Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Report on the national evaluation 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)

June 2015

C:\Users\U80831615\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\EALUOOGN\75503_Ber-GeldwaeschRisiko-Terrorfinanzier-CH_e.doc

Table des matières

Summary

Understanding the risks incurred by a country in the area of money laundering and terrorist financing is a key element of any strategy that aims to reduce them. This report highlights the risks incurred by Switzerland and takes into account not just the financial sector, which is directly subject to specific anti-money laundering standards, but other sectors too. It is the first report of this kind and includes contributions from all of the authorities involved in combating money laundering and terrorist financing.

This report has been drawn up by the interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF). The CGMF is a permanent body that was set up by the Federal Council on 29 November 2013 and mandated to coordinate anti-money laundering and terrorist financing policy matters. In this context, the CGMF is primarily responsible for ensuring the ongoing evaluation of the risks of money laundering and terrorist financing in Switzerland and for proposing the necessary modifications to the system for combating money laundering and terrorist financing, where appropriate, based on the risks identified.

This report shows that Switzerland has a full, coordinated and effective range of legal and institutional resources for combating money laundering and terrorist financing. This system has been strengthened several times in recent years to adapt it to the latest developments and new international standards in the fight against financial crime. Most recently, the Federal Act for Implementing the Revised Financial Action Task Force (FATF) Recommendations was adopted by Parliament on 12 December 2014 and will come into force on 1 January 2016, with the exception of the transparency measures linked to legal entities and bearer shares, which will come into force as early as 1 July 2015. This also applies for the implementing ordinances. Given the importance of its strongly integrated and international financial sector, however, Switzerland is still exposed to risks of money laundering and terrorist financing, in spite of the good prevention and repression system it has in place. Furthermore, the Swiss repression system depends on international cooperation in the area of international mutual assistance.

Based on methodology that combines quantitative data and a qualitative approach, the report shows that the main threats for the Swiss financial sector in terms of predicate offences are fraud (Art. 146 of the Swiss Criminal Code, SCC), including online fraud (e.g. computer fraud, Art. 147 of the SCC), bribery committed abroad (Art. 322^{septies} of the SCC), misappropriation (Art. 138 of the SCC), and support for and participation in a criminal organisation (Art. 260ter of the SCC). Predicate offences are for the most part committed abroad. Moreover, the threat of money laundering linked to cases of bribery abroad and to participation in a criminal organisation pose a higher risk because of their complexity, the large sums of money involved and the difficulty experienced by the criminal prosecution authorities in providing evidence of felonies committed abroad. At the national level, the predicate offences concern street crime in particular, including drug trafficking.

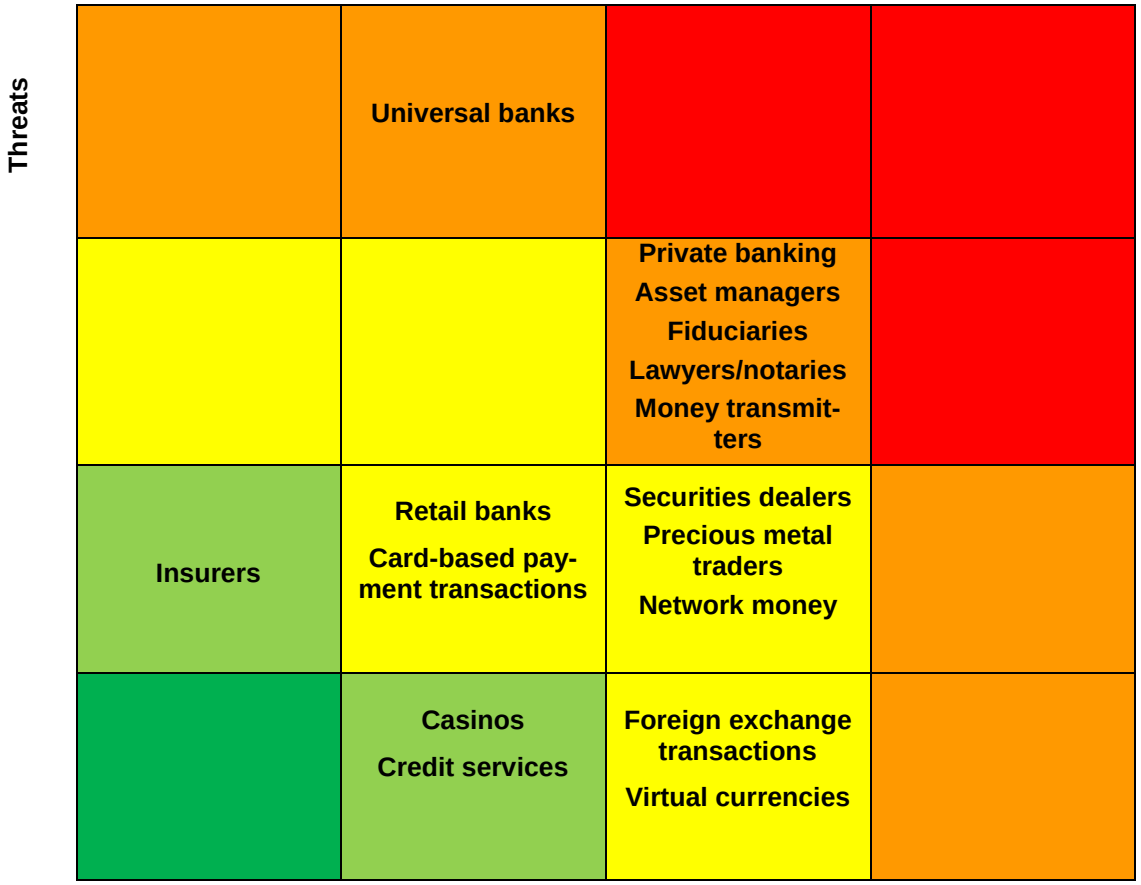
Financial intermediaries are subject to the due diligence requirements of the Anti-Money Laundering Act (AMLA). They are considered an integral part of the system with regard to the detection and analysis of suspicious cases. They have direct contact with clients, are familiar with their profile and activities, and verify their transactions. Based on this, the existing legislation gives them the responsibility of acting as an initial analytical filter so that only the cases where initial suspicions persist are sent to the Money Laundering Reporting Office Switzerland (MROS). This inclusion of financial intermediaries in the system gives rise to close collaboration between them and the authorities responsible for combating money laundering and terrorist financing, which is also reflected in this report.

The analysis shows that the financial intermediaries most exposed to money laundering risks are banks (especially universal banks and private banks), independent asset managers, fiduciaries, lawyers and notaries, and money transmitters. The risk criteria taken into account in the analyses in this report stem from the standards drawn up by the Swiss Financial Market Supervisory Authority (FINMA).

As a key component of the financial centre, the banking sector is exposed to all of the threats. Nevertheless, the risk is reduced by consolidated regulations that are rigorously applied by the sector and by FINMA's direct risk-based supervision. The analysis shows a medium risk for all banks, but a higher risk for universal and private banks. Asset managers, fiduciaries, lawyers and notaries carry a relatively high risk because of the complexity of their business relationships, which very often involve legal structures and higher risks related to the presence of politically exposed persons (PEPs). Independent

securities dealers pose a money laundering risk that varies depending on their type of activity: while the risk tends to be low for proprietary trading, it is higher in the case of dealers acting on behalf of clients and offering asset management and accounting services. Money transmitters pose a medium-to-high risk depending on 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 transaction services pose a medium risk, but this varies depending on the technology used and the degree of regulation in the place where the service has its registered office. There is a medium risk related to trade in precious metals, which is higher, however, for cross-border trade in refined gold involving foundries and for retail trade in old gold. Insurers and casinos carry a money laundering risk that can be considered low, as do credit and leasing services.

