changed, and which will be more complicated to combat, the increase in reports cannot be regarded as a risk-reducing factor either. It is therefore undoubtedly more reasonable to see it simply as a change in banks' behaviour.

The greater number of SARs submitted by the banking sector concern suspicions of predicate offences that are generally similar to those prevailing between 2004 and 2014. Nonetheless, beyond the stability of the overall picture of money laundering risk from one period to another as regards predicate offences, some factors have changed which warrant a more detailed risk assessment than the main risks that they represent separately.

2.4. Predicate offences

The analysis of the SARs received by MROS between 2015 and 2019 confirms the predominance of the same predicate offences as identified in 2015, but the ranking is different. The relative increase in bribery and criminal mismanagement, and the appearance of aggravated tax misdemeanour automatically cause a decline in the other suspected predicate offences. Nevertheless, even in the case of fraud, where the decrease is substantial, going from 39.8% of cases associated with a specific predicate offence to 26.5% (22.52% of all reports), the number of SARs received annually in relation to the various predicate offences shows a general upward trend in absolute figures, despite occasional fluctuations for some of the offences. The only exception is computer fraud, which has been decreasing steadily since its surge between 2015 and 2016.

2.4.1. Bribery

In addition to the raw figures for the number of reports, the indicators combine to point to the predicate offence of bribery as the main money laundering threat in Switzerland. Firstly, the amounts of money deposited in business relationships suspected of laundering the proceeds of such acts are significant. They alone accounted for 47.2% of the suspicious assets reported to MROS between 2015 and 2019, i.e. a total of CHF 27,063,658,709, even though they represented only 24.49% of the total number of SARs received during that period. This amount is particularly impressive, given that more than half of the business relationships reported to MROS in connection with bribery between 2015 and 2019 had already been closed at the time of reporting. Furthermore, in 43.34% of cases, these relationships were established in the name of domiciliary companies.[21] In 19.63% of cases, they involve PEPs; this is above the average for both indicators. However, it is difficult to say whether such percentages are indicative of the heightened risks associated with business relationships established in the name of domiciliary companies or involving PEPs, or whether they reflect financial intermediaries' heightened vigilance when it comes to business relationships involving domiciliary companies or PEPs, which they consider to be risk indicators.

Secondly, the analysis of the SARs associated with bribery illustrates the significant risk of Switzerland being used as a money laundering centre for felonies committed abroad. The main predicate offence cited in the SARs received by MROS, i.e. the bribery at the origin of the alleged money laundering reported to MROS, is committed in Switzerland in only 1.2% of

[21] Taking the figures for SARs received up to 22 November 2019

cases[22], while the contracting parties of the business relationships concerned are domiciled in Switzerland in only 12.8% of cases and their beneficial owners in only 13.95% of cases.

Switzerland is thus exposed to a high risk of money laundering resulting from foreign corruption. Despite the increase in the number of related SARs and the significance of the threat suggested by these indicators, it would probably be unreasonable to say that the risk associated with bribery was higher in 2020 than in 2015. More than half of the bribery-related reports received between 2015 and 2019 involved already closed business relationships, i.e. old ones. Part of their rise can be explained by financial intermediaries' verifications following the spate of international cases such as those mentioned above. While the implications for Switzerland from the laundering of assets from these large-scale bribery cases are becoming clearer, they have not been established in the past five years and go back further in time. They are associated with two of the main sectors that underpin the Swiss financial centre's international appeal and which have already been identified as vulnerable to money laundering: cross-border asset management and commodity trading. These findings were the subject of a sectoral report and a Federal Council report, to which we refer for a more detailed analysis[23].

2.4.2. Fraud and computer fraud

After bribery, fraud is the second most prevalent predicate offence to money laundering and a sectoral analysis report has likewise been devoted to it[24]. However, this report makes a subtle distinction regarding the extent of the risk associated with fraud by highlighting the small amounts involved. An analysis of the SARs received by MROS between 2015 and 2019 confirms this point: during that period, reports of suspected money laundering associated with fraud concerned only 6.24% of the assets reported to MROS even though they accounted for 22.52% of all reports received. The money laundering risk associated with fraud is moreover based on less complex financial schemes than average. For example, only 16.63% of the business relationships reported to MROS in connection with suspected fraud were established in the name of a domiciliary company and only 2.69% of them involved PEPs. Furthermore, as regards the threat of money laundering, fraud has a less international character than bribery: of the cases known to MROS between 2015 and 2019, 42.27% of the fraud predicate offences were committed in Switzerland, while 63.48% of the contracting parties to the reported business relationships were domiciled in Switzerland, as were 62.62% of the beneficial owners.

Computer fraud, most often in the form of online phishing scams, also constitutes a significant money laundering threat, as it is difficult to identify and, if applicable, impose criminal penalties on the main protagonists, who usually operate from abroad, even if the money mules are convicted of money laundering. However, this threat needs to be put into perspective because, despite a few cases involving spectacularly high amounts, phishing scams often involve sums of a few hundred francs when taken individually. Between 2015 and 2019, reports of suspected money laundering associated with computer fraud totalled only 0.07% of the assets reported to MROS, even though they accounted for 3.68% of all reports received. Moreover, the Swiss authorities have stepped up their warnings about making Swiss banking relationships available to criminals. Overly gullible accountholders are deceived by various false pretexts and thereby play the role of money mules in this type of online scam. These warnings seem to be paying off, as the number of cases reported to MROS has been decreasing since 2016.

[22] Of the SARs received between 1 July 2015 and 22 November 2019. See p. 20, note 18 above
[23] See 1.2.5 and 1.2.6 above
[24] See 1.2.7 above

2.4.3. Misappropriation and criminal mismanagement

As it is often difficult for financial intermediaries to distinguish between misappropriation and criminal mismanagement, their classification in MROS statistics is quite arbitrary. Taken together, they accounted for 13.29% of SARs between 2015 and 2019, which is similar to the 11.5% they represented in the period from 2004 to 2014.

As in the past, the main money laundering threat associated with these two predicate offences is linked to the internationalisation of the Swiss financial centre. When committed abroad, criminal mismanagement and misappropriation often involve the embezzlement of funds for various forms of financial investment for asset management purposes, for which the criminals use the services of Swiss financial intermediaries. In this respect, criminal mismanagement and misappropriation are often difficult to distinguish from bribery, as they may involve misconduct in public office or a breach of trust in public office, but the counterpart of a possible corrupt deal cannot be identified. In cases where criminal mismanagement and misappropriation are committed abroad, the risk factors associated with them are high: business relationships suspected of laundering the proceeds of such acts are established in the name of domiciliary companies in more than 40% of cases. PEP involvement is above average and the amounts in question are significant (11.8% of the total amounts reported to MROS).

However, the funds resulting from misappropriation and criminal mismanagement that are laundered in Switzerland also originate from misappropriation and criminal mismanagement committed in Switzerland, which bear no relation to bribery and are more typically related to embezzlement of funds to the detriment of Swiss companies by their managers, or to the detriment of individuals deceived by their representatives or relatives. Although it is smaller than the threat linked to the internationalisation of the Swiss financial centre, this domestic threat appears to be greater than during the 2015 assessment. The SARs received by MROS show that a higher-than-average proportion of suspected misappropriation and criminal mismanagement offences are committed in Switzerland: 27.08% of misappropriation cases and 25.02% of criminal mismanagement cases, compared with an average of 22.28% for all SARs received between 2015 and 2019.

2.4.4. Criminal organisation

In the SARs received by MROS, the suspicions of criminal organisation membership are often based on a definition of criminal organisation that is sometimes very far removed from the corresponding Swiss legal concept. In many cases, they concern other economic crimes committed by a gang. The threat of money laundering linked to criminal organisation membership or support in this broad sense has not changed much since 2015. As in the past, it continues to be associated with foreign criminal organisations active in Switzerland's neighbouring countries and in the former USSR, which are suspected of establishing a presence in Switzerland primarily to launder their criminal assets, particularly with the help of commercial enterprises and service providers operating in the financial and real estate sectors and in the restaurant trade. However, some of the money laundering suspected of being under the control of criminal organisations also takes the form of investments in Switzerland for asset management purposes. This explains the high percentage (43%) of business relationships reported to MROS in connection with criminal organisations that are established in the name of domiciliary companies.

2.4.5. Money laundering

An important development during the period under review is the significant increase in SARs without a specific predicate offence identified by the financial intermediaries. As already mentioned, this increase is linked to the laundromat cases that broke out between 2015 and 2019, to which the Swiss financial centre was highly exposed. In the vast majority of cases, the inability to identify a specific predicate offence to money laundering leads to MROS abandoning these reports, which means that criminal proceedings in this context are very rare in Switzerland. Yet the indications of money laundering are significant: a clear desire to conceal the identity of the beneficial owners, systematic use of opaque corporate structures, especially domiciliary companies, multiple transactions with no economic justification between accounts held by such structures and opened in different countries, the use of these accounts solely as transitory accounts, etc. It appears that these laundromat cases are now finished. However, they may have been replaced by different schemes that have not yet been identified, so the threat in this respect remains high, as does the vulnerability of the Swiss financial centre.

2.4.6. Aggravated tax misdemeanour

Aggravated tax misdemeanours are a new money laundering threat for the Swiss financial centre, as they did not become a predicate offence to money laundering until 1 January 2016. Between then and 22 November 2019, MROS received 767 reports of business relationships suspected of harbouring funds from such a crime (3.79% of the reports received between 2016 and 2019). Due to the new nature and particular characteristics of an aggravated tax misdemeanour as a predicate offence to money laundering, the 2015 NRA report (p. 126) recommended examining the money laundering risk associated with it in a specific sectoral report dedicated to predicate tax offences. That report has yet to be completed.

2.4.7. Terrorist financing

While the 2015 NRA report identified the threat posed by the possible use of the Swiss financial sector to finance terrorist actions or groups active abroad, it considered the actual risk of terrorist financing in Switzerland to be limited. Since then, the very perception of the threat posed by terrorist financing has changed and encompasses much broader dimensions: whereas the definition of terrorist financing in the 2015 NRA report referred to the financing of organisations planning terrorist actions abroad, it now additionally covers the financing of terrorist fighters, including jihadi tourists. This development thus calls for a more detailed examination of the risk of terrorist financing in Switzerland. This is discussed in section 4.2 of this report (see below).

2.5. Financial intermediaries

The threats posed by the various predicate offences to money laundering do not weigh uniformly on all financial intermediation categories. In this respect, the sectoral risk analysis reports on bribery, fraud and computer fraud as predicate offences to money laundering have revealed the financial intermediaries most vulnerable to these offences. More generally, as Switzerland is primarily exposed to the risk of laundering funds derived from predicate offences

committed abroad, financial intermediaries with the most internationalised activities appear to be the most vulnerable. This is the case above all when they are active in two areas whose specific risk was identified back in 2015: cross-border asset management and commodity trade finance.

With around CHF 2,300 billion of foreign assets under management, representing a stable rate of around 27% of the global market since 2013, Switzerland is the leader in cross-border asset management, where it has succeeded in attracting a highly diversified client base in geographical terms[25]. However, this sector of activity carries a high risk of money laundering, with one of the main factors being the complexity of the financial schemes concerned, which involve multiple players. The banks, where wealthy clients deposit their assets, are pivotal. But cross-border asset management also frequently involves the services of fiduciaries, independent asset managers or lawyers, who act on behalf of their clients, create the investment instruments they use or manage their assets[26]. In this respect, the number of SARs sent to MROS since 2015, which is low for fiduciaries and very low for lawyers and notaries, seems to indicate a significant risk associated with these two categories of financial intermediation.

To a lesser degree, another factor already identified in 2015 and in successive reports explains the predominance of the risk of assets derived from economic crimes committed abroad being laundered in Switzerland: the prominence of Switzerland in commodity trading. Companies active in this field are often domiciled in Switzerland essentially for tax purposes and those with a controlling interest are often resident abroad. However, they often use Swiss banks to finance their activities. These banks likewise carry a high risk of bribery-related money laundering, as outlined in a recent Federal Council report[27].

As in the past, although money transmitters are mainly active in the international transfer of funds, they nevertheless carry a moderate money laundering risk, as the transactions rarely involve large amounts. By contrast, they are highly vulnerable from a terrorist financing point of view and could be used to finance the activities of terrorist fighters. Although the amounts involved here are also small, the vulnerability of money transmitters is nevertheless significant.

Since 2015, one of the main new developments found in the analysis of financial intermediaries has been the 185 SARs received by MROS from virtual asset service providers (VASPs). The financial intermediaries that sent these reports are either companies offering exchange services between virtual currencies and fiat currencies, companies providing crypto asset advice and management, or companies promoting initial coin offerings (ICOs). The small number of such reports does not necessarily indicate a low risk of money laundering, but rather that the financial intermediaries active in this sector are still not very sensitive to the risk of money laundering. The CGMF prepared a report that assessed the risk of money laundering involving cryptocurrencies in 2018. It concluded that, although the limited information available did not allow the actual risk to be assessed, the threat posed by crypto assets and the vulnerability of the Swiss and foreign financial system were both considerable. Over the past two years, this sector has developed spectacularly and very rapidly both from a technological point of view and in terms of the number of financial intermediaries active in it. Given the changes in the cryptocurrency financial intermediation landscape in Switzerland, the understanding of the associated money laundering risk needs to be examined in more detail. It is covered in section 4.3 (below).