In summary, the overall evaluation of the risks of money laundering showed a medium risk for all of the sectors covered by the AMLA. The existing legislation and related measures enable the vulnerabilities with regard to the current threat to be controlled adequately.



Source: CGMF

Switzerland has a limited risk with regard to terrorist financing, primarily through financial intermediation. Currently, the most exposed financial intermediaries are banks, money transmitters and credit services. The sums of money involved are often small. Alongside the method of collecting and transmitting funds and assets through financial services subject to the AMLA, it was found that alternative methods of money transmission, such as the hawala system or the physical transfer of funds, may be used in Switzerland to finance possible terrorist acts. The risk of terrorist financing could therefore develop quickly, especially if terrorist financing networks were to use these alternative money remittance methods more systematically. Not only are these alternative methods beyond the control of the financial system, they also leave very little in terms of a paper trail, which makes them more difficult to detect and considerably obstructs the establishment of evidence in connection with legal proceedings.

In the area of terrorist financing, there is close cooperation at both the national and international levels. The continuation and strengthening of this cooperation, awareness-raising among social partners potentially affected by the issue of terrorist financing – particularly non-profit organisations – and the application of other available legal remedies to combat this scourge are essential for controlling the risk.

The CGMF is of the opinion that the existing legislation for the areas covered by the AMLA, which was supplemented by the Federal Act of 12 December 2014 for Implementing the Revised FATF Recommendations of 2012, responds appropriately to the current risks of money laundering and terrorist financing. Nevertheless, it believes that the implementation of the instruments established by the legislation should be improved further at the operational level. Consequently, the CGMF recommends the following measures to consolidate the current system:

1. Dialogue with the private sector about risks will be intensified. This means that MROS and FINMA are to further increase awareness among financial intermediaries exposed to risks as part of their respective tasks. Furthermore, as part of the CGMF's work and in coordination with the authorities concerned, a regular dialogue will be established with the financial sector and, as needed, with other sectors regarding the outcome and forthcoming risk evaluation work and the ways in which to tackle the issues. This dialogue will also look at emerging risks from the perspective of a mutual early warning system between the public and private sectors.
2. The Office of the Attorney General of Switzerland is to continue gathering and analysing information from the cantonal and federal criminal prosecution authorities in the field of money laundering and terrorist financing, particularly for establishing consolidated statistics on the processing of cases in these areas.
3. The public and private players involved in combating money laundering and terrorist financing are to develop and systematise statistics taking the quantitative measurements used in this report into consideration, particularly when entering information on suspected predicate offences and the place they were committed. This information will be made available to MROS once a year so it can be included in its annual report, where relevant.
4. The CGMF will continue to perform risk analyses. It will update existing analyses based on the development of money laundering and terrorist financing threats and extend its analyses to include new predicate offences for which there are currently no risk analyses, particularly tax-related predicate offences.

This report also includes analyses of six areas, based on qualitative studies, that are not directly subject to the AMLA and which were selected as a result of their economic significance and the interest triggered in Switzerland by certain activities in these areas in recent years. These areas are the real estate sector, non-profit organisations, cross-border cash transfer, free ports, trade in works of art and commodities trading. Measures have been put in place to reduce the risks in these areas. Nevertheless, the CGMF has drawn up additional measures to respond to the shortcomings identified in this report:

5. In order to reduce the vulnerabilities identified in the real estate sector, the national real estate register envisaged in the Federal Council dispatch of 16 April 2014[1], and which is accessible to the federal authorities, must be implemented swiftly. However, the national register will be limited to registering only the AHV numbers of building owners. In order to enable the federal authorities to carry out effective searches on foreign owners of property in Switzerland too, it should be possible to perform searches based on full names, or on company names for legal entities that own property.
6. To enhance supervision and thus reduce the risks of foundations being used for money laundering and terrorist financing purposes, the Federal Supervisory Board for Foundations should be strengthened and allocated additional resources. The CGMF will also work with the authorities responsible for supervising foundations and with the authorities involved in the area of non-profit organisations to draw up proposals for specific measures where necessary.
7. The Federal Council's strategy on customs warehouses[2] must be put into practice primarily by implementing the recommendations of the Swiss Federal Audit Office and by establishing a legal framework through an implementing ordinance. In particular, the warehousing of goods for export should only be permitted for a defined period of time, and inventory

[1] Dispatch of 16 April 2014 concerning the amendment of the Swiss Civil Code (Recording of marital status and real estate register), Federal Gazette (BBI) 2014 3395, 3420

[2] Cf. Dispatch of 6 March 2015 on the amendment to the Customs Act, BBI 2015 2657, p. 2665

contents should be expanded together with the disclosure obligation of the warehouse-keeper and storing party. When implementing the recommendations of the Swiss Federal Audit Office, it is essential that the inspections conducted in free ports are made more consistent.

8. The proposals contained in the preliminary draft of the amendment to the Swiss Code of Obligations (law on companies limited by shares)[3] concerning accounting rules for raw materials extraction companies in order to ensure greater transparency in this area, and the extension of these rules to the commodities trading sector as part of an internationally coordinated approach, should be included in the future bill and the corresponding dispatch which will be submitted to Parliament.

[3] Preliminary draft of the amendment to the Swiss Code of Obligations (law on companies limited by shares), in consultation from 28 November 2014 to 15 March 2015

1 Introduction

Switzerland attaches great importance to preserving the integrity, attractiveness and efficiency of its financial centre. It does everything it can to ensure that the financial centre is not abused for criminal purposes, in particular for money laundering or terrorist financing. Over the past few decades, Switzerland has been gradually developing a robust and comprehensive system for combating money laundering and terrorist financing which combines preventive and repressive measures. It regularly adapts this system in order to take account of the latest threats and the development of international standards in this area and to maintain the system's effectiveness.

Combating money laundering and terrorist financing effectively and successfully, particularly in terms of prevention, also depends on the creation and pooling of initial risk analysis skills at the national level and on the various competent authorities' understanding of criminal activities.

Taking effective action against money laundering and terrorist financing requires resources to be concentrated based on the risks in question. Long before the Financial Action Task Force (FATF) adopted a standard on the matter in 2012[4], Switzerland had already been applying a risk-based approach and regularly coordinating policies on the matter between anti-money laundering and terrorist financing authorities, which included dialogue on the risks of money laundering and terrorist financing in the financial and non-financial sectors. Since 2003, the Swiss Federal Banking Commission (SFBC) and the Anti-Money Laundering Control Authority (AMLCA), both of which are now part of the Swiss Financial Market Supervisory Authority (FINMA), had been calling on all banks to invest in the prevention of money laundering by systematically adopting a risk-based approach. The risk-based approach allows banks to adapt their anti-money laundering system to their activities, to the individual features of these activities and to the specific risks they entail. The analysis of money laundering and terrorist financing risks is not just a matter for the various private-sector players concerned; it is also to a large extent the responsibility of national authorities. Close operational contacts – via the regular exchange of information – had existed since 2007 between the authorities responsible for combating money laundering and terrorist financing at the federal and cantonal levels[5]. Moreover, the relevant authorities had already been conducting isolated risk analyses for several years for their own monitoring needs. However, the Federal Council felt it was time to establish a permanent structure to enhance coordination and analytical capabilities with regard to the global issue of combating money laundering and terrorist financing. It believed that this type of structure would strengthen coordination between the authorities concerned at the policy and operational levels and provide a mechanism for performing new specific tasks, such as the systematic evaluation of the risks of money laundering and terrorist financing.