[25] Swiss Banking, *Banking Barometer 2019. Economic trends in the Swiss banking industry*, September 2020, SBA_Banking Barometer_2019_EN.pdf (swissbanking.ch)
[26] CGMF, *Money laundering risks in the case of legal entities*, cit., p. 86 *et seq.*
[27] Federal Council, *Supervision of commodity trading activities…, cit.*

2.6. Evolution of risks in non-financial sectors

The 2015 NRA report also looked at the risks of money laundering and terrorist financing associated with non-financial sectors, and in particular the real estate sector, bonded warehouses, the trade in works of art, non-profit organisations, cross-border cash transfers, and commodity trading. Moreover, these last three sectors were the subject of a more in-depth analysis as part of the sectoral reports mentioned above (see section 1.2).

Since these different sectors are not involved in financial intermediation, they are not subject to the AMLA. However, under the definitions set out in Article 2 paragraph 3 letter c of the AMLA and Article 5 of the AMLO[28], traders are. They are subject to special due diligence requirements when they accept cash payments of CHF 100,000 or more (Art. 8a of the AMLA) and are required to report their suspicions to MROS when they know or suspect that the cash used in the transaction is of criminal origin. Despite these legal provisions, only two reports were submitted to MROS by traders during the period under review and neither of them concerned the non-financial sectors mentioned above. By contrast, they do feature in the reports to MROS from traditional financial intermediaries, in criminal proceedings, in international mutual assistance procedures and in information collected by the customs authorities. The related information does not permit any conclusion to be drawn as to whether the risk associated with these different sectors fundamentally changed during the period under review.

As regards the real estate sector, there is a risk that illegally obtained assets are invested in it, often in cash, and that they are the proceeds of organised crime and bribery committed abroad. Firstly, real estate purchases are also aimed at establishing economic activities allowing illegally obtained assets to be laundered, for example in the restaurant business. Secondly, criminals frequently try to launder their illegally acquired assets in luxury real estate[29]. Although these kinds of cases continue to be regularly observed by the Swiss authorities, numbers do not appear to have risen since 2015. Moreover, measures have been taken to mitigate the money laundering risk in the real estate sector (see section 3.7 below).

As the sectoral report on the subject points out, the predominant risk for non-profit organisations is above all the risk of terrorist financing associated with humanitarian or charitable NPOs operating in regions where religious or ethnic nationalist terrorist organisations are active. Nonetheless, the suspicions of this kind reported to MROS and relating to Swiss NPOs are very rare, and none has yet been confirmed. In addition, the authorities have stepped up their monitoring of associations (see section 3.6 below).

The risk associated with cross-border cash transfers essentially comprises that of a break in the paper trail for financial flows[30]. As an estimated 2.2 million people cross the border every day[31], the checks performed by the FCA as part of its duty to monitor the cross-border movement of persons and goods are done on a random basis and adjusted according to the risks. Even so, the FCA's statistics on cross-border cash transfers that are spontaneously declared or discovered during a random check show that the amounts involved have trended downwards since 2013. This is illustrated by the table below.

[28] *Ordinance of 11 November 2015 on Combating Money Laundering and Terrorist Financing*, (Anti-Money Laundering Ordinance, AMLO, SR 955.01)
[29] 2015 NRA report, p. 109; *CGMF, Corruption as a predicate offence to money laundering, cit.*, p. 25
[30] CGMF, *Report on the use of cash…, cit.*, p. 29
[31] Federal Customs Administration (FCA), *FCA facts and figures 2021*, FaktenZahlenEZV_2021_EN_Webversion.pdf

Year	Incoming traffic	Outgoing traffic	Cases in Switzerland	Total	Total amount for all checks in CHF	Average amount per occurrence in CHF
2013	247	42	3	292	36,620,027	125,411
2014	263	23	28	314	30,882,373	98,351
2015	152	23	26	201	17,036,938	84,761
2016	94	17	16	127	9,113,600	71,761
2017	81	29	24	134	7,749,458	57,832
2018	99	8	16	138	9,793,162	70,964
2019	106	7	15	128	9,850,930	76,960

Moreover, in the overwhelming majority of cases, those carrying the funds can prove the legality, so the risk associated with cross-border cash transfers continues to be rated as moderate.

The money laundering risk that characterises commodity trading is generally linked to bribery of foreign public officials. Switzerland is particularly exposed, owing to its dominant position in this sector. This observation, which was already made in the 2015 NRA report, the sectoral report on bribery and the Federal Council report in response to the Seydoux-Christe postulate, continues to be valid, as demonstrated by the SARs about money laundering in connection with commodity trading, the numerous pending criminal proceedings and some headline-grabbing convictions handed down recently to major commodity traders, both companies and individuals.

The main money laundering and terrorist financing risk to which Swiss bonded warehouses and open customs warehouses are exposed appears to be associated with aggravated tax misdemeanours. As already observed in the 2015 report, the prevalence of this threat has not changed since then according to the Federal Customs Administration, although the threat has materialised in very few cases. The risk it represents nonetheless remains difficult to assess, because aggravated tax misdemeanours did not become a predicate offence to money laundering until the beginning of 2016. However, it should be pointed out that the assets deposited in bonded warehouses and open customs warehouses are high-value objects (fine wines, jewellery, works of art, cultural property), rather than money in the pure sense. While these items are susceptible to being purchased with illegally obtained assets, their acquisition – and hence the money laundering involved – generally takes place outside Switzerland. In this regard, the trade in works of art poses a greater risk than the depositing of these items in bonded warehouses and open customs warehouses. But according to information gleaned from the few reports received by MROS in relation to this area of activity, the main risk stems from the laundering of misappropriated or stolen cultural property rather than from money laundering. As a result, there is nothing that allows us to conclude that the 2015 NRA report's assessment of this sector's risk as moderate needs to be changed.

2.7. Action by prosecution and supervisory authorities

Of the 23,792 SARs received by MROS between 2015 and 2019, 47.62% were referred to prosecution authorities. In 45.67% of the reports submitted, the competent prosecution authority was the Office of the Attorney General of Switzerland (OAG). The OAG was also

affected by the major international money laundering cases mentioned above. To tackle the caseload, the OAG supplemented its investigative teams by creating task forces.

The reports referred to the OAG by MROS, not all of which are linked to major international money laundering cases, were one of the main sources of the 4,804 criminal proceedings initiated in Switzerland between 2015 and 2019 on suspicion of money laundering and terrorist financing. In these proceedings, the main predicate offence is general economic crime, which includes fraud, misappropriation and criminal mismanagement in particular. The share of bribery is similar to that reflected in the reports to MROS: between 2010 and 2019, it was largely unchanged, accounting for around 25% of predicate offences in the proceedings initiated by the OAG for money laundering offences.

Moreover, the number of people convicted in Switzerland annually for money laundering is on the rise. There were 223 in 2017, 247 in 2018 and 315 in 2019. The majority of convictions were in proceedings launched before 2015 and did not necessarily stem from cases reported to MROS. However, the 11,330 reports received by MROS between 2015 and 2019 and referred to the prosecution authorities resulted in 732 convictions. In the overwhelming majority of cases (96.72%), the convictions were handed down by cantonal courts. Essentially, these were money laundering cases related to predicate offences involving fraud or computer fraud, which come under the remit of the cantonal prosecution authorities. In addition, the modest number of convictions in criminal proceedings initiated by the OAG based on reports referred to it by MROS does not cover all its activities in this regard, which also involve the confiscation of assets and the processing of international mutual assistance requests.

Since 2016, according to the figures from the Federal Office of Justice (FOJ), the number of mutual assistance requests to Switzerland in connection with money laundering has increased in line with that of SARs. Between 2016 and 2019, they ranged from 200 to 300 cases annually. Requests by Switzerland to other countries did not experience similar growth, and have hovered around 150 to 200 cases annually for a decade. By contrast, the number of spontaneous reports under Article 67*a* of the IMAC[32] sent to other countries by Swiss public prosecutors in connection with money laundering has risen since 2016 (between 30 and 80 cases per annum, compared to a range of 20 and 40 cases for the preceding years).

Whether they originate in Switzerland or are reported by other countries, the international mutual assistance procedures relating to money laundering associated with fraud and international bribery have increased since 2016. With regard to fraud, Switzerland submits 20 to 60 requests annually to other countries and receives 30 to 60 requests from abroad; with regard to international bribery, Switzerland sends between 10 and 30 requests and receives the same number.

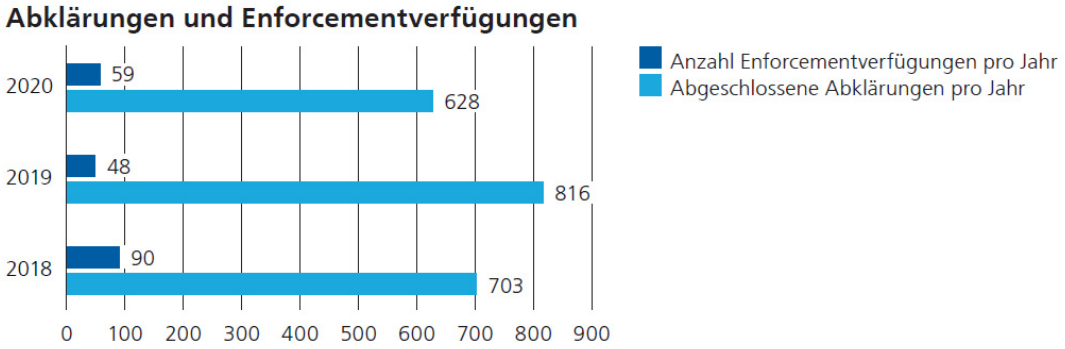
This confirms the conclusions from the assessment of SARs, i.e. the main risk is linked to fraud and international bribery. As a corollary to the rise in reports, the number of criminal proceedings, mutual assistance procedures and convictions has risen globally since 2015. Nonetheless, this increase in proceedings does not mean that risk has increased. The significant number of mutual assistance procedures can be explained by the notification of the OAG of several complex international money laundering cases in particular, which had a considerable impact on Switzerland, such as proceedings in Brazil in the Lava Jato case.

Given the major risks of money laundering in Switzerland, FINMA treats the issue of money laundering as a priority, resulting in a number of supervisory measures being introduced and, for serious violations, investigations and enforcement proceedings. Over the last few years, the Swiss financial centre has been heavily exposed as a result of international bribery cases

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

(Petrobras, Odebrecht, 1MDB, Panama Papers, FIFA or PDVSA). FINMA is therefore planning to exert a positive influence on the behaviour of the most exposed institutions, especially as regards combating bribery. In the 2015-2020 period, FINMA focused on reporting suspected money laundering and the management of risk at these institutions by performing numerous onsite anti-money laundering audits each year, including on the reporting duty since, according to the AMLA, reporting is an important element in the fight against financial crime. Thus, the criminal players in the market will be less tempted to funnel corrupt assets to Switzerland if they think there is a high probability that financial institutions will report their suspicions to MROS, quite apart from the fact that the reports to MROS are instrumental in the success of the prosecution authorities' efforts.

As demonstrated by the statistics below, FINMA has conducted numerous investigations and enforcement proceedings concerning violations of the money laundering provisions:



Source: FINMA, *Annual Report 2020*, p. 65, https://www.finma.ch/en/news/2021/03/20200325-mm-jb2020/

3. Legal and operational measures for limiting the sectoral risks identified since 2015

The assessment of money laundering risks between 2015 and 2019 largely confirms the assessment carried out in 2015, and shows that the main threats continue to exist. However, to mitigate them, since 2015 Switzerland has adopted a number of measures based, in particular, on the risk assessment in the 2015 report and the subsequent sectoral reports. Some measures are prudential. For instance, since 1 January 2020, asset managers and trustees are subject to supervision bodies authorised by FINMA. While this measure does not change the actual risk facing this kind of financial intermediary, it does contribute to improving their supervision. Other measures adopted since 2015 are operational and legislative. They involve both increasing the effectiveness of certain anti-money laundering measures, especially the legal requirements on due diligence by financial intermediaries, and introducing rules on transparency in certain retail sectors. This chapter provides an overview of these measures.

3.1. Federal Act for Implementing the Revised Financial Action Task Force Recommendations of 2012

In 2012, the Financial Action Task Force's (FATF) internationally recognised standards on combating money laundering and terrorist financing were partly revised. In order for them to be transposed into Swiss law, on 12 December 2014 Parliament passed the Federal Act for Implementing the Revised Financial Action Task Force Recommendations of 2012[33], which contained the amendments planned in eight areas. They included the introduction of a predicate offence for serious cases in the area of direct taxation, the creation of a legal basis[34] for identifying the private individuals that ultimately own or control the legal entity which is a contractual party to a business relationship, as well as the obligation for traders to either involve a financial intermediary or apply due diligence for purchases of movable or immovable property where the purchase price exceeds CHF 100,000. A detailed description of the remaining provisions that entered into force on 1 January 2016 (or 1 July 2015 as regards transparency on legal entities and bearer shares) can be found in the 2015 NRA report (p. 19). Moreover, these amendments were welcomed in the FATF's evaluation of Switzerland conducted in 2016. A few of the amendments needed to be fleshed out in implementing provisions (changes to the AMLO-FINMA, AMLO-FGB[35], CDB, SRO regulations).

3.2. Increasing the effectiveness of precious metals control

In the area of precious metals trading, the risks identified by the 2015 NRA report have been mitigated by developments since the Precious Metals Control Act[36] was applied by the Central Office for Precious Metals Control, and its impact on the sector has enabled these vulnerabilities to be reduced.