Establishment of a permanent interdepartmental body

On 29 November 2013, the Federal Council established the interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF). The CGMF is a permanent body mandated to coordinate anti-money laundering and terrorist financing policy matters, including risk evaluation. Its main tasks are: (i) coordinating anti-money laundering and terrorist financing policy; (ii) ensuring the ongoing evaluation of money laundering and terrorist financing risks; (iii) proposing risk-based modifications to the anti-money laundering and terrorist financing system; and (iv) helping to

[4] According to the first FATF recommendation, countries should identify, evaluate and understand the money laundering and terrorist financing risks to which they are exposed and should take measures, including the appointment of an authority or mechanism for coordinating risk evaluation actions, and mobilise resources to ensure that risks are effectively reduced. Based on this evaluation, countries should apply a risk-based approach to ensure that the measures for preventing and reducing money laundering and terrorist financing risks are commensurate with the risks identified. This approach should constitute the essential basis for the efficient allocation of resources within the anti-money laundering and terrorist financing mechanism and for the implementation of risk-based measures for all of the FATF recommendations. Whenever countries identify higher risks, they should ensure that their mechanism is able to deal with these risks satisfactorily. Whenever countries identify lower risks, they may decide to authorise simplified measures for some FATF recommendations under certain conditions.

Countries should oblige financial institutions and designated non-financial companies and professions to identify and evaluate their money laundering and terrorist financing risks and to take effective measures to reduce them.

[5] Mainly between FINMA (managing the coordinating group), the Money Laundering Reporting Office Switzerland (MROS), the Federal Gaming Board (FGB) and the criminal prosecution authorities.

ensure that Switzerland's anti-money laundering and terrorist financing policy is consistent with international developments.

The CGMF is under the leadership of the Deputy State Secretary of SIF, which is attached to the FDF, and is composed of members of management from the following offices: FCA (FDF); fedpol, FOJ, FGB (FDJP); FIS (DDPS); DIL, SFPD (FDFA); FINMA and the OAG. The CGMF meets regularly. It consists of three permanent technical working sub-groups that hold regular meetings and have been assigned specific tasks in the areas of (i) risk evaluation, (ii) exchange of information and coordination of operational matters, and (iii) the processing of foreign terrorist lists. The Federal Council adopted a mandate for the CGMF and its working sub-groups. The CGMF has met eight times since it was established, and its working sub-groups have met at regular intervals. The CGMF reports to the Federal Council at least once a year on the status of its work, primarily regarding risks evaluated, and submits proposals for measures to address the situation, where necessary.[6]

This report on the national evaluation of the risks of money laundering and terrorist financing in Switzerland, which has been drawn up by the CGMF, is in line with the Federal Council's overall policy to guard against threats that could jeopardise the integrity of Switzerland's financial centre. In this way, Switzerland is also contributing to concerted efforts at the international level to prevent money laundering and terrorist financing.

This report is part of the strengthening of the efforts made by Switzerland over the past twenty years in response to the increasing scale of financial flows linked to money laundering and terrorist financing globally. It assesses the threats and vulnerabilities related to money laundering and terrorist financing in the main areas subject to the Federal Act of 10 October 1997 on Combating Money Laundering and the Financing of Terrorism in the Financial Sector (AMLA)[7] and in other selected areas not subject to it. To ensure the largest possible range of sources and data for this national risk analysis, the CGMF asked a considerable number of public and private players[8] to provide relevant analyses, statistics and information related to their areas of activity, thereby supplementing the detailed information contained in the suspicious activity reports already in the possession of MROS.

The report is structured as follows:

The first part contains the aims of the report (chapter 2) and the basic concepts (chapter 3). It also provides definitions of money laundering, terrorist financing and related key terms.

The second part (chapter 4) describes the methodology used for the analysis, which has a quantitative component for risk measurement and a qualitative component for aspects relating to threats and vulnerabilities.

The third part (chapter 5) provides an overview of Switzerland's economic, political, legal and institutional framework to facilitate understanding of the overall conditions for combating money laundering and terrorist financing in Switzerland, and the existing risk mitigation measures.

The fourth part (chapters 6 and 7) contains the actual risk analysis. The overall analysis of the threat of money laundering and terrorist financing is followed by sector-by-sector analyses, for which the methodology described in the second part was applied. These chapters also outline the measures that have been taken to date to reduce the risks identified.

The final part of the report contains conclusions and recommendations for the areas where additional measures appear necessary (chapter 8), based on the analyses carried out.

2 Aims of the report

Money laundering and terrorist financing are forms of financial crime which develop in parallel with the growing interdependence of economies and with technological progress, particularly in communication. This promotes the mobility of capital, which in turn produces the potential and opportunities for abuse, especially for laundering the proceeds from criminal activities and financing terrorist activities. Not only does this lead to increased risks and more significant predicate offences to money laundering and terrorist financing globally, it also gives rise to a growing internationalisation of crime, which often

[6] The CGMF reported to the Federal Council for the first time at its meeting on 5 December 2014.

[7] SR 955.0

[8] The public-sector players are FINMA, the FGB, the FOJ, the Offices of the Attorney General of Switzerland and three cantons, the Federal Supervisory Board for Foundations and the FIS. The private-sector players that contributed included banks, money transmitters, self-regulatory organisations (SROs) and professional associations.

involves several jurisdictions. Moreover, money laundering and terrorist financing techniques are constantly evolving, which calls for constant vigilance and the regular adaptation of measures to combat these phenomena. Given the importance of its largely integrated, international financial sector, Switzerland is exposed to money laundering and terrorist financing risks. Setting out from this premise, the main aim of the report is therefore to identify and gauge the size of the various money laundering and terrorist financing threats at the national level and to detect the vulnerabilities, i.e. the specific factors which enable these threats to materialise in the country's various economic sectors.

In parallel, this report will enable the main players involved in the national risk analysis process to develop a common understanding of the main threats and, at the same time, to better understand the risks identified in their respective sectors.

This national risk analysis will also serve as a basis for demonstrating, within the scope of Switzerland's fourth FATF mutual evaluation, the adequacy and effectiveness of the measures applied nationally through the prevention, detection, communication and repression systems in respect of the extent of the threats and vulnerabilities identified in this report.[9] The results of this evaluation will also enable the different authorities and players involved in combating money laundering and terrorist financing to make specific recommendations, where necessary, on the action to be taken with regard to the risks identified and to set priorities according to the importance attached to the risks. Similarly, the results of the national risk analysis will guide the private-sector players concerned, primarily financial intermediaries, and enable them to optimise the preventive efforts made in their respective areas of activity.

3 Basic concepts

3.1 Money laundering

From a criminological perspective, money laundering can be defined as a process that consists in integrating the proceeds from a criminal activity into the regular economic system with the aim of concealing their criminal origin by making them appear permanently legitimate to other players[10]. In this way, money laundering serves a dual objective. Firstly, money launderers aim to prevent the authorities from seizing their assets through concealment so that they can actually use and benefit from them. Its second objective is to avoid the detection and establishment of the offence and consequently, to prevent the conviction of the perpetrators and the forfeiture of their assets of criminal origin. The proceeds of the crime are important evidence for determining the predicate offence.

In Switzerland, money laundering is punishable under Article 305bis of the Swiss Criminal Code (SCC)[11]; it is defined as an act obstructing the administration of justice which aims to frustrate the identification of the origin and the tracing or forfeiture of assets of criminal origin.[12] The term "assets" refers to a very broad concept and includes all of the typical financial market instruments, such as Swiss and foreign banknotes and coins, foreign currencies, precious metals, securities, including cer-

[9] In keeping with the FATF guidelines in National Money Laundering and Terrorist Financing Risk Assessment 2013

[10] IMF, UNODC 2005

[11] SR 311.0; Art. 305bis of the SCC: Money laundering

1. Any person who carries out an act that is aimed at frustrating the identification of the origin, the tracing or the forfeiture of assets which he knows or must assume originate from a felony, is liable to a custodial sentence not exceeding three years or to a monetary penalty.
2. In serious cases, the penalty is a custodial sentence not exceeding five years or a monetary penalty. A custodial sentence is combined with a monetary penalty not exceeding 500 daily penalty units.

A serious case is constituted, in particular, where the offender:

a. acts as a member of a criminal organisation;
b. acts as a member of a group that has been formed for the purpose of the continued conduct of money laundering activities; or
c. achieves a large turnover or substantial profit through commercial money laundering.

3. The offender is also liable to the foregoing penalties where the main offence was committed abroad, provided such an offence is also liable to prosecution at the place of commission.

[12] Article 305bis paragraph 2 of the SCC also defines aggravating circumstances and establishes a custodial sentence not exceeding five years for such cases.

tificated and uncertificated, and their derivatives[13]. The AMLA defines due diligence requirements for financial intermediaries and – from 1 January 2016 – traders for cash transactions in excess of CHF 100,000.

Money laundering presupposes that the assets in question are of criminal origin and that a predicate offence to the act of money laundering itself was committed. In Switzerland, offences that carry a custodial sentence of more than three years are deemed felonies (Art. 10 para. 2 of the SCC). All felonies can constitute predicate offences to money laundering to the extent that they generate assets. The Federal Act of 12 December 2014 for Implementing the Revised FATF Recommendations of 2012[14] broadens the spectrum of predicate offences, which will also include certain misdemeanours defined under direct taxation (Art. 305bis para. 1 and 1bis of the SCC) from 1 January 2016. Article 305bis paragraph 3 of the SCC establishes that "the offender is also liable to the foregoing penalties where the main offence was committed abroad, provided such an offence is also liable to prosecution at the place of commission".

Money laundering is also punishable in the case of guilt through failure to act[15]. In parallel, Swiss legislation defines insufficient vigilance on the part of financial intermediaries as an offence under Article 305ter paragraph 1 of the SCC, of which a financial intermediary can be convicted, even in the absence of a predicate offence giving rise to specific acts of money laundering.

3.1.1 The money laundering process

Money laundering is generally described as a process consisting of three stages. The first stage is *injection* or *placement* (stage I). The assets, often in the form of cash, are moved geographically, converted into other physical or banking assets, or commingled with assets of a legitimate origin, such as through trade based mainly on cash exchanges. In the second stage, known as *layering* (stage II), the origin of the assets is further concealed by physically or virtually separating them from the felony committed. This stage is often carried out by multiplying and/or increasing the frequency of cross-border transfers, which both splits up and transforms the apparent nature of the assets into different structures, for instance through offshore companies, foundations or commercial enterprises, with the aim of reducing their traceability. The third stage, known as *integration* (stage III), involves the dilution and reintegration of the assets into the regular economic system, for example by purchasing real estate or different commercial establishments[16]. In this respect, the Swiss financial sector is exposed to all three stages of money laundering. The acts of money laundering which ensue as a result of predicate offences committed abroad primarily concern stages II and III.

3.1.2 Complexity

The probability of detecting money laundering cases and the effectiveness of their criminal prosecution depends considerably on the degree of complexity of the individual cases. Paradoxically, suspicions of money laundering often arise as a result of the complexity of relationships and financial transactions because it is precisely this complexity that is recognised as being likely to conceal a potential link to assets of criminal origin. The most common complexity factors are: the commission of a predicate offence abroad, the number of jurisdictions involved (cross-border crime), the number and nature of the economic players, the use of somewhat opaque structures (domiciliary companies, trusts, etc.) and the number of financial intermediaries[17]. The complexity of cases calls for increased vigilance and therefore greater efforts from the authorities responsible for detecting and prosecuting money laundering.

3.2 Terrorist financing

Terrorist financing can be defined as an act which collects assets and makes them available to persons or entities for the purpose of financing a terrorist operation, or which makes assets available to persons or organisations that will use them to lead, sponsor or facilitate terrorist activities. From a criminological perspective, the main objective of a terrorist financing act is to conceal the intention of using the assets provided for terrorist purposes. The fact that the assets used can stem from criminal

[13] Cf. "Délimitations dans le domaine de la gestion de valeurs patrimoniales", FDF, 8 March 2007
[14] AS 2015 1389
[15] Federal Supreme Court, decision of 18 September 2008, SK.2007.28 and 2008.16
[16] Bernasconi 1988
[17] Similarly, Article 12 paragraph 2 letter h of the AMLO-FINMA stipulates that the complexity of structures must be considered a higher risk factor.

activities as well as very often legitimate activities, or a mixture of both, makes detection more difficult. Moreover, the financing of terrorist acts, such as the procurement of weapons and explosives, requires only small amounts of funds.

The Swiss legal system has a broad range of provisions for effectively combating and punishing terrorist financing. Specifically, the financing of terrorism is an offence under Article 260^{quinquies} of the SCC. It is not necessary for the objective of intimidation or coercion to be achieved in order for the felony to be considered as having been committed. The punishability of financing is not incidental, which means that it does not depend on an act of terrorism actually being carried out or even attempted. As a separate offence under Article 260^{quinquies} of the SCC, terrorist financing does not require there to be a causal relationship with a previous act of terrorism. This article also enables the targeting of terrorists acting alone or of groups that are not as well as structured as a criminal organisation. When a specific act of terrorism is financed or is about to be financed, a large number of criminal provisions are applicable, under which the act of financing is punishable as an act of participation. It is worth mentioning here that under Article 260bis of the SCC (Acts preparatory to the commission of an offence), activities in preparation of an act of terrorism (including financing) may also be prosecuted even before the commission of the act has commenced.

With regard to suppressing the financing of terrorist organisations and terrorists, Article 260ter of the SCC (Criminal organisation) and the Federal Act of 12 December 2014 on the Prohibition of al-Qaeda, Islamic State and Associated Organisations[18] are also applicable. Article 260ter of the SCC prohibits participation in and support for a criminal or terrorist organisation. All types of financing acts constitute typical forms of support. The Federal Act on the Prohibition of al-Qaeda, Islamic State and Associated Organisations exhaustively prohibits all behaviour aimed at supporting terrorist organisations, which also includes supplying human or material resources (direct or indirect financing). This provision also covers acts of financing for the benefit of individuals who support such organisations in any manner.

All of the acts prohibited under the key criminal provisions, and particularly terrorist financing and participation in and support for a terrorist organisation (Art. 260ter and Art. 260^{quinquies} of the SCC), as well as those prohibited by the new Federal Act on the Prohibition of al-Qaeda, Islamic State and Associated Organisations fall under the category of felonies and also constitute predicate offences to money laundering.

3.3 Criminal risk assessment

3.3.1 Criminal risk

Criminal risk is defined as the fact that a crime phenomenon may materialise in the future with a certain probability. In order to assess the criminal risk associated with money laundering and terrorist financing, two distinct elements that make up the risk should be taken into account: the threat and the existing possible weaknesses (known as vulnerabilities) that would make the commission of an act of money laundering or terrorist financing easier.