Between 2014 and 2019, largely because the Central Office for Precious Metals Control introduced the principle of systematic audits which are triggered by at least every licence renewal request, the number of licensed foundries has fallen sharply, from 45 to 24. During the preparation of the audits, a number of companies stated that they no longer ran a foundry operation or no longer owned the requisite equipment; this constitutes an infringement of the licensing conditions in accordance with Article 165*b* of the PMCO[37]. In those cases, the licences were withdrawn in accordance with Article 166*a* of the PMCO. Among the 24 licence holders still operating in 2020, 11 are also authorised to act as trade assayers[38]. In addition, one company holds this authorisation but does not have a foundry licence. This presupposes that it does not operate as a foundry, i.e. that it does not carry out foundry work for third parties as set out in Article 24 of the PMCA and Article 164 of the PMCO. For the sector, the fall in the number of licensed foundries, together with the systematic stance and consequently increased frequency of audits by the Central Office, has contributed to a reduction of risks under the

[33] *Federal Act of 12 December 2014 for Implementing the Revised Financial Action Task Force (FATF) Recommendations of 2012*, (BBl 2014 9689)
[34] Art. 4 of the AMLA in conjunction with Art. 2a para. 3 of the AMLA
[35] *Ordinance of the Federal Gaming Board of 24 June 2015 on the Diligence of Casinos in Combating Money Laundering and the Financing of Terrorism*, (FGB Anti-Money Laundering Ordinance, AMLO-FGB, SR 955.021)
[36] *Federal Act of 20 June 1933 on the Control of the Trade in Precious Metals and Precious Metal Articles* (Precious Metals Control Act, PMCA, SR 941.31)
[37] *Ordinance of 8 May 1934 on the Control of Trade in Precious Metals and Precious Metal Articles* (Precious Metals Control Ordinance, PMCO, SR 941.311)
[38] Trade assayers are authorised to conduct determinations of the fineness of melt material and melt products on behalf of third parties. An assayer licence from the Central Office for Precious Metals Control is required to operate as a trade assayer. A company may be licensed to act as a trade assayer if it employs at least one sworn assayer (see Arts. 28 and 29 of the PMCO).

PMCA but also, indirectly, under the AMLA. Examples include cases in which PMCA-related shortcomings discovered at trade assayers subject to the provisions of the AMLA (e.g. due diligence obligations) are reported to FINMA within the scope of its supervision of self-regulatory organisations (SROs).

An audit report published by the Swiss Federal Audit Office in 2020 welcomed the tightening of these controls[39]. The audit nonetheless gave rise to four recommendations, which are now the subject of an implementation plan involving, in particular, more in-depth checks prior to the auditing of licence holders and better integration of risk assessment in relation to licence holders' activities, and partly also their imports. These processes are constantly being improved, and a further milestone will be reached with the planned increase in resources, the creation of the FCA's DaziT digitalisation project and, over the longer term, the establishment of the new Federal Office for Customs and Border Security (FOCBS). In addition, on 19 March 2021 Parliament passed the amendment to the Anti-Money Laundering Act (AMLA). At the request of the industry concerned, the Central Office for Precious Metal Control will now assume the AMLA-related oversight of trade assayers operating commercially with banking precious metals. The bill will also introduce a control mechanism for the purchase of precious metal scrap. It is likely to enter into force from mid-2022.

3.3. Changes with regard to bonded and open customs warehouses

At the recommendation of the SFAO[40], on 6 March 2015 the Federal Council approved a strategy on bonded and open customs warehouses, in which it advocated a clear legal framework for operating these warehouses. In order that the Federal Customs Administration (FCA) can perform its tasks efficiently and effectively, the conditions for operating bonded warehouses were tightened and the Customs Ordinance amended.

With effect from 1 January 2016, amendments were made in the following areas in particular:

- The list of sensitive goods (e.g. banknotes, securities, diamonds, precious stones and works of art)[41] for which an inventory must be kept was expanded to include additional goods that can be used as a store of value (wine, tobacco products, passenger vehicles, motorbikes and furniture).

- When sensitive goods are warehoused, the person responsible for declaring the goods for customs clearance must submit a customs declaration.

- In addition to the exact designation of the goods (e.g. type of painting, dimensions, title, artist), the value, the incoming customs docket and the warehouse location, etc., the inventory must also contain the name and address of the owner instead of the name and address of the person authorised to dispose of the goods in storage.

- The export period for goods awaiting export was restricted and the requirements for an extension were defined.

[39] Swiss Federal Audit Office, *Effectiveness of the precious metals control – Federal Customs Administration, audit mandate 19476*, June 2020, https://www.efk.admin.ch/en/publications/economy-and-administration/public-finances-and-taxes/3850-effectiveness-of-the-precious-metals-control-federal-customs-administration.html
[40] Swiss Federal Audit Office, *Free ports and open customs warehouses: licensing and inspection activities, audit mandate 12490*, April 2014, https://www.efk.admin.ch/en/publications/economy-and-administration/public-finances-and-taxes/2407-free-ports-and-open-customs-warehouses-an-evaluation-of-licensing-and-inspection-activities.html
[41] Annex 2, *Customs Ordinance of 1 November 2006* (CustO; SR 631.01)

- The conditions for operating a customs warehouse were supplemented with guide values on the number of annual warehouse entries and removals (more than 5,000 for bonded warehouses, more than 200 for open customs warehouses).

- Operating licences for customs warehouses are issued for fixed periods (10 years for bonded warehouses, 5 years for open customs warehouses).

As a result of the new requirements for bonded warehouses, the FCA reviewed all bonded warehouses and licenced only seven of them.

On 1 July 2019, the SFAO published the report[42] on the follow-up of the implementation of its 2014 recommendations on bonded and open customs warehouses. The follow-up audit took place between February and August 2018. In its report, the SFAO acknowledges that the FCA made a great effort to remedy the shortcomings identified in 2014. It concludes that, by and large, its recommendations were well implemented. In its opinion, the FCA now has the necessary tools to perform its tasks and ensure the proper use of the warehouses. The SFAO criticises only that the FCA continues to tolerate exceptions as regards the minimum number of movements, and that the regulations on requirements for those hiring warehouse space and their supervision do not go as far as it had recommended.

In the context of the Anti-Money Laundering Act, there is a lack of transparency in the case of foreign trading and financial transactions that involve high-value goods warehoused in Switzerland. If, for example, the goods are in a bank safe in Switzerland at the time of the financial transaction, the ownership details remain unknown. If, however, the goods are under customs supervision in a bonded warehouse, each change of ownership must be recorded in the inventory – irrespective of whether the transaction takes place in Switzerland or abroad.

The FCA has complete transparency as regards sensitive goods placed in Swiss customs warehouses, and this helps to reduce potential risks of money laundering and terrorist financing.

3.4. Exchange of information on tax matters

Aggravated tax misdemeanours were not defined as a predicate offence to money laundering until 1 January 2016; as a result, the risk of money laundering associated with aggravated tax misdemeanours was not assessed in the 2015 NRA report. However, since 2015, wide-ranging measures have been taken to mitigate this risk.

Firstly, transparency on the shareholders of legal entities has been improved by the Federal Act on Implementing the Recommendations of the Global Forum on Transparency and Exchange of Information for Tax Purposes, which was passed by Parliament on 21 June 2019[43]. This reform aims to remedy certain shortcomings noted by the Global Forum in 2016, as well as those identified by the FATF in the same year. The Act, which entered into force on 1 November 2019, contains the following modifications. In accordance with Article 622 of the

[42] Swiss Federal Audit Office, *Supervisory activities at free ports and open customs warehouses – Federal Customs Administration, audit mandate 17458*, July 2019, https://www.efk.admin.ch/en/publications/economy-and-administration/public-finances-and-taxes/3628-supervisory-activities-at-free-ports-and-open-customs-warehouses-federal-customs-administration.html

[43] BBl 2019 4313, https://www.admin.ch/opc/fr/federal-gazette/2019/4313.pdf

CO[44], bearer shares are no longer permitted unless the company has equity securities listed on a stock exchange or if the bearer shares are organised as intermediated securities and are deposited with a custodian in Switzerland designated by the company or are entered in the main register (para. 1bis). In addition, a company with bearer shares must note in the commercial register that it has equity securities listed on a stock exchange or its bearer shares are organised as intermediated securities (para. 2bis). In order to ensure compliance with these new requirements, the new Articles 327 and 327*a* of the SCC[45] now foresee fines for any infringement of the obligation to specify the beneficial owners or keep a share register and the list of beneficial owners of the shares. Finally, Article 22*f*^{bis} of the Tax Administrative Assistance Act (TAAA)[46] requires legal entities that are based abroad but are in fact managed in Switzerland to keep a register of its proprietors at their actual place of management.

On the other hand, since 1 January 2017, Switzerland has been applying the global standard for the automatic exchange of financial account information in tax matters (AEOI) of the Organisation for Economic Co-operation and Development (OECD). Since that time, the reporting Swiss financial institutions – including banks, insurance companies, trusts, etc. – have collected the reportable identification and financial account data of their clients, where the latter are based in one of Switzerland's partner states, of which there are over a hundred. The information is submitted annually to the competent authority in the partner state. By implementing the global AEOI standard, Switzerland is making a significant contribution to increasing transparency on tax matters and preventing cross-border tax evasion.

3.5. Federal Decree on the Approval and Implementation of the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol and the Strengthening of Criminal Justice Instruments for combating Terrorism and Organised Crime

On 25 September 2020, Parliament passed the Federal Decree on the Approval and Implementation of the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol[47]. The revision was mainly aimed at bringing Swiss criminal legislation into line with the above-mentioned laws, especially as regards the financing of travel and training for terrorist purposes. However, the legislator also took advantage of the revision to strengthen MROS's powers under the Anti-Money Laundering Act (AMLA) and to formalise the dynamic mutual assistance under the Federal Act on International Mutual Assistance in Criminal Matters (IMAC). These amendments entered into force on 1 July 2021 and can be summarised as follows:

Strengthening the criminal provisions
Article 260ter of the SCC, which refers only to criminal organisations, will now explicitly mention terrorist organisations. The legislator thus used this law to anchor what the prosecution authorities and courts have always done, i.e. apply this article to both criminal and terrorist organisations. Moreover, the stipulation that an organisation must keep its structure secret to be criminal, which has been roundly criticised by doctrine and practitioners, will be removed. The maximum custodial sentence will be increased from five to ten years. In addition, a new

[44] *Federal Act of 30 March 1911 on the Amendment of the Swiss Civil Code (Part Five: The Code of Obligations)*, (Code of Obligations, CO, SR 220)
[45] *Swiss Criminal Code of 21 December 1937* (SCC, SR 311.0)
[46] *Federal Act of 28 September 2012 on International Administrative Assistance in Tax Matters (Tax Administrative Assistance Act*, TAAA, SR 651.1)
[47] BBl 2020 7651, https://www.admin.ch/opc/fr/federal-gazette/2020/7651.pdf

Article 260^{sexies} will be introduced in the Criminal Code, aimed at punishing the recruitment, training and travel for terrorist acts, as well as the financing of such activities. This new provision foresees a maximum custodial sentence of five years. Next, and at the appropriate time, the Federal Council will use the new Article 74 of the Intelligence Service Act[48] to issue a decision aimed at prohibiting the terrorist organisations targeted by the law prohibiting al-Qaeda and Islamic State[49] – which will expire at the end of 2022. This law could then be repealed. Reminder: under Article 74 of the IntelSA, the Federal Council can ban an organisation or a group which directly or indirectly propagates, supports or otherwise promotes terrorist or violent extremist activities. Associating with or supporting a banned organisation is punishable by a maximum custodial sentence of five years or a monetary penalty. Finally, as regards Article 260^{quinquies} of the Criminal Code (terrorist financing), the Federal Council has come to the conclusion that the criticisms voiced about it were not sufficiently serious to prompt a revision of this provision[50].

All the offences punishable as support for a criminal or terrorist organisation are crimes and thus predicate offences to money laundering within the meaning of Article 305bis of the SCC.

Strengthening MROS's powers

In the December 2016 mutual evaluation report on Switzerland[51], the FATF criticised the fact that MROS did not have the power to request information from a Swiss financial intermediary on behalf of a foreign counterpart in the absence of a link with a suspicious activity report sent to MROS by a Swiss financial intermediary. The OECD Working Group on Bribery had made a similar observation in March 2018[52]. An amendment of Article 11*a* of the AMLA remedies this shortcoming by granting this power to MROS (see, in particular, Article 11*a* paras. 2bis and 3). The entry into force of this new AMLA provision should be accompanied by the creation of ten additional analyst positions at MROS.

Strengthening mutual assistance

While the mutual assistance provided by the Swiss authorities on criminal matters is acknowledged by other countries, it is sometimes mentioned that the accused person's right of appeal on this matter can slow down the procedure. Indeed, this aspect was highlighted by the FATF in 2016[53] and the OECD Working Group in 2018[54]. Rights of appeal were not reviewed in this context; however, the spontaneous exchange of information and joint investigation teams have now been formalised under Articles 80*d*^{bis} and 80*d*^{ter} of the IMAC for investigations into organised crime or terrorism. These instruments should help to speed up mutual assistance procedures in the areas mentioned above.