3.3.2 Threats

Threats are defined as the probability of a person or a group of people committing acts of money laundering or terrorist financing. A threat assessment identifies the scale of the threat by measuring both its size (quantitative element) and its characteristics (qualitative element). At the same time, a distinction should be made between potential and real threats. A *potential threat* (or abstract threat) is defined as the probability of a threat actually being able to materialise given certain structural and contextual elements. A *real threat* (or concrete threat) is defined as the set of threats that materialise and that can, in principle, be measured.

3.3.3 Vulnerabilities

Vulnerabilities are the set of (structural and institutional) factors that make the commission of a felony appealing to a person or group of people who wish to launder money or contribute to the financing of terrorist acts. The probability of a risk materialising is even greater if there are vulnerabilities. *General vulnerabilities* are inherent in the structural characteristics of a country and its financial centre. *Specific vulnerabilities* are linked to the practices and instruments used in a certain area of activity. The last

[18] SR 122

category is *vulnerabilities linked to the institutional system* (regulation and supervision) for combating money laundering and terrorist financing.

4 Methodology

Based on experience with the risk-based approach applied in Switzerland, the CGMF opted for a combination of quantitative and qualitative approaches. The combined approach offers the double benefit of setting an objective basis for the threat assessment and increasing the information sources that are likely to consolidate and complete the risk evaluation. The combined approach also makes it possible to set an open framework for private-sector parties, who can thus contribute to the risk analysis with their own experience and evaluations. Furthermore, with the aim of perceiving the risks as realistically as possible, the quantitative measurements were compared with the potential threats that were established using a large number of sources. For this, the CGMF considered all relevant information from international and national, public and internal reports, as well as the official statistics available in Switzerland that were likely to focus on money laundering and terrorist financing risks (the complete list of public reports and statistics consulted can be found in the appendix). The CGMF mapped all of the existing national assessments that dealt with the threat of money laundering and terrorist financing in Switzerland and took these into account for the risk evaluation. The CGMF also decided to perform analyses on the areas of activity that are not directly covered by anti-money laundering and terrorist financing legislation, based on their economic significance and the interest that certain activities in these areas have triggered in Switzerland in recent years. Given the absence of suspicious activity reports from these areas of activity, the corresponding analyses are mainly based on a qualitative evaluation.

4.1 Quantitative measurements

To identify the *real threat* in Switzerland, the CGMF initially relied on the database of suspicious activity reports submitted to MROS between 2004 and 2014. Due to the singularity of Swiss legislation, which stipulates that financial intermediaries are required to perform a prior analysis of the facts and elements available to them if suspicions arise, the statistics produced on the basis of suspicious activity reports can be considered as the statistical instrument available that best represents real threats in Switzerland, in terms of both their size and their characteristics. Using these statistics, it is possible in particular to identify the scale of the main predicate offences associated with the different areas and the place of domicile of the counterparties and beneficial owners. The statistics based essentially on the data generated as part of the regulated activity of financial intermediaries were supplemented with information about financial circuits outside of financial intermediation. Moreover, the CGMF gave more than 20 mandates to representative players in the private sector, which provided it with quantitative and qualitative data specifically established for this analysis.

In parallel, on the basis of the suspicious activity reports submitted between 2004 and 2014, a quantitative risk matrix was prepared with a view to establishing an objective measurement of the risk vis-à-vis the areas active in the financial intermediation covered by the AMLA. To this end, five main risk factors stemming from the FINMA regulations were taken into account. These involved risk associated with:

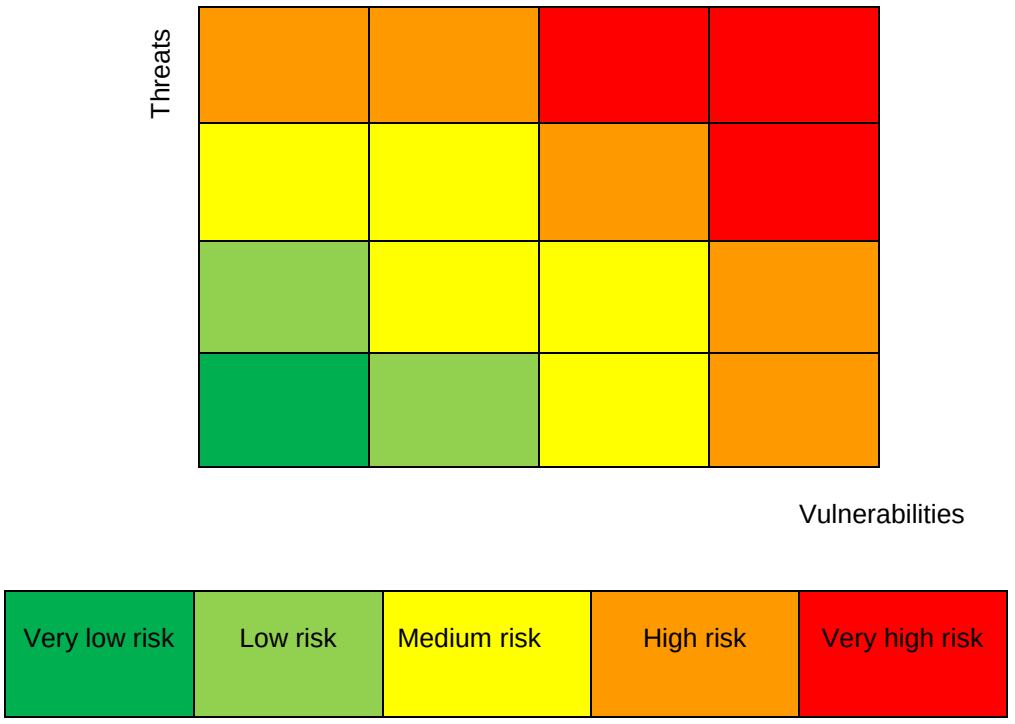
1. the country(ies) involved,
2. the size of the amounts involved,
3. the number of players involved,
4. the involvement of domiciliary companies, and
5. the presence of politically exposed persons (PEPs) as an increased risk factor.

The result for each factor was then weighted using a coefficient deemed relevant[19], which thus completed the risk calculation algorithm (the results achieved for each area and a detailed description of the procedure used can be found in the appendix). For the CGMF, the results achieved in this way were an additional initial indicator for the overall evaluation of the risks for each of the areas examined.

[19] A high coefficient was used for the presence of foreign PEPs and the use of domiciliary companies given that these risk factors significantly influence the level of risk.

4.2 Qualitative risk assessment matrix

For the overall risk assessment, the CGMF performed an evaluation tailored to each area in a second phase, which took into account the information provided by the private-sector players and all relevant information that could enlighten the CGMF on the level and development of threats as well as the particular nature and size of the specific vulnerabilities (existing and future) in the area in question. In this regard, the CGMF gave specific analysis mandates to the relevant services within the administration concerned with the various areas of activity examined. For the sake of readability, the result of this overall risk evaluation process has been summarised in a two-axis matrix which represents the levels of threats and vulnerabilities identified in the respective areas. The result achieved in this way was classified according to one of the following five risk levels: very low risk, low risk, medium risk, high risk and very high risk. Given that the risk criteria used for the quantitative calculation are applied solely to financial intermediaries, only a qualitative analysis was conducted on the areas not covered by the AMLA.



5 Information on Switzerland's general framework

Switzerland is a federal state consisting of 20 cantons and six half-cantons, which are broken down further into communes. The cantons are considered sovereign in that they have their own constitutions and laws and have considerable autonomy. They all have their own parliament, government and their own judicial institutions. The cantons are responsible for all of the affairs which do not come under the Confederation's responsibility. Powers are shared in the areas of policing and justice, as well as for social and economic matters. The cantons are responsible for applying not only their own laws and rules, but also a considerable number of regulations issued by the Confederation. In relation to combating money laundering and terrorist financing, the Confederation has the power to establish legislation, while both the cantons and the Confederation are responsible for implementation and criminal prosecution.

5.1 Composition of the economic and financial sector

In 2013, Switzerland's gross domestic product (GDP) stood at CHF 635 billion. Although 72% of its GDP comes from the service sector, the industrial sector is still an important pillar of the Swiss economy, accounting for 27% of GDP. The key industries are chemicals, capital goods (machine tools, precision instruments, mechanical equipment), watchmaking, food and construction, while the service sector is dominated by banks, insurers, tourism and the public sector. The Swiss economy is strongly geared towards exportation, with foreign trade accounting for approximately two thirds of its GDP. The

European Union (EU) is Switzerland's most important trade partner (59.7% of exports, 78% of imports). The prevalence of small and medium-sized enterprises (SMEs) has always been characteristic of the structure of the Swiss economy. Over 99% of companies in Switzerland have fewer than 250 employees expressed in full-time equivalents (FTEs).

5.1.1 Economic significance of the financial sector[20]

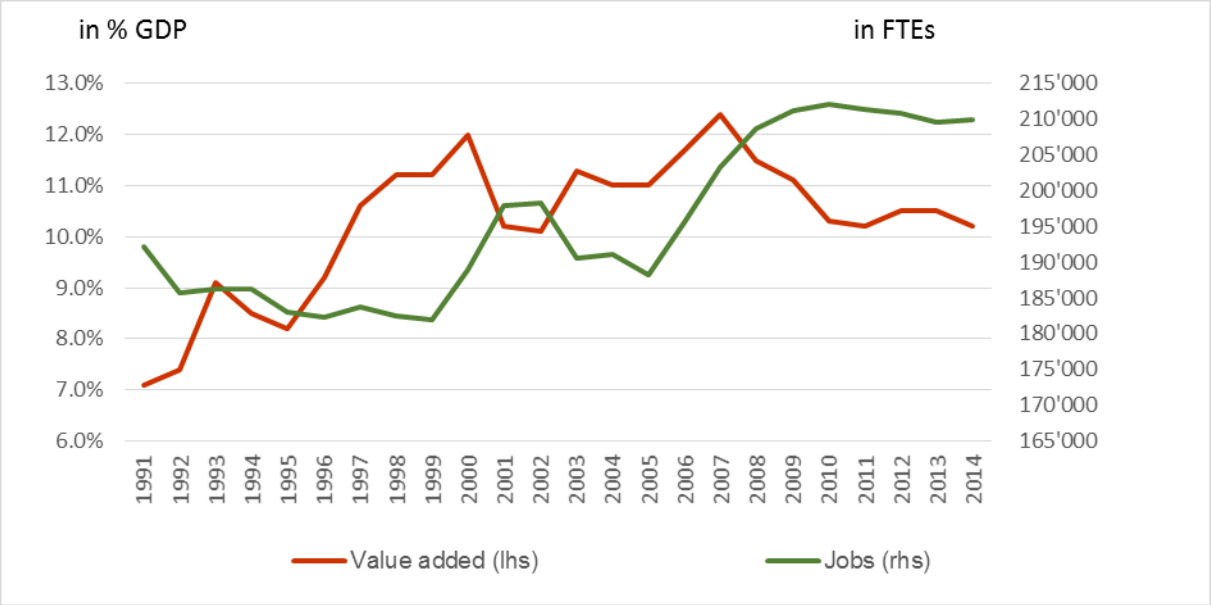
The Swiss financial centre is extremely important for the national economy, both as a catalyst enabling its proper functioning and in terms of revenue and employment. Its key participants are banks, followed by insurers, the fund industry, the stock exchange and pension funds, which together contributed 10.2 % to GDP in 2014 (cf. Figure 1). This represents a decline of some two percentage points on the financial sector's share of GDP in 2007 – the year prior to the outbreak of the financial crisis. With around 210,000 full-time equivalent (FTE) positions, the financial sector accounted for 5.9% of overall employment in Switzerland in 2014 and has been relatively stable for many years.[21]

Switzerland's financial centre also accounts for a significant share of the country's tax receipts. In 2012, the financial sector contributed some CHF 5.7 billion to taxes from natural persons and legal entities; this represented around 7.4% of the total tax receipts of the Confederation, cantons and communes.

Nevertheless, the outbreak of the financial crisis, the changing needs of clients (particularly private), technological progress and the development of standards for financial sector governance at the international level have accelerated the structural changes in the Swiss financial sector. At the end of 2014, the Swiss banking sector thus comprised 283 active banking institutions, 59 less (-17.3%) than in 2003.

Around two thirds of all banks are either foreign banks or have an international focus – such as the big banks, the private banks, and the stock exchange banks.[22] This clearly reflects the heavily international orientation of the Swiss financial centre. Nevertheless, it is worth noting that there is a significant cluster of predominantly domestic-oriented banks, in addition to those with an international focus. At the end of 2013, for example, the cantonal and regional banks had on their balance sheets claims and liabilities relating to Swiss counterparties that stood at 99% and 94% respectively.[23]

Figure 1: Proportion of GDP accounted for by the financial sector from 1991 to 2014 and jobs in this sector



Sources: Federal Statistical Office (FSO); State Secretariat for Economic Affairs (SECO)

[20] "Report on Switzerland's financial market policy" of 19 December 2012; updated in September 2014

[21] Source: Federal Statistical Office (FSO)

[22] SNB, Banks in Switzerland 2013

[23] SNB, Monthly Bulletin of Banking Statistics, August 2012

The provision of financial services is concentrated in a number of urban cantons, giving rise to the three hubs of the Swiss financial centre. The most important of these is the region of Zurich and its neighbouring cantons in central Switzerland, the second-most important is the Lake Geneva region, with Geneva as its centre, and the third is the region of Lugano in Ticino. The table below shows the breakdown of financial intermediaries by canton.