[48] *Federal Act of 25 September 2015 on the Intelligence Service* (IntelSA, SR 121)
[49] *Federal Act of 12 December 2014 on the Prohibition of the Groups "al-Qaeda" and "Islamic State" and Associated Organisations* (SR 122)
[50] Federal Council, *Dispatch on the federal decree on the Approval and Implementation of the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol and the Strengthening of Criminal Justice Instruments for combating Terrorism and Organised Crime*, 14 September 2018 (BBl 2018 6469), https://www.fedlex.admin.ch/eli/fga/2018/2301/fr
[51] Financial Action Task Force (FATF), *Anti-money laundering and counter-terrorist financing measures, Switzerland, Mutual Evaluation Report*, December 2016, mer-suisse-2016.pdf (fatf-gafi.org)
[52] Organisation for Economic Co-operation and Development (OECD), *Implementing the OECD Anti-Bribery Convention, Phase 4 Report: Switzerland*, 15 March 2018, Switzerland Phase 4 Report.pdf (oecd.org)
[53] FATF, *Anti-money laundering and counter-terrorist financing measures, op. cit*, criterion 37.5, p.245
[54] OECD, *Implementing the OECD Anti-Bribery Convention, op. cit.*, para. 119 et seq., p. 55 et seq. and recommendation 12(a), p. 81

3.6. Revision of the Anti-Money Laundering Act and additional measures in connection with the FATF mutual evaluation

As mentioned earlier, the Financial Action Task Force (FATF) conducted its fourth review of Switzerland in 2016. In its fourth mutual evaluation report on Switzerland in December 2016, it acknowledged the good quality overall of the Swiss system for combating money laundering and terrorist financing. At the same time, it identified weaknesses in certain areas and made recommendations. A bill proposing revisions to the Anti-Money Laundering Act takes account of the most important recommendations from the FATF's mutual evaluation report on Switzerland and strengthens the integrity of the Swiss financial centre. The bill was passed by Parliament on 19 March 2021; it enshrines the following **main measures** in law:

- **Checking the identity of the beneficial owner:** creation of an explicit legal framework for checking the identity of the beneficial owner. This anchors the existing practice in law.
- **Checking that client data is up to date:** introduction of an explicit legal obligation to regularly check that client data is up to date.
- **Reporting system:**
  - Anchoring of case law on reporting thresholds in law.
  - Various measures to improve the reporting system, especially the removal of the 20-day deadline for the processing of money-laundering reports by MROS and the introduction of a provision on terminating business relationships.
- **Associations:** for associations that distribute/collect assets abroad, in particular for charitable purposes, an entry in the commercial register is now mandatory. The reason for this requirement is the risk of such associations being misused for money laundering or terrorist financing. In addition, all associations entered in the commercial register must now maintain a membership list and have a representative office in Switzerland.
- **Traders in precious metal scrap and trade assayers:**
  - introduction of a control mechanism for the purchase of precious metal scrap.
  - assumption of AMLA-related oversight over trade assayers by the Central Office for Precious Metal Control.

Other, less fundamental amendments to the AMLA are aimed at strengthening national cooperation and improving the compliance of Swiss legislation with the FATF's recommendations on international cooperation. These apply in particular to the use of MROS information by Swiss prosecution authorities and the consent of a foreign reporting office to pass on information to the Swiss authorities or third parties such as self-regulatory organisations. As regards national cooperation, in future MROS and the recognised self-regulatory organisations should be able to exchange all information necessary for the implementation of the AMLA. Moreover, it resolves a conflict between the client's right to information, on the one hand, and the prohibition on financial intermediaries providing information to clients, on the other.

Additional measures in connection with the FATF mutual evaluation are implemented in the Federal decree on the prevention of terrorism and organised crime (see section 4.6 below), and the Federal Act of 21 June 2019 on the Implementation of the Recommendations of the Global Forum on Transparency and Exchange of Information for Tax Purposes (see section 4.5). Similarly, the FINMA Anti-Money Laundering Ordinance (AMLO-FINMA), the Agreement on the Swiss Banks' Code of Conduct with Regard to the Exercise of Due Diligence (CDB) and the self-regulatory organisations' regulations which came into force in January 2020 provide for the implementation of measures from the FATF evaluation. In addition, various sectoral risk analyses (see section 2.2) have been conducted.

3.7. Consultation procedure on the Amendment of the Land Register Ordinance

On 16 April 2014, the Federal Council submitted a bill to Parliament, which is aimed at improving nationwide land searches for the authorities. In 2015, the NRA report recommended that this measure be implemented rapidly, in order to improve the identification of property owners in Switzerland and, in turn, mitigate the risks of money laundering in the real estate sector. Following the parliamentary debates, the Federal Act on the Amendment of the Swiss Civil Code (Recording of marital status and real estate register)[55] was passed on 15 December 2017. It entered into force on 1 January 2019.

The aim of this amendment was to enable the AHV number to be used for maintaining the land register and allow it to be communicated, subject to strict criteria, and to be used to search for real estate across Switzerland (Arts. 949*b* and 949*c* of the CC). On 14 October 2020, the Federal Council initiated the consultation on the amendment of the Land Register Ordinance (LRO)[56]. The bill aims to implement the new Articles 949*b* and 949*c* of the CC by means of the new legislation mentioned above. Under Article 949*b* paragraph 1 in conjunction with Article 949*c* of the CC, all land owners must be identifiable by means of their AHV number, including the beneficial owners of easements or pledgees[57]. According to Article 949*c*, the Federal Council must regulate property searches across the country. In order to simplify searches, the Federal Council is planning to set up a national IT system, which will be managed by the Confederation. This is aimed at providing the authorities with access, within the scope of their legal mandate, to information enabling them to ascertain with certitude whether someone has rights to a piece of real estate and, if so, what those rights are. Thus, the authorities will be able to consult data on the legally effective rights entered in the main register, but the property search function will not allow them to access complete extracts from the land register. The consultation period ended on 1 February 2021. The results of the consultation were evaluated and the draft was amended accordingly. A Federal Council decision on the draft is expected at the end of 2021. The provisions are due to enter into force in January 2023 at the earliest.

3.8. Innovations in the area of virtual assets (VA) and virtual asset service providers (VASPs)

Since the advent of cryptocurrency-related activities on the financial market, Switzerland has applied the existing regulatory framework in the fight against money laundering and terrorist financing to certain cryptocurrencies (also referred to as "virtual assets" in the FATF standards) and to virtual asset service providers (VASPs), which clearly equate to traditional financial service providers as defined by FINMA[58]. Under this regulatory framework, all financial intermediation activities linked to cryptocurrencies fall within the scope of the Anti-Money Laundering Act (AMLA). These include, in particular, currency exchange activities between cryptocurrency providers and fiduciary currencies and/or between one or more forms of cryptocurrency, all cryptocurrency transfer activities, activities involving the custody and/or

[55] *Swiss Civil Code of 10 December 1907* (Civil Code, CC, SR 210), (Recording of marital status and real estate register), BBl 2017 7475, https://www.admin.ch/opc/de/federal-gazette/2017/7899.pdf

[56] *Ordinance of 23 September 2011 on the Land Register* (Land Register Ordinance, LRO, SR 211.432.1); Federal Council, *Land register: country-wide search using the AHV number,* 14 October 2020, https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-80702.html

[57] Federal Council, *Dispatch concerning the amendment of the Swiss Civil Code (Recording of marital status and real estate register)*, BBl 2014 3395, https://www.fedlex.admin.ch/eli/fga/2014/785/fr

[58] FINMA, *Circular 2011/01, Activity as a financial Intermediary in accordance with the Anti-Money Laundering Act*, entered into force on 1 January 2011, finma rs 2011 01 01 01 2017.pdf

administration of cryptocurrencies or instruments enabling the management of cryptocurrencies. To avoid any ambiguity, FINMA has also published a practical guide on initial coin offerings (ICOs), as a reminder that, in cases where tokens issued during such initial coin offerings can be equated to payment tokens, the ICO activities constitute financial intermediation and, as such, are subject to the AMLA[59]. Before starting operations in Switzerland, any private individual or legal entity acting as a financial intermediary, and hence subject to the AMLA, must either obtain prudential authorisation from FINMA (e.g. banking licence, authorisation as a securities firm) or affiliate themselves with a self-regulatory organisation (SRO) subject to FINMA supervision.

For payment orders, Article 10 of the AMLO-FINMA contains an obligation to disclose details of the originator and the beneficiary ("travel rule"). The financial intermediary receiving the payment is then able to check whether the sender's name is on a sanctions list, for example. They can also check whether the beneficiary's details are correct; if not, they must return the payment to the sender. Under the AMLA and its technical ordinances, the requirements on the application of the travel rule to payments are neutral as regards technology, and are thus applicable to VASPs and financial intermediaries using cryptocurrencies. Thus, the amendment of the AMLO-FINMA takes account of the FATF's revised standards of 2019, which requires VASPs to comply with the preventive measures in FATF recommendations 10 to 21, including the requirements on applying the travel rule. In principle, institutions supervised by FINMA can send cryptocurrencies or other tokens only to external wallets belonging to their own, pre-identified clients, and accept cryptocurrencies or tokens only from such wallets. FINMA-supervised institutions may not receive tokens from other institutions' clients, nor send them to such clients. This rule also applies where the sender's or beneficiary's details cannot be reliably transmitted within the payment system concerned[60]. Moreover, from 1 January 2021, the threshold requiring the counterparty's identity to be checked during an exchange transaction, or in cases where several exchange transactions in virtual currency appear to be linked, has been lowered from CHF 5,000 to CHF 1,000 (Art. 51*a* of the AMLO-FINMA), in line with the requirements in the FATF's recommendation 15. These rules have been adopted by the SROs whose members include cryptocurrency service providers.

In addition, having observed an increase in blockchain-based projects aimed at creating so-called stablecoins since 2018, in September 2019 FINMA published a supplement to its ICO guidance, setting out its stance on these new types of crypto assets[61]. The projects concerned are often designed to limit the usual price volatility of payment tokens (such as bitcoin) by backing the token with assets (e.g. fiat currencies, commodities, real estate or securities). In the supplement to its guidance on ICOs, FINMA provides guidance on how it evaluates these stablecoins from the perspective of the law and Swiss supervisory practice, and thereby creates transparency for financial market players. As regards the classification of these stablecoins according to Swiss financial market legislation, FINMA applies the principle of technology neutrality. In its assessment, FINMA focuses on a token's economic function and objective ("substance over form") and takes account of relevant existing legislation as well as the particularities of the case *(same risks, same rules)*. The actual structure of stablecoins varies widely depending on the type of assets used to back the tokens, and the rights conferred on the token holder can be subject to different prudential requirements[62]. There are points of overlap with financial market legislation, especially in the areas of combating money laundering and in the trading of securities. Given that the purpose of stablecoins is often to act as a means

[59] FINMA, *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, 16 February 2018, wegleitung%20ico.pdf
[60] FINMA, *FINMA Guidance 02/2019, Payments on the blockchain*, 26 August 2019, p. 3, 20190826%20finma%20aufsichtsmitteilung%2002%202019.pdf
[61] FINMA, *Supplement to the guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, September 2019, wegleitung stable coins (1).pdf
[62] *Ibid.*, Annex 2

of payment, the AMLA is frequently applied. In a number of cases, the Banking Act, the Collective Investment Schemes Act and the Financial Market Infrastructure Act also apply[63].

3.9. Federal Act on the Freezing and the Restitution of Illicit Assets held by Foreign Politically Exposed Persons (FIAA)

At the latest since the events of the Arab Spring in 2011, the retrieval of assets unlawfully acquired by politically exposed persons has become a topic of global proportions. In this connection, at the end of 2015 Parliament passed the Federal Act on the Freezing and the Restitution of Illicit Assets held by Foreign Politically Exposed Persons (FIAA)[64]. The FIAA can apply in exceptional circumstances in which people in positions of authority abroad have unlawfully enriched themselves. It makes provision for targeted measures to support legal cooperation with the foreign country (preventive freezing of assets in Switzerland in the case of the sudden collapse of a regime), as well as for specific cases in which mutual assistance procedures will definitely not succeed (administrative procedure with a view to possible confiscation and restitution of the assets). The freezing of deposed dictators' assets under the FIAA gives the new authorities in the country of origin time and the best possible conditions in which to investigate offences which could be relevant as predicate offences to money laundering (or bribery and misappropriation of public funds). The FIAA thus contributes indirectly to combating money laundering.

[63] FINMA, *FINMA publishes 'stable coin' guidelines*, 11 September 2019, https://finma.ch/en/news/2019/09/20190911-mm-stable-coins/

[64] *Federal Act of 18 December 2015 on the Freezing and the Restitution of Illicit Assets Held by Foreign Politically Exposed Persons* (FIAA; SR 196.1)

4. Changes in risks since 2015

Although the main money laundering risks in Switzerland and the measures taken to mitigate them have hardly changed since 2015, new threats have emerged in relation to certain financial activities and certain types of economic crime. This means that the risks changed during the period under review, or that they were not taken into account in previous risk assessment reports, and that it is therefore not possible to draw conclusions on the risk they pose.

One area for which it is difficult to draw conclusions is the financing of the proliferation of weapons of mass destruction, which was not addressed in the 2015 NRA report, nor in successive sectoral reports. As the FATF revised its standard in this regard in 2020, and now expressly requires its member states to perform risk analysis on the financing of proliferation, the need to examine this question and carry out a targeted study in this regard should be evaluated. However, such a study is outside the scope of this report. Another area that could not be assessed as part of the 2015 NRA report is the crime of aggravated tax misdemeanour, which was not defined as a predicate offence to money laundering until 1 January 2016. This direct tax fraud is part of the complex problem of tax offences in general. An evaluation should be performed to ascertain whether it is worth examining it in detail, although such an examination is outside the scope of this report. Nonetheless, as mentioned in section 3.4, Switzerland has implemented measures which help to limit the risk of money laundering in this area.

Among the areas in which there have been recent developments that will be looked at in more detail below are online casinos, terrorist financing and cryptocurrencies. The money laundering risk associated with online casinos is hard to quantify. The lifting of the ban on casinos in Switzerland under the Federal Gambling Act of 29 September 2017 also opens up the possibility of their being used for money laundering. Yet, the first Swiss online casinos did not start up until summer 2019; as a result, it was too early for the associated money laundering risk to be assessed in the period under review. The first section of this chapter nonetheless explains the legal and regulatory framework in place to mitigate this risk. By contrast, an assessment of the money laundering risk associated with cryptocurrencies and the risk of terrorist financing has to take account of the major changes that have occurred in these two areas.

4.1. Online casinos

The 2015 NRA report assessed the money laundering risk associated with casinos as low, and stressed that the main risks identified in this sector at international level stemmed from online casinos, which at that time were banned in Switzerland. The Gambling Act of 29 September 2017 (GamblA)[65], which supersedes earlier gambling legislation, revoked this ban. It allowed 21 casinos that are already licensed for a physical presence to request, with effect from 1 July 2019, a licence extension to cover the operation of online casino games.

When authorising online casinos to operate on Swiss territory, the legislator also put in place the legislative tools to mitigate the potential risks inherent in this new form of financial transaction, especially as regards money laundering. The Federal Council grants licence extensions after consulting the Federal Gaming Board (FGB) and if all the conditions are met.

[65] *Federal Act of 29 September 2017 on Gambling* (GamblA, SR 935.51)

These conditions are essentially the same as those for granting an ordinary licence. Article 68 of the GamblA sets out the specific due diligence obligations for online gambling in connection with the fight against money laundering. It gives the FGB the power to define the monthly amounts for bets and winnings, either individual or cumulative, that are deemed to be large and therefore require players to be identified. Based on this article, the FGB fleshed out the due diligence obligations for online casinos by revising its Ordinance on the Diligence of Casinos in Combating Money Laundering and the Financing of Terrorism (AMLO-FGB), also with effect from 1 January 2019. Article 3 of the AMLO-FGB sets the threshold for identifying and registering players at CHF 4,000 within a 24-hour period for payments into the player account or payment account.

There are several stages to setting up a player account with an online casino. A temporary account can be opened by the operator if the player provides the information specified in Article 47 paragraph 3, Article 48 and Article 52 paragraph 1 of the GamblO[66] (surname, first name(s), date of birth and address of domicile/residence in Switzerland, adult player, no gambling ban or exclusion, and absence of concrete indications that the information provided is not factual). The total amount of payments by the players may not exceed CHF 1,000 and players cannot withdraw their winnings.

One month at the latest after opening the temporary account, the operator must verify the player's identity in accordance with Article 49 of the GamblO. If the player meets the conditions specified in Article 47 paragraph 3 of the GamblO, their player account becomes permanent. Under Articles 49 and 52 paragraph 2 of the GamblO, the operator must then check that its client does not have more than one player account, obtain a copy of an official identification document and perform a second verification of the information that was provided when the temporary account was set up.

As soon as the transaction volume exceeds the CHF 4,000 threshold specified in Article 3 of the AMLO-FGB, the operator must identify the beneficial owners and register the player in accordance with Articles 7 and 8 of the AMLO-FGB. In addition, in accordance with Article 50 paragraph 2 of the GamblO, winnings and funds deposited in the player account may be withdrawn only by means of a transfer to a payment account in the name of that player.

The casino fulfils its obligation to register online gambling transactions by gathering the information specified in Article 39 of the FDJP Gambling Ordinance[67]. This information includes details of the transactions carried out performed by the player, as well as information on their gambling activity, especially the type and version of game, the date of the gambling session, and the start and end times of the session.

The information is also entered in a data register located on Swiss territory, in accordance with Article 60 of the GamblO. Under Article 61 of the GamblO, all information is retained in the register for a period of five years starting from the transfer of the casino tax. This information is also transferred in real time to a database set up by the FGB. This provides the FGB with a tool for checking casinos' compliance with their obligations.

The casinos' use of automatic alerts and checks on the information in the register makes it easier to apply Article 15 of the AMLO-FGB (Art. 6 para. 2 lit. c of the AMLA) to detect high-risk transactions, and also mitigates the risk of money laundering.

Article 15 paragraph 2 of the AMLO-FGB sets out the high-risk cases for which casinos must clarify the background and objective of the financial transaction in accordance with Article 6 paragraph 2 of the AMLO-FGB. For this purpose, a player account can be blocked temporarily until certain documents are obtained (e.g. form detailing the beneficial owners, bank statements or tax documents).

[66] *Gambling Ordinance of 7 November 2018 on Gambling* (GamblO, SR 935.511)
[67] *FDJP Gambling Ordinance of 7 November 2018* (GamblO-FDJP, SR 935.511.1)

Finally, online casinos, like their physical counterparts, are required to refer instances of suspected money laundering to MROS in accordance with Article 9 of the AMLA.

The legal framework put in place by the legislator helps to considerably reduce the risk of money laundering and allows suspicious transactions to be detected. In addition, the transaction tracking that has been put in place allows financial flows to be reconstructed in cases where money laundering is suspected.

As of 31 December 2019, four casinos held an extended licence, which they had obtained between July and October of that year. At the end of 2019, these four casinos' gross income from gambling totalled CHF 23,492,821, quite a modest amount compared to the gross income from gambling earned by physical casinos, which came to CHF 742,454,645 in 2019[68]. While these figures appear to suggest that, for the time being, the money laundering risk associated with online casinos is low, the fact that they have only recently been legalised and started operating precludes any firm conclusions, and the situation should therefore be monitored closely.

4.2. Terrorist financing

The evolution of the very notion of terrorist financing described above (see section 2.4.7) explains why the number of reports to MROS about related suspicions increased between 2015 and 2019. Whereas MROS received around thirteen such reports annually from 2004 to 2014, the figure was 341, i.e. 68.2 on average per year, between 2015 and 2019.

In 74% of cases, business relationships reported for suspected terrorist financing are established in the name of private individuals, two thirds of whom are domiciled in Switzerland. Most of the transactions performed by these individuals involve small amounts transferred to personal accounts in high-risk countries, which explains why nearly 22.5% of such reports come from money transmitters, as against 73% from banks. In a few cases, the amounts involved are substantial, sometimes several million francs. This is the case when the reported accounts belong to wealthy individuals suspected of providing financial support to terrorist organisations in their country of origin, for example. In a quarter of cases, the reported business relationships are set up in the name of legal entities, including non-profit organisations, whose vulnerability in this respect was already emphasised in 2015. In some cases, the reported relationships involve operating companies or domiciliary companies.

Of the 341 suspicious activity reports (SARs) related to terrorist financing that were received by MROS between 2015 and 2019, 115 were referred to the prosecution authorities (of which, 84 to the Office of the Attorney General and 31 to the offices of the cantonal public prosecutors). In 55 of the 115 referred cases, the prosecution authorities launched proceedings. Ten cases ended with proceedings being dropped. In 28 cases, proceedings were launched or the SAR was integrated into ongoing proceedings, although these did not relate to terrorist financing or an infringement of the ban on Islamic State or al-Qaeda. In 10 cases, proceedings were launched owing to terrorist financing or an infringement of the Federal Act on the Prohibition of al-Qaeda, Islamic State and Associated Organisations. Six prosecutions were suspended and one report is still being evaluated. In the 10 cases involving prosecution for suspected terrorist financing or infringement of the prohibition against al-Qaeda and Islamic State, the business relationship at the time of the report to MROS was either wound up or the amount involved was zero. In three cases, the amount involved was between zero

[68] *Annual report of the Federal Gaming Board*, 2019, pp. 20-21, Federal Gaming Board: 2019 annual report (admin.ch)

and CHF 500. In one case, the amount was CHF 4,082, in another case CHF 12,044 and in a third CHF 21,699.

In addition to the cases described above in connection with reports to MROS, the prosecution authorities initiated 92 proceedings in 2015-2019 relating to financial support for a criminal organisation in a global terrorism context. These proceedings were based on police reports and complaints.

When investigating cases involving terrorist financing, the prosecution authorities are confronted with familiar and usually similar challenges. These relate to the origin of the funds, the transfer routes, the beneficiaries and the purpose of the payments.

It should be noted first and foremost that terrorist financing usually involves much smaller amounts than money laundering. Smaller amounts are generally more difficult to detect and trace, or are not immediately suspected of being destined for criminal structures. Moreover, the funds usually come from legitimate sources and income streams.

Generally speaking, three different phenomena related to terrorist financing preoccupied the Swiss prosecution authorities in the past, particularly in the period from 2015 to 2019: money transfers to crisis regions via money transmitters; support networks in Switzerland and third countries; and hawala networks, which act as informal funds transfer systems.

A *first* phenomenon that the Swiss prosecution authorities typically focus on concerns payments sent to a high-risk country (e.g. Turkey, Lebanon) via money transmitters. Once there, the transferred funds are probably intended to benefit people suspected of being members or supporters of a terrorist organisation in, say, Syria or Iraq. The recipients of the payments are probably people with jihadist motives who have travelled to a war zone from Switzerland. Often, several people close to these travellers transfer funds to recipients in a high-risk country. The funds are then presumably also used to enable travellers with jihadist motives (and their children) to flee from imprisonment or pay people smugglers to get them across the border, for example from Syria to Turkey.

With the *second* phenomenon, too, money transmitters are the focus of investigations. In this case, the recipients are not in a high-risk country, but are well connected within the various violent Islamist or ethno-nationalist circles in their home country, as well as the diaspora in Switzerland. It is harder to link the recipient of a payment to a specific organisation because his/her contacts with terrorist organisations are organised via looser and farther-flung networks. However, these people are often also under observation by the security services in their home country. In Switzerland, investigations generally focus on various payments to a suspicious person abroad from different people, usually friends, within Islamist or ethno-nationalist circles.

In the *third* phenomenon, the investigation focuses less on the recipient, and more on the systems used to transfer the funds. Transfer systems play a major role in obscuring the recipient or purpose of a transaction. In this regard, investigators in terrorism prosecutions have been able to identify people or networks that are probably part of transnational, informal value transfer systems. An example of this is so-called hawala networks. A person in country X (P_x) gives a hawaladar (a hawala service provider) in country X (H_x) the amount that he/she wants to transfer to a person in country Y (P_y). P_x also sets a password and gives it to H_x. H_x then contacts a hawaladar of his/her choice in country Y (H_y) and informs them of the password agreed with P_x. H_y pays the amount to P_y, once P_y has given them the password received from P_x. Thus, no money passes between either P_x and P_y or H_x and H_y, although H_y now has an outstanding claim against H_x. In addition, both have earned a fee for their services.

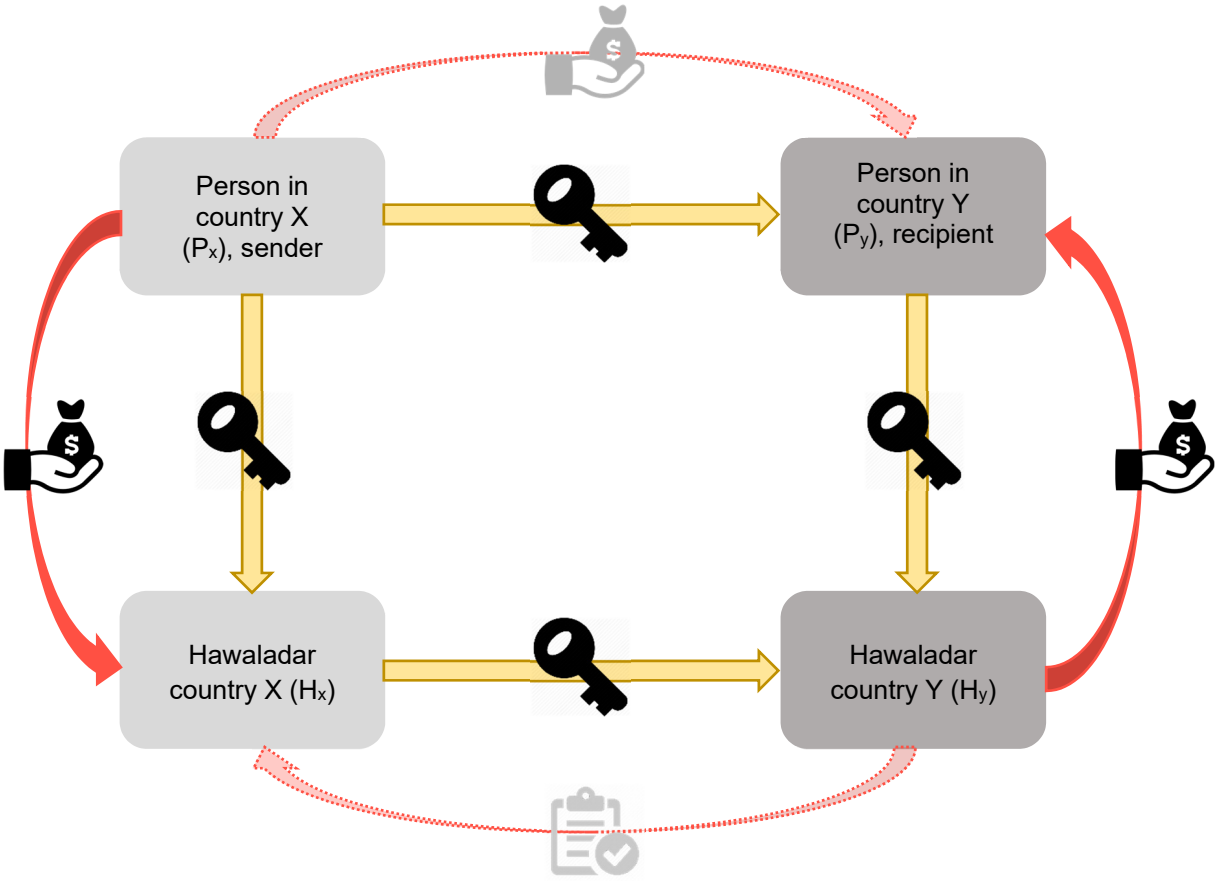


Chart: FCP criminal analysis

Hawala services are not illegal per se, provided the financial intermediation activity is declared. Payments that take place within informal networks are almost impossible to trace. The networks or parts thereof are detected by the prosecution authorities only if they can access someone's personal correspondence with people from such networks, for example. Informal financial intermediaries do not just play a role in the hawala system. Other transactions which would otherwise run through official financial channels also make use of intermediaries in order to obscure the destination or purpose of a payment. Various networks are thus interlinked, making it impossible for a payment to be traced.