Table 1: Number of financial intermediaries in 2014, by canton

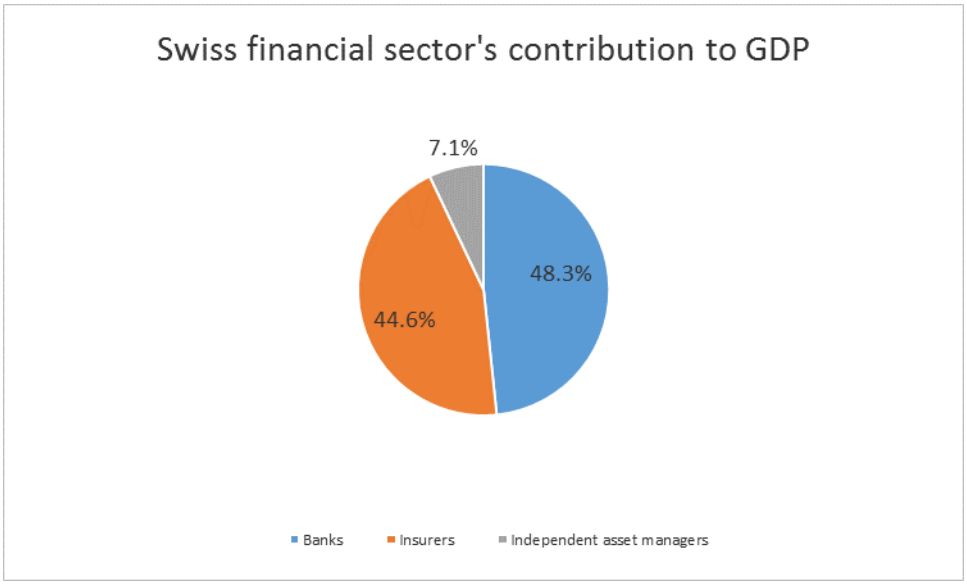
Canton	Banking sector	Non-banking sector[24]	Institutions subject to the Collective Investment Schemes Act	Insurers also active in financial intermediation[25]	Total
Aargau	6	99	15		120
Appenzell (AR)	1	25	3		29
Appenzell (AI)	1	17	1		19
Basel Landschaft	1	51	9	1	62
Basel Stadt	13	166	26	4	209
Bern	25	170	34	2	231
Fribourg	2	76	2		80
Geneva	**64**	**1430**	**78**		**1572**
Glarus	2	18	2		22
Graubünden	1	137	1		139
Jura	1	6	1		8
Lucerne	4	106	16	1	127
Neuchâtel	2	48	9		59
Nidwalden	1	31			32
Obwalden	1	32			33
Schaffhausen	4	28			32
Schwyz	4	190	19		213
Solothurn	6	31	3		40
St. Gallen	16	181	17	1	215
Ticino	**19**	**884**	**34**	**1**	**938**
Thurgau	2	62	10		74
Uri	1	6			7
Valais	3	62	4	1	70
Vaud	**10**	**334**	**53**	**7**	**404**
Zug	**3**	**604**	**35**		**642**
Zurich	**104**	**1689**	**222**	**10**	**2025**
Total	**297[26]**	**6483**	**594**	**28**	**7402**

Source: FINMA

The main branches of the financial sector contributed to GDP as follows:

Figure 2: Swiss financial sector's contribution to GDP in 2014

[24] Including primarily fiduciaries and independent asset managers
[25] Life and non-life insurers that offer mortgages
[26] This figure includes fourteen institutions that ceased operating or went into liquidation in 2014



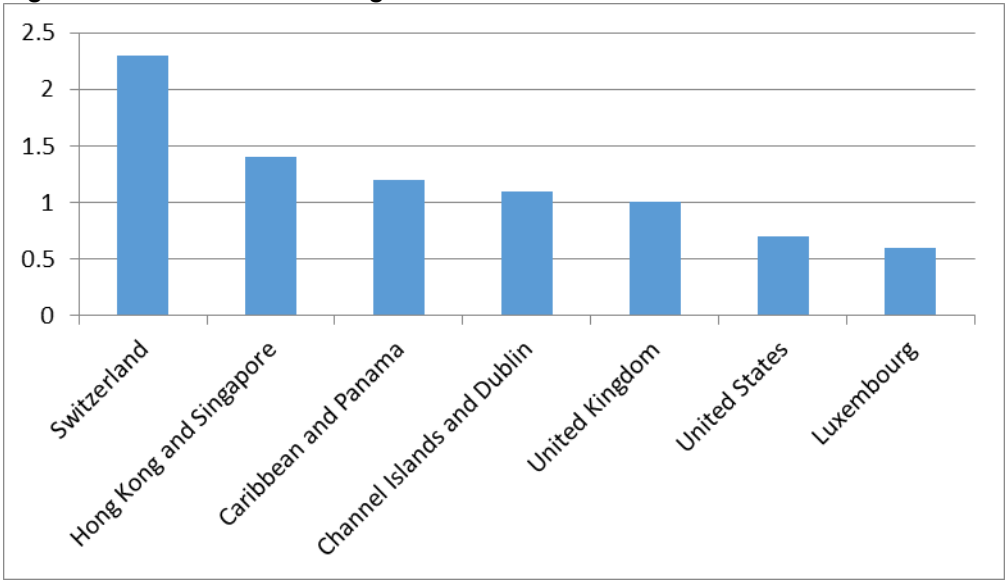
Source: FSO; SECO – Annual GDP and its components, production-based approach; ZHAW

5.1.2 International significance of the Swiss financial centre

At 10.2%, the financial sector's proportion of GDP is comparatively high in Switzerland by international standards (United States: 6.6%; United Kingdom: 8.6%), and is almost as high as that of Singapore (11.2%) but remains significantly lower than that of Luxembourg (25.4%).[27]

The Swiss financial centre is home to a wide range of specialised financial service providers, with one of its strengths being wealth management. For instance, private wealth booked across borders amounts to some USD 2.3 trillion, or 26% of the global offshore wealth management market. By comparison, private wealth booked across borders amounts to a total of USD 1.4 trillion in Hong Kong and Singapore combined, USD 1 trillion in the United Kingdom, USD 0.7 trillion in the United States and USD 0.6 trillion in Luxembourg (see Figure 3).[28]

Figure 3: Assets under management in offshore centres in USD trillion in 2013



Source: The Boston Consulting Group 2014

Furthermore, many cross-border transactions of Swiss financial institutions are undertaken with counterparties based in the EU. The Swiss financial centre is therefore heavily interconnected with other

[27] Grand Duchy of Luxembourg: Statistics Portal (2011); Singapore: Singapore Department of Statistics (2011); United Kingdom: Office for National Statistics (2011); United States: Bureau of Economic Analysis (2011)

[28] The Boston Consulting Group (BCG) 2014, Global Wealth 2014 – Riding a Wave of Growth, p. 10

European financial centres (such as London, Luxembourg and Liechtenstein), as well as with those in the United States and Asia. Over the past five years, the financial centres in Hong Kong and Singapore have continued to grow in line with their GDP growth rates, which has resulted in a sharp rise in private wealth too.

5.2 Political and legal framework for combating financial crime

5.2.1 Federal Council's policy on combating financial crime

Preserving a sound, attractive and efficient financial centre is one of the Federal Council's stated objectives. This objective involves doing everything possible to ensure that the financial centre is not abused for criminal purposes, in particular for money laundering or terrorist financing. Switzerland contributes actively and cooperates in the development of standards on this issue at the international level. It also regularly amends its legislation to take account of new threats and the development of international standards in this field and to enhance its effectiveness. Over the past few decades, Switzerland has been gradually developing a robust and comprehensive system for combating money laundering which combines preventive and repressive measures.

This policy, together with the specific measures adopted as part of it, make a significant contribution to reducing the risks and thus ensuring the integrity of the Swiss financial centre, whether in relation to money laundering, terrorist financing or the taxing of assets. Among these measures, it is worth highlighting the establishment at the institutional level of the CGMF, as mentioned above, as well as the development of regulations on financial crime and the other legal developments in this area. The following sections will summarise these developments, but will not describe them in detail. A separate report by the FATF, which will be drawn up as part of Switzerland's mutual evaluation, will provide a detailed description of the legal regime for combating money laundering and terrorist financing and its connection to risk management, and demonstrate the effectiveness of existing measures.