Moreover, it should be noted that in terrorism investigations which are not primarily motivated by the suspicion of terrorist financing, the prosecution authorities often uncover evidence of a person's close associates raising funds that are suspected of benefiting terrorist networks. These are mostly small amounts, often received in cash. It is also suggested to the donors that their payments are fulfilling a religious duty. This allows the organisers to fundraise from people who reject terrorist acts and structures, and who genuinely believe that their donation is going to a good cause. The reference to religious rules also serves to conceal the purpose of the funds and makes it more difficult for the prosecution authorities to identify a payment as illegal. The collected cash is forwarded many times, making it even harder to trace. In chat forums, the investigators also uncover forwarded calls for fundraising which originate from sources close to a terrorist organisation itself. For instance, people who were being prosecuted for terrorism were promoting fundraising in aid of IS women detained in a Syrian internment camp. These fundraising calls also contain information on how to make donations to a terrorist organisation as unobtrusive as possible, i.e. without raising the suspicions of a financial service provider's compliance unit or the prosecution authorities (e.g. by avoiding the use of Arabic or Islamic wording).

In all the phenomena described above, the key challenge is to prove that a payment really is destined for terrorist organisations or people who are local members of a terrorist organisation. In this regard, evidence that will stand up in court is particularly difficult to obtain in the destination country of the payment ("battlefield evidence"). Moreover, the judicial authorities in high-risk countries are often rather uncooperative when faced with mutual assistance requests. It should also be noted that it is frequently hard to prove that someone making a payment or donation in Switzerland knew that the funds were going to a terrorist organisation – particularly if they can credibly claim that the donation was to fulfil a religious duty or for humanitarian reasons; it is then virtually impossible to prove that the person knew the money would benefit a terrorist organisation. Complex or hybrid structures in recipient organisations present a further challenge. Even if a recipient organisation can be clearly identified, it is difficult to prove that it or its individual members are supporting terrorist activities.

Even though the Federal Council recently concluded that Article 260^{quinquies} of the SCC does not need to be revised, application of this provision remains difficult, especially when it comes to demonstrating intent. The recent adoption of Articles 260ter and 260^{sexies} of the SCC and Article 74 of the IntelSA[69], which are the main provisions to be applied with regard to terrorist financing, should nonetheless help to improve the situation and facilitate the work of the prosecution authorities.

Against this problematic background, it is evident that personal networks generally play a role in terrorist financing. Although these networks do also make use of official funds transfer channels, they often operate partly or completely outside the official financial infrastructure. As a result, for investigations into terrorist financing and the subsequent identification of potentially illegal payments, the key legislation is not so much the laws that focus specifically on combating financial crime, but rather those that generally prohibit terrorist organisations and their support. It is not until the prosecution authorities are investigating the associates of a person suspected of spreading propaganda for the banned organisations IS or al-Qaeda, for example, that they uncover suspicious payments, fundraising or people that are probably members of informal funds transfer networks. As regards these networks, the investigations should focus on combating terrorist financing. International cooperation between authorities is crucial here, as these networks generally have transnational connections. As a rule, however, the prosecution authorities do not yet know enough about such structures, nor do they know how widespread such systems are in Switzerland.

4.3. Cryptocurrencies

It is difficult to judge whether the significant threat of money laundering and terrorist financing associated with cryptocurrencies and VASPs, as well as Switzerland's vulnerability in this regard, has changed since the publication of the sectoral report on the subject. By contrast, new risk factors have emerged that are linked to the constant technological change which is a feature of this sphere of activity, and the growing popularity of this kind of payment method.

In the FATF's view[70], stablecoins, which have seen considerable growth since 2018, pose risks similar to those associated with other cryptocurrencies, inasmuch as they have the same anonymous character and lend themselves to peer-to-peer transactions between non-custody wallets, i.e. service providers that are neither registered nor subject to supervision. Moreover, since stablecoins stimulate financial innovation and efficiency and foster financial inclusion while reducing the risk associated with price volatility, they could be adopted on a global scale,

[69] See section 3.5 above for details

[70] FATF, *Report to the G20 Finance Ministers and Central Bank Governors on so called Stablecoins*, June 2020, p. 7-9, Virtual Assets – Draft FATF Report to G20 on So-called Stablecoins (fatf-gafi.org)

particularly if they are sponsored by large technology, telecoms or financial companies, which would constitute a major risk factor.

The last few years have also seen the development of new, decentralised business models using cryptocurrencies, in which it is more difficult to identify the traditional role attribution of financial intermediary. Instead of a sole financial service provider, their applications are operated in a decentralised manner, using open-access DLT systems which mimic well-known financial market services. These include, for example, custody, currency exchange and trading in digital assets in the form of tokens. With such models, it is generally difficult to identify an operator. Moreover, certain activities are divided into multiple components, making it even more difficult to categorise them as a service requiring a licence in order to operate as a whole.

In addition, these technological innovations are taking place in an environment of spectacular growth in the circulation of cryptocurrencies. According to estimates by some sector participants, the global daily volume of currency exchange transactions in cryptocurrency, which amounted to around USD 10 million in 2018, grew between five and ten-fold in a year[71], while one of the world's largest cryptocurrency-based currency exchange platforms saw its client base increase by 5 million between 2019 and 2020[72]. Some studies estimate that the fifty largest companies in this group represent nearly 20% of the global stock market capital of the cryptocurrency sector[73]. These developments can also be observed in Switzerland. The growth in the cryptocurrency sector that makes up Switzerland's "Crypto Valley" is exemplified by the number of VASPs affiliated to SROs, which has risen from 2 to 82 in three years, and the increase in banks subject to FINMA supervision that now also offer services in cryptocurrency: there are currently six, as opposed to none in 2018.

Characterised by technological innovations of this kind and by growing popularity, cryptocurrencies might end up providing new opportunities to criminals wanting to use them for laundering their illegally acquired assets or for financing terrorist acts or organisations. Several studies carried out by companies in the sector estimate that the amount of assets and the number of transactions stemming from criminal activity are on the rise[74]. The FATF draws attention to the new risks emerging in connection with these cryptocurrencies, and recommends that they be carefully examined[75]. In a recent report, it also calls on member states to improve implementation of the standard it has drawn up on this subject[76]. The United Kingdom estimates that the risk of money laundering and the associated terrorist financing rose between 2017 and 2020 in the UK[77], while in a number of countries FIUs are observing an increase in the number of SARs relating to crypto assets[78]. On 20 July 2021, the European Commission issued legislative proposals aimed at strengthening the EU rules on combating money laundering and terrorist financing in the area of crypto assets[79].

---

[71] CoinMarketCap, *Total Market Capitalization and 24h Volume*, https://coinmarketcap.com/charts/ (17.08.2020)
[72] Di Salvo, Mathew, *Crypto exchange Coinbase discloses how many users it has*, 26 July 2020, Crypto exchange Coinbase discloses how many users it has – Decrypt
[73] Fintechnews Switzerland, *New Top 50 Crypto Valley Swiss Blockchain List – the Largest and Most Important Companies,* 24 January 2019, https://fintechnews.ch/blockchain_bitcoin/new-crypto-valley-top-50-swiss-blockchain-companies/24878/
[74] Chainalysis*, The 2020 State Of Crypto Crime*, January 2020, p. 5, 257 – 001 Appendix A – 2020-Crypto-Crime-Report Chainalysis.pdf (gov.bc.ca); McGuire, Michael*, Into the Web of Profit. Understanding the Growth of the Cybercrime Economy*, Bromium Inc., April 2018, pp. 26-27, Microsoft Word – Into the Web of Profit FINAL (bromium.com)
[75] Financial Action Task Force (FATF), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, June 2019, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html
[76] Financial Action Task Force (FATF), *Second 12-Month Review of Revised FATF Standards – Virtual Assets and VASPs*, July 2021, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatfguidanceontherisk-basedapproachtocombatingmoneylaunderingandterroristfinancing-highlevelprinciplesandprocedures.html
[77] HM Treasury and Home Office, *National risk assessment…, cit.*, p. 70 *et seq*.
[78] FIU the Netherlands, *Annual Review 2019*, May 2019, p. 18, FIU-the Netherlands Annual Review 2019 (fiu-nederland.nl); TRACFIN, *Annual report* 2019, p. 26; FIU Germany*, Annual report 2019*, pp. 46-47, Zoll online – Jahresberichte
[79] European Commission, "Beating financial crime (europa.eu)", 20 July 2021

In Switzerland too, a rise in reports relating to cryptocurrencies has been observed by MROS. They originate from both VASPs domiciled in Switzerland and traditional financial intermediaries, whose suspicions are increasingly raised by transactions or business relationships linked to cryptocurrencies. However, it has been seen that only a small number of VASPs registered in Switzerland report suspicions, with the result that it is difficult to assess the extent to which the increase in reports reflects changes in risks. As regards the volume of exchanges between fiat currency and cryptocurrency and the exact magnitude of financial flows in cryptocurrencies at international level, no reliable statistical data is currently available. It is also not known what amount of money leaves the Swiss financial centre through purchases of cryptocurrency, or is injected through the sale of cryptocurrency.

To mitigate this risk, which is estimated to be high despite precise measurement not being possible, a legislative ordinance entered into force on 1 August 2021[80]. It takes account of the risks linked to decentralised systems and, accordingly, changes the criteria for becoming subject to the AMLA. Indeed, as the development of new cryptocurrency business models makes it increasingly difficult to identify institutions or people with power of disposal over the assets involved and threatens to create inequality of treatment for different participants, it no longer seems appropriate to regard power of disposal as the decisive criterion for distinguishing between financial service providers that are subject to the AMLA and those that are not. Consequently, the decision on whether services must be subject to the AMLA is now based on whether they permit the transfer of virtual currencies as part of a permanent business relationship. The proposed solution takes into account the heightened money laundering risks in this area and provides this practice with a clearer and sounder footing than hitherto[81]. It is also closer to the solution under European law, which imposes money laundering regulations on services that allow payments to be initiated, irrespective of any power of disposal.

Despite this ordinance, which entered into force on 1 August 2021, Switzerland's growing economic and political exposure to cryptocurrencies, the rapid evolution of this sector and the difficulties in assessing the risks associated with it mean that it is crucial for the situation to be closely monitored, and the sectoral report on cryptocurrencies may need to be updated.

[80] See *Federal Act of 25 September 2020 on the Adaptation of Federal Law to Developments in Distributed Ledger Technology*, (BBl 2020 7559); *Ordinance of 18 June 2021 on the Adaptation of Federal Law to Developments in Distributed Ledger Technology* (AS 2021 400)

[81] FDF, *Federal Council Ordinance on the Adaptation of Federal Law to Developments in Distributed Ledger Technology. Explanatory report on the initiation of the consultation procedure*, p.15, section 4.5 on Article 4 paragraph 1 letter b of the AMLO, Explanatory notes (admin.ch)

5. Conclusion

While the risk of money laundering in Switzerland is considerable, it has not fundamentally changed since the publication of the 2015 NRA report. Switzerland's main exposure still lies in the risk of laundering assets stemming from predicate offences committed abroad, which is the result of its financial centre being so internationally interconnected. In this regard, the impact on Switzerland of large-scale international money laundering incidents, while partly bringing about a change in the measurement of risk according to the reports received by MROS, actually tends to confirm the conclusions of the 2015 NRA report: these incidents underscore the magnitude of the risk associated with foreign corruption, the complexity of the money laundering cases faced by the authorities in charge of pursuing them, the substantial amounts involved and the vulnerability of financial intermediaries that are most involved in international financial activities.

Nonetheless, despite the continuity that can be observed when comparing the risk observed in recent years and that estimated in 2015, some changes are discernible in three areas: online casinos, terrorist financing and cryptocurrencies. The recent legalisation of online casinos and the opening of the first of them in 2019 could give rise to a risk that is not yet precisely quantifiable, while the rapid growth of the cryptocurrency sector could be accompanied by a parallel rise in money laundering risks. As regards terrorist financing, the only notable development has been the inclusion of the financing of individual terrorists and those travelling for jihadist motives, a phenomenon that is subject to appropriate and precise monitoring by the Swiss authorities. Moreover, some areas, such as the financing of proliferation or aggravated tax misdemeanours, have not yet been assessed for their associated risks.

As chapter 3 explains, the Swiss regulatory and legal arsenal in the fight against money laundering and terrorist financing has been improved since 2015, with loopholes being closed and shortcomings addressed, in particular through the adoption of a number of legislative revisions. As emphasised by the Federal Council, including in its latest strategic report on Swiss financial market policy in December 2020, the Swiss authorities will continue to prioritise effective systems for combating money laundering and terrorist financing, and continuously review these systems in order to identify potential areas for improvement.

Annex: Summary table of recommendations made in analysis reports published since 2015 and changes to the mechanisms to combat money laundering and terrorist financing adopted as a result

Report	Recommendations or other suggestions for improvement	Implementation	Brief description of the methods of implementation	Amended law
2015 NRA report	Intensification of the dialogue with the private sector	Recommendation implemented	- Creation by the CGMF of a liaison group with the private sector; the first meeting took place on 27 November 2015 - Awareness-raising by MROS and FINMA - MROS's strategy includes the establishment of a PPP	
	Data gathering and compilation of national statistics by the OAG	Recommendation implemented	The OAG has set up an IT platform and a reporting form for statistical data, which are available to all cantonal public prosecutors. This platform allows full and detailed statistics to be collected on investigations, prosecutions and guilty verdicts, seized or confiscated assets, and international mutual assistance requests. The OAG statistics on mutual assistance are also harmonised with the FOJ.	
	Systematisation of statistics by different players in the fight against money laundering, and transmission of these statistics to MROS	In progress	The introduction of a computerised communication system by MROS in 2020 has paved the way for progress in the statistical treatment of the information it receives. However, not all the Swiss players in the fight against money laundering and terrorist financing send it the information envisaged in the recommendation. MROS is in contact with them to improve the provision of this information.	
	Follow-up of risk assessments	Recommendation implemented	Publication of several thematic risk assessment reports	
	Acceleration of the planned introduction of a national land register accessible to all authorities involved in the fight against money laundering, allowing the identification of people and companies owning real estate in Switzerland	Being partly implemented	The consultation of the offices on the draft amendments to the Land Register Ordinance (LRO) ended on 1 February 2021. The text will be submitted to Parliament soon; however, it envisages the identification of property owners only by means of the AHV number, which excludes foreign owners and corporate owners.	LRO (SR 211.432.1)
	Strengthening of the Federal Supervisory Board for Foundations by providing it with extra resources	Recommendation implemented	Phased increase in headcount since 2015	
	Rapid implementation of Swiss Federal Audit Office recommendations, as part of the Federal Council's strategy on bonded warehouses	Recommendation implemented	- Definition by the FCA of a strategy on the future of bonded warehouses and open customs warehouses which includes measures to combat money laundering and terrorist financing	

			- Review of all operating licences for bonded warehouses and public customs warehouses - Revision of minimum standards for maintaining inventories of warehoused goods, which now include the owner's name and address - Greater frequency of warehoused goods checks triggering administrative measures upon discovery of non-compliant operators - Improved access to information thanks to better IT management of inventories - Amendment of the Customs Act (CustA; SR 631.0) and the Customs Ordinance (CustO; SR 631.01)	
	Amendment of the Code of Obligations concerning accounting rules for raw materials extraction companies with a view to increasing transparency in this area, and international commitment to extending these rules to the entire commodity trading sector	Recommendation partly implemented	On 19 June 2020, Parliament approved an amendment to the Code of Obligations (CO) which requires Swiss companies engaged in raw materials extraction to publish details of the payments they make to governments or other authorities and public sector companies in the countries where they operate. This provision, which entered into force on 1 January 2021, was accompanied by the delegation of powers to the Federal Council, which can decide to extend this measure to cover the entire commodity trading sector. The Federal Council could thus apply it within the context of an international harmonisation procedure.	CO (SR 220).
Report on money laundering and terrorist financing risks in non-profit organisations (NPOs)	Extending the requirement to be entered in the commercial register to cover associations, and requiring associations entered in the commercial register to maintain an up-to-date list of members	Recommendation implemented	As a corollary to the amendment of the AMLA which was approved by Parliament on 19 March 2021, the Swiss Civil Code was also amended and now includes the obligation for all associations whose main activity is collecting or distributing funds abroad to be entered in the commercial register. This amendment also requires such associations to maintain an up-to-date list of members.	Arts. 61, 61*a* and 69 of the CC (SR 210).
	Awareness-raising among NPOs, specifically through the publication of an ad hoc notice by the CGMF	Recommendation partly implemented	Although the CGMF has not yet published the awareness-raising notice for NPOs as recommended in the report, the FDF has raised awareness about the risks identified for the two government agencies that provide financing and organisational support to NPOs, i.e. the SDC and SECO, so that they can take account of them in their activities, specifically in the extended checks they perform on the activities of the NPOs they support.	
Money laundering risks in the case of legal entities	Advisory services provided by lawyers, notaries and fiduciaries during the establishment of a domiciliary company are to be made subject to the AMLA, with sanctions envisaged for breaches	Proposal examined but rejected at parliamentary stage	The draft revision of the AMLA aimed at amending Swiss legislation to take account of the FATF's mutual evaluation report included this proposal to cover the activities of lawyers, notaries, fiduciaries and other financial advice professionals when establishing and managing companies; this was rejected by Parliament.	
	Introduction of the right of anti-money laundering authorities to request information from lawyers,	Proposal rejected at parliamentary stage	As above	

	notaries and fiduciaries regarding their advisory activities on establishing companies			
	Introduction of criminal sanctions for breaches of the obligation to maintain a complete and up-to-date list of those controlling the company as well as the beneficial owners	Proposal accepted and implemented	The 2019 adoption of the Federal Act on Implementing the Recommendations of the Global Forum on Transparency and Exchange of Information for Tax Purposes introduced this provision.	Art. 790*a* paras. 1 to 5 of the CO; Art. 327*a* of the SCC
	Introduction of criminal sanctions for holders of bearer shares who do not report their shareholdings to the company	Proposal accepted and implemented	The 2019 adoption of the Federal Act on Implementing the Recommendations of the Global Forum on Transparency and Exchange of Information for Tax Purposes introduced this provision.	Art. 327 of the SCC
	Direct access for all authorities to companies' shareholder registers	Proposal considered and rejected	Examined as part of the draft Federal Act on Implementing the Recommendations of the Global Forum on Transparency and Exchange of Information for Tax Purposes; it was deemed that the existing legal provisions already ensure transparency in this regard.	
	Introduction of the right for MROS to request information from financial intermediaries on the basis of information requests received from its foreign counterparts	Proposal accepted and implemented	This new prerogative for MROS was incorporated into the AMLA on 25 September 2020 and entered into force on 1 July 2021.	Art. 11*a* para. 2bis of the AMLA
Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding[82]	Switzerland's advocacy within the FATF for the international harmonisation of regulations for companies active in trading and transactions with cryptocurrencies	Recommendation implemented	- Switzerland's active involvement in the FATF's Policy and Development Group	
	Evaluation of the possibility of expanding the AMLA to cover electronic crowdfunding platforms	Recommendation implemented	The advisability of making electronic crowdfunding platforms subject to the AMLA was examined. It was concluded that the number of such platforms in Switzerland and their turnover did not warrant such a step.	
	Explicit mention in the legislation that the issuance of virtual currencies equivalent to means of payment is subject to the AMLA	Recommendation implemented	The Ordinance on the Adaptation of Federal Law to Developments in Distributed Ledger Technology, which was passed on 18 June 2021 and entered into force on 1 August 2021, amends the AMLO and makes the issuance of virtual currencies, which are actually or according to the intention of the organiser or issuer used as a means of payment for the acquisition of goods or services or serve the transfer of money and value, subject to the AMLA.	Art. 4 para. 1bis lit. c AMLO

[82] Most of the recommendations issued on the basis of the risk assessments published in this report were made in the Federal Council report *Legal bases for distributed ledger technology and blockchain in Switzerland*. *Status report, with a special focus on the financial sector*, 14 December 2018. This table includes the recommendations and other suggestions for improvements to combat money laundering contained in this report.

	Explicit mention in the law of FINMA practice, according to which decentralised trading platforms with power of disposal over third-party assets are subject to the AMLA	Recommendation implemented	The Ordinance on the Adaptation of Federal Law to Developments in Distributed Ledger Technology, which was passed on 18 June 2021 and entered into force on 1 August 2021, amends the AMLO and incorporates this explicit stipulation. The Ordinance applies the AMLA not only to decentralised trading platforms with power of disposal but also to those that, although not equipped with power of disposal, permit the transfer of virtual currencies to third parties, in cases where they have a permanent business relationship with the counterparty.	Art. 4 para. 1 lit. b AMLO
Bribery as a predicate offence to money laundering	Amendment of the Code of Obligations concerning accounting rules for raw materials extraction companies with a view to increasing transparency in this area, and international commitment to extending these rules to the entire commodity trading sector	Suggestion partly implemented	See above	
	Introduction of the right for MROS to request information from financial intermediaries on the basis of information requests received from its foreign counterparts	Suggestion accepted and implemented	See above	
	Advisory services provided by lawyers, notaries and fiduciaries during the establishment of a domiciliary company are to be made subject to the AMLA, with sanctions envisaged for breaches	Suggestion rejected	See above	
Supervision of commodity trading activities from an anti-money laundering perspective	Private sector implementation of non-legally binding anti-bribery initiatives	In progress	On 15 January 2020, the Federal Council adopted the revised "Corporate social responsibility (CSR)" action plan for 2020 to 2023, thereby confirming its commitment to corporate social responsibility, including as regards combating bribery.	
	Development and adoption of sector-specific guidelines on anti-money laundering due diligence	In progress	In 2020, the FDF (SIF), together with the association of commodity traders, established a process and a timetable for drawing up these guidelines.	
	Assessment of the scope of the duty to report suspicions	In progress	In autumn 2020, the CGMF decided to wait for the outcome of the parliamentary discussion on the definition of "justified suspicion" warranting a report to MROS under Article 9 paragraph 1 letter a of the AMLA before assessing the appropriateness of extending traders' reporting obligation.	

	International commitment to drawing up a standard that treats relationships with state-owned enterprises (SOEs) and companies which themselves have business relationships with SOEs as high-risk	In progress	Switzerland has engaged in a dialogue with other major commodity trading centres to plan the development of a new joint approach based on the knowledge of the risks of bribery and money laundering in the sector in order to mitigate them.	
	Improving the anti-bribery arrangements by taking into account the OECD's recommendations in this area	Partly implemented	The OECD's evaluation report on Switzerland on the implementation of the OECD anti-bribery convention considers that Switzerland has fully implemented 11 recommendations, partly implemented 18 and not implemented 17.	
Fraud and phishing for the purpose of fraudulent misuse of a data processing system as a predicate offence to money laundering	Improving crime statistics on fraud	In progress	Cybercrime phenomena such as online fraud have been included in the police crime statistics since 2020. https://www.bfs.admin.ch/bfs/fr/home/statistiques/criminalite-droit-penal.assetdetail.16484104.html.	
	Pursuing public awareness campaigns	Recommendation implemented; work in progress	For the past two years, websites promoted by the cantonal and federal police authorities, created well before the report's publication, have focused on warnings against on- and offline fraud. See, for example, the website of Swiss Crime Prevention (PSC – Prévention Suisse de la Criminalité (skppsc.ch)), promoted by the Conference of heads of cantonal justice and police departments, or that of fedpol, specifically: NCSC homepage (admin.ch).	

Bibliography

Federal Customs Administration (FCA), *FCA facts and figures 2021*, FaktenZahlenEZV_2021_EN_Webversion.pdf

Federal decree on the Approval and Implementation of the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol and the Strengthening of Criminal Justice Instruments for combating Terrorism and Organised Crime (BBl 2020 7651), BBl 2020 7651 – Federal decree on the Approval and Implementation of the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol and the Strengthening of Criminal Justice Instruments for combating Terrorism and Organised Crime (admin.ch)

Swiss Banking, *Banking Barometer 2020*. *Economic trends in the Swiss banking industry,* September 2020, Studies, analyses and reports – Swiss Banking (swissbanking.org)

Swiss Banking, *Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CDB 20)*, 2020, SBA_CDB_2020_Agreement EN.pdf (swissbanking.ch)

Swiss National Bank, *Banks in Switzerland*, 2019, Swiss National Bank (SNB) – Banks in Switzerland (snb.ch)

Swiss Civil Code (Recording of marital status and real estate register), BBl 2017 7475, https://www.admin.ch/opc/de/federal-gazette/2017/7899.pdf

Chainalysis*, The 2020 State Of Crypto Crime*, January 2020, p. 5, 257 – 001 Appendix A – 2020-Crypto-Crime-Report Chainalysis.pdf (cullencommission.ca)

Swiss Civil Code of 10 December 1907, (CC, SR 210), SR 210 – Swiss Civil Code of 10 December 1907 (admin.ch)

Swiss Criminal Code of 21 December 1937, (SCC, SR 311.0), SR 311.0 – Swiss Criminal Code of 21 December 1937 (admin.ch)

CoinMarketCap, *Total Market Capitalization and 24h Volume*, https://coinmarketcap.com/charts/

Federal Gaming Board (FGB), *Annual report of the Federal Gaming Board*, 2019, Federal Gaming Board: 2019 annual report (admin.ch)

Federal Council, *Dispatch concerning the amendment of the Civil Code (recording of marital status and real estate register)*, BBl 2014 3395, BBl 2014 3395 – Dispatch concerning the amendment of the Civil Code (recording of marital status and real estate register) (admin.ch)

Dispatch on the federal decree on the Approval and Implementation of the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol and the Strengthening of Criminal Justice Instruments for combating Terrorism and Organised Crime, (BBl 2018 6469), BBl 2018 6469 – Dispatch on the federal decree on the Approval and Implementation of the Council of Europe Convention on the Prevention of Terrorism and its Additional Protocol and the Strengthening of Criminal Justice Instruments for combating Terrorism and Organised Crime (admin.ch)

Federal Council, *Legal framework for distributed ledger technology and blockchain in Switzerland*. *An overview with a focus on the financial sector*, 14 December 2018, Legal framework for distributed ledger technology and blockchain in Switzerland – An overview with a focus on the financial sector (admin.ch)

Federal Council, *Supervision of commodity trading activities from a money laundering perspective. Federal Council report in response to the Seydoux-Christe postulate (17.4204) of 14.12.2017*, 26 February 2020, Supervision of commodity trading from a money laundering perspective – Federal Council report in response to Seydoux-Christe postulate (17.4204) of 14.12.2017 (parlament.ch)

Federal Council, *Land register: country-wide property search using the AHV number, 14* October 2020, Land register: country-wide property search using the AHV number (admin.ch)

Swiss Federal Audit Office, *Free ports and open customs warehouses: licensing and inspection activities, audit mandate 12490*, April 2014, Free ports and open customs warehouses: licensing and inspection activities – Swiss Federal Audit Office (admin.ch)

Swiss Federal Audit Office, *Supervisory activities at free ports and open customs warehouses – Federal Customs Administration, audit mandate 17458*, July 2019, Supervisory activities at free ports and open customs warehouses – Federal Customs Administration – Swiss Federal Audit Office

Swiss Federal Audit Office, *Effectiveness of the precious metals control – Federal Customs Administration, audit mandate 19476*, June 2020, Effectiveness of the precious metals control – Federal Customs Administration – Swiss Federal Audit Office

Federal Department of Finance, *Federal Council Ordinance on the Adaptation of Federal Law to Developments in Distributed Ledger Technology. Explanatory report on the initiation of the consultation procedure*, 19 October 2020, https://www.newsd.admin.ch/newsd/message/attachments/63327.pdf

Di Salvo, Mathew, *Crypto exchange Coinbase discloses how many users it has*, 26 July 2020, https://decrypt.co/36762/coinbase-client-base-up-again-to-35-million-report

Financial Action Task Force (FATF), *National Money Laundering and Terrorist Financing Risk Assessment,* 2013, National Money Laundering and Terrorist Financing Risk Assessment (fatf-gafi.org)

Financial Action Task Force (FATF), *Anti-money laundering and counter-terrorist financing measures, Switzerland, Mutual Evaluation Report*, December 2016, mer-switzerland-2016.pdf (fatf-gafi.org)

Financial Action Task Force (FATF), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, June 2019, VASP guidance.pdf (fatf-gafi.org)

Financial Action Task Force (FATF), *Report to the G20 Finance Ministers and Central Bank Governors on so called Stablecoins*, June 2020, Virtual Assets – Draft FATF Report to G20 on So-called Stablecoins (fatf-gafi.org)

Financial Action Task Force (FATF), *Second 12-Month Review of Revised FATF Standards – Virtual Assets and VASPs*, July 2021, Documents - Financial Action Task Force (FATF) (fatf-gafi.org)

FINMA, *Circular 2011/01. Activity as a financial intermediary in accordance with the Anti-Money Laundering Act (AMLA)*, 20.10.2010, https://www.finma.ch/en/documentation/circulars/.

FINMA, *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, 16 February 2018, https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

FINMA*, FINMA Guidance 02/2019, Payments on the blockchain*, 26 August 2019, finma guidance 02 2019.pdf

FINMA, *Supplement to the guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)*, September 2019, wegleitung stable coins.pdf

FINMA, *FINMA publishes 'stable coin' guidelines*, 11 September 2019, https://finma.ch/en/news/2019/09/20190911-mm-stable-coins/

FINMA, *Annual Report 2020*, FINMA Annual Report 2020.pdf

Fintechnews Switzerland, *New Top 50 Crypto Valley Swiss Blockchain List – the Largest and Most Important Companies,* 24 January 2019, https://fintechnews.ch/blockchain_bitcoin/new-crypto-valley-top-50-swiss-blockchain-companies/24878/

FIU Germany*, Annual report 2019*, pp. 46-47, Zoll online - Jahresberichte

FIU Liechtenstein*, Annual report 2019*, a202783_fiu_jahresbericht_2019_de_Einzelseiten.indd (llv.li).

FIU Luxembourg, *Annual report 2019*, 2019 annual report (public.lu)

FIU Netherlands, *Annual Review 2019*, May 2019, FIU-the Netherlands Annual Review 2019 (fiu-nederland.nl)

HM Treasury and Home Office, *National risk assessment of money laundering and terrorist financing* 2020, December 2020, NRA_2020_v1.2_FOR_PUBLICATION.pdf (publishing.service.gov.uk)

CGMF, *Report on the national evaluation of the risks of money laundering and terrorist financing in Switzerland*, 2015, https://www.newsd.admin.ch/newsd/message/attachments/42276.pdf

CGMF, *Report on money laundering and terrorist financing risks in non-profit organisations*, June 2017, nra-bericht-juni-2017-d (4).pdf

CGMF, *Money laundering risks in the case of legal entities*, November 2017, National Risk Assessment (NRA) - D (5).pdf

CGMF, *Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding*, October 2018, https://www.newsd.admin.ch/newsd/message/attachments/56167.pdf

CGMF, *Report on the national evaluation of the risks of money laundering and terrorist financing in Switzerland*, October 2018, https://www.newsd.admin.ch/newsd/message/attachments/55177.pdf

CGMF, *Corruption as a predicate offence to money laundering,* April 2019, 20190710_ber-korruption-geldwaescherei-d-final.pdf.download.pdf

CGMF, *Fraud and phishing for the purpose of fraudulent misuse of a data processing system as a predicate offence to money laundering,* January 2020, NRA_Bericht_Betrug und Phishing (4).pdf

Federal Act of 30 March 1911 on the Amendment of the Swiss Civil Code, Part Five: The Code of Obligations (CO, RS 220)*,* SR 220 – Federal Act of 30 March 1911 on the Amendment of the Swiss Civil Code (Part Five: The Code of Obligations) (admin.ch)

Federal Act of 20 March 1981 on International Mutual Assistance in Criminal Matters (IMAC, SR 351.1), SR 351.1 – Federal Act of 20 March 1981 on International Mutual Assistance in Criminal Matters (International Mutual Assistance Act (IMAC) (admin.ch)

Federal Act of 10 October 1997 on Combating Money Laundering and Terrorist Financing (AMLA, SR 955.0), SR 955.0 – Federal Act of 10 October 1997 on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA) (admin.ch)

Federal Act of 28 September 2012 on International Administrative Assistance in Tax Matters (SR 651.1), SR 651.1 – Federal Act of 28 September 2012 on International Administrative Assistance in Tax Matters (Tax Administrative Assistance Act, TAAA)

Federal Act of 12 December 2014 on the Proscription of the Groups "Al-Qaeda" and "Islamic State" and Associated Organisations (SR 122), SR 122 – Federal Act of 12 December 2014 on the Proscription of the Groups "Al-Qaeda" and "Islamic State" and Associated Organisations (admin.ch)

Federal Act of 12 December 2014 for Implementing the Revised Financial Action Task Force Recommendations of 2012 (BBl 2014 9465), BBl 2014 9465 – Federal Act for Implementing the Revised Financial Action Task Force Recommendations of 2012 (admin.ch)

Federal Act of 25 September 2015 on the Intelligence Service (IntelSA, SR 121), SR 121 – Federal Act of 25 September 2015 on the Intelligence Service (Intelligence Service Act, IntelSA) (admin.ch)

Federal Act of 18 December 2015 on the Freezing and the Restitution of Illicit Assets Held by Foreign Politically Exposed Persons (FIAA, SR 196.1), SR 196.1 – Federal Act of 18 December 2015 on the Freezing and the Restitution of Illicit Assets Held by Foreign Politically Exposed Persons (Foreign Illicit Assets Act, FIAA) (admin.ch)

Federal Act of 29 September 2017 on Gambling (GamblA, SR 935.51), SR 935.51 – Federal Act of 29 September 2017 on Gambling (Gambling Act, GamblA) (admin.ch)

Federal Act of 21 June 2019 on Implementing the Recommendations of the Global Forum on Transparency and Exchange of Information for Tax Purposes (BBl 2019 4313 and AS 2019 3161), AS 2019 3161 – Federal Act on Implementing the Recommendations of the Global Forum on Transparency and Exchange of Information for Tax Purposes (admin.ch)

Federal Act of 25 September 2020 on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (BBl 2020 7559), BBl 2020 7559 – Federal Act of 25 September 2020 on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (admin.ch)

McGuire, Michael, *Into the Web of Profit. Understanding the Growth of the Cybercrime Economy*, Bromium Inc., April 2018, pp. 26-27, Microsoft Word – Into the Web of Profit FINAL (bromium.com)

Federal Statistical Office, "Adults and minors: Convictions and persons convicted for a misdemeanour or felony under the articles of the Swiss Criminal Code (SCC), by year [2008-2019]", https://www.bfs.admin.ch/bfs/en/home/statistics/crime-criminal-justice/criminal-justice.assetdetail.13407207.html

Ordinance of 8 May 1934 on the Control of Trade in Precious Metals and Articles of Precious Metals (Precious Metals Control Ordinance, PMCO, SR 941.311), SR 941.311 – Ordinance of 8 May 1934 on the Control of Trade in Precious Metals and Articles of Precious Metals (Precious Metals Control Ordinance, PMCO) (admin.ch)

Customs Ordinance of 1 November 2006 (CustO, SR 631.01), RS 631.01 – Customs Ordinance of 1 November 2006 (CustO) (admin.ch)

Ordinance of 23 September 2011 on the Land Register (LRO, SR 211.432.1), SR 211.432.1 – Ordinance of 23 September 2011 on the Land Register (LRO) (admin.ch)

Ordinance of the Swiss Financial Market Supervisory Authority of 3 June 2015 on the Prevention of Money Laundering and the Financing of Terrorism (AMLO-FINMA, SR 955.033.0), SR 955.033.0 – Ordinance of the Swiss Financial Market Supervisory Authority of 3 June 2015 on the Prevention of

Money Laundering and the Financing of Terrorism (FINMA Anti-Money Laundering Ordinance, AMLO-FINMA) (admin.ch)

Ordinance of the Federal Gaming Board of 12 November 2018 on the Diligence of Casinos in Combating Money Laundering and the Financing of Terrorism (FGB Anti-Money Laundering Ordinance, AMLO-FGB, SR 955.021), SR 955.021 – Ordinance of the Federal Gaming Board of 12 November 2018 on the Diligence of Casinos in Combating Money Laundering and the Financing of Terrorism (FGB Anti-Money Laundering Ordinance, AMLO-FGB) (admin.ch)

Gambling Ordinance of 7 November 2018 (GamblO, SR 935.511), SR 935.511 – Gambling Ordinance of 7 November 2018 (GamblO) (admin.ch)

FDJP Gambling Ordinance of 7 November 2018, (GamblO-FDJP, SR 935.511.1), SR 935.511.1 – FDJP Gambling Ordinance of 7 November 2018 (GamblO-FDJP) (admin.ch)

Ordinance of 18 June 2021 on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (AS 2021 400), AS 2021 400 – Ordinance of 18 June 2021 on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (admin.ch)

Organisation for Economic Co-operation and Development (OECD), *Implementing the OECD Anti-Bribery Convention, Phase 4 Report: Switzerland*, 15 March 2018, Switzerland Phase 4 Report.pdf (oecd.org)

Organized Crime and Corruption Reporting Project (OCCRP), *The Russian Laundromat exposed*, 20 March 2017, The Russian Laundromat Exposed – OCCRP

Organized Crime and Corruption Reporting Project (OCCRP), *The Troika Laundromat*, 4 March 2019, The Troika Laundromat – OCCRP

Organized Crime and Corruption Reporting Project (OCCRP), *The Azerbaijani Laundromat*, 4 September 2017, The Azerbaijani Laundromat – OCCRP

Draft Ordinance on the Adaptation of Federal Law to Developments in Distributed Ledger Technology, Consultation initiated on blanket ordinance in area of blockchain (admin.ch)

TRACFIN, *Annual report 2019*, web-ra-analyse-tracfin-19-20-v26_0.pdf (economie.gouv.fr)

Transparency International UK, *Hiding in plain sight. How UK companies are used to launder corrupt wealth*, November 2017, HidingInPlainSight_WEB3.pdf (transparency.org.uk)