5.2.2 Regulatory developments in the area of financial crime since 2005

5.2.2.1 Implementation of the FATF recommendations

Switzerland's contribution to defining international standards on financial market integrity, specifically the harmonisation of the rules to combat financial crime, is an important pillar of its strategy to ensure a healthy and flourishing financial centre. For this reason, Switzerland has been actively involved in the FATF's activities ever since it was first established. Following the partial revision of the FATF recommendations in 2003, Switzerland modified its anti-money laundering and terrorist financing regime several times to bring it into line with new FATF requirements. It carried out legislative amendments in 2007, 2009 and 2013 to take account of the criticism raised in the report on Switzerland's mutual evaluation report in 2005 and the 2009 follow-up report, as well as the Egmont Group[29] requirements with regard to the exchange of information between financial intelligence units (FIUs). On 13 December 2013, the Federal Council adopted for the attention of Parliament the dispatch on the draft of the new Federal Act for Implementing the Revised Financial Action Task Force (FATF) Recommendations of 2012. This bill aims to strengthen the effectiveness of the Swiss anti-money laundering and terrorist financing system by completing the implementation of international standards in Switzerland. The bill was approved by Parliament on 12 December 2014.[30] The law will come into force on 1 January 2016, with the exception of the transparency measures in the case of legal entities and bearer shares, which will come into force as early as 1 July 2015.

The law introduces new developments or modifications in eight areas as follows:

- extension of the obligation to enter foundations in the commercial register to now include ecclesiastical and family foundations (amendment to the Swiss Civil Code [CC[31]]);
- improved transparency in the case of legal entities through measures targeting both unlisted companies issuing bearer shares and the identification of the beneficial owners of legal entities. These measures also aim to meet the requirements of the Global Forum on Transparency and Exchange of Information for Tax Purposes (amendment to the CC, the Swiss Code of

[29] Egmont Group is an informal network comprised of 147 member FIUs. Its aim is to promote cooperation between FIUs in the fight against money laundering and terrorist financing, especially in the areas of information exchange and training.

[30] BBl 2014 9465

[31] SR 210

Obligations [CO][32], the Federal Act of 23 June 2006 on Collective Capital Investment Schemes [CISA][33] and the Federal Act of 3 October 2008 on Intermediated Securities [FISA][34]);

- more stringent obligations for financial intermediaries when identifying the beneficial owners of legal entities (amendment to the AMLA);
- extension of the term PEP to include domestic PEPs and PEPs in international organisations and international sports federations, as well as introduction of corresponding risk-based due diligence obligations (amendment to the AMLA);
- introduction of a predicate offence in connection with direct taxation and, in connection with indirect taxation, extension of the existing criminal offence of smuggling in the customs area to other taxes levied by the Confederation (amendment to the SCC and the Federal Act of 22 March 1974 on Administrative Criminal Law [ACLA][35]);
- obligation for traders to involve a financial intermediary or to fulfil due diligence requirements for cash payments in excess of CHF 100,000 for purchases of movable or immovable property (amendment to the AMLA and the Federal Act of 11 April 1889 on Debt Enforcement and Bankruptcy [DEBA][36]);
- increased effectiveness of the system for reporting suspicious activity (amendment to the AMLA); and
- improved implementation of the FATF standard regarding targeted financial sanctions related to terrorism and terrorist financing (amendment to the AMLA).

Work is under way on preparing and revising the implementing ordinances, particularly for the AMLA, and the regulations of self-regulatory organisations (SROs). These implementing ordinances and regulations are expected to come into force at the same time as the corresponding legislative provisions.

5.2.2.2 Developments in the area of bribery

Switzerland is a party to the three main international conventions for combating bribery. On 31 May 2000, it ratified the OECD Convention of 17 December 1997 on Combating Bribery of Foreign Public Officials in International Business Transactions[37]. This was followed by its accession, on 1 July 2006, to the Criminal Law Convention on Corruption of 27 January 1999[38], concluded under the aegis of the Council of Europe. For the purpose of implementing these conventions, Switzerland completely reformed the provisions of the Criminal Code which penalise bribery of national and foreign public officials as well as bribery in the private sector. Finally, on 24 September 2009, Switzerland ratified the United Nations Convention Against Corruption[39], adopted on 31 October 2003, which did not require any amendments to Swiss legislation. Switzerland has been examined as part of the peer review mechanism with regard to the aforementioned international conventions.

Currently, bribery in the private sector is prosecuted on complaint and is covered by the Federal Act of 19 December 1986 on Unfair Competition (UCA)[40]. In response to a recommendation of the Council of Europe's Group of States Against Corruption (GRECO), the Federal Council decided that bribery in the private sector should be prosecuted and punished ex officio in the future, even in cases where it does not result in distortions of competition. The new standard will be incorporated into the Criminal Code. The Federal Council adopted the corresponding dispatch and bill and submitted them to Parliament on 30 April 2014[41].

As a result of the political upheaval in northern Africa, the *Task Force Asset Recovery* was set up in 2011 and is responsible for the restitution of the illegally acquired assets of dictators. Attached to the Directorate of Public International Law (DIL) of the Federal Department of Foreign Affairs (FDFA), it is

[32] SR 220
[33] SR 951.31
[34] SR 957.1
[35] SR 313.0
[36] SR 281.1
[37] SR 0.311.21
[38] SR 0.311.55
[39] SR 0.311.56
[40] SR 241
[41] BBI 2014 3433

tasked with implementing Switzerland's asset recovery policy at the international level. The Federal Act of 1 October 2010 on the Restitution of Assets Obtained Unlawfully by Politically Exposed Persons (RIAA)[42], which came into force in 2011, provides for the freezing and confiscation of assets whenever mutual assistance is unsuccessful due to the state of failure in the country of origin; it is subsidiary to the Federal Act of 20 March 1981 on International Mutual Assistance in Criminal Matters (IMAC)[43]. On 21 May 2014, the Federal Council approved the dispatch for a federal act on unlawfully obtained assets[44], the intention of which is to establish comprehensive provisions for the freezing, confiscation and recovery of dictators' assets and to thus enshrine in law the practices applied by Switzerland in this area to date. The RIAA will be repealed by the entry into force of this act. The key elements of the Swiss asset recovery policy are contained in Switzerland's strategy for the freezing, confiscation and recovery of dictators' assets, which was approved in 2014.

5.2.3 Policy and regulation in the fight against tax evasion at the international level

The outbreak of the financial crisis in 2008 brought with it a clear strengthening of the fight against tax evasion at the international level. Keeping pace with this development, the Federal Council decided in 2009 to adopt the entire standard on the exchange of information upon request in tax matters (Art. 26 of the OECD Model Convention). Since then, the administrative assistance clause in keeping with the OECD standard has been included in a large number of double taxation agreements, and several tax information exchange agreements have also been concluded. Furthermore, the Federal Act of 28 September 2012 on Tax Administrative Assistance (TAAA)[45], which governs the provision of administrative assistance in the tax area, entered into force in 2013.

Collaboration has been strengthened with regard to both bilateral and multilateral international administrative assistance. In 2013, for instance, Switzerland signed the multilateral OECD/Council of Europe Convention on Mutual Administrative Assistance in Tax Matters. It also supported transparency and the exchange of information for tax purposes within the Global Forum, where it is represented in the Steering Group as well as the Peer Review Group. In 2011, a Global Forum report concluded that Switzerland had certainly made enormous progress since 2009 in administrative assistance procedures, but it was still non-compliant or only partially compliant with important conditions necessary for the effective exchange of information. Switzerland proceeded to take additional measures, which involved extending its network of standard-compliant double taxation agreements and tax information exchange agreements, adopting derogations from the rules governing the information of the taxpayers concerned, and increasing transparency with regard to bearer shares.

Switzerland and the EU had already agreed in 2004 to pursue greater collaboration in the tax area. In application of the Agreement on the Taxation of Savings[46], Swiss financial institutions levy, for the country of origin, withholding tax on the savings income of natural persons domiciled in the EU, or, if these persons have given their consent, disclose such income to the country of origin.

In 2014, the FATCA agreement between Switzerland and the United States along with the federal act implementing this agreement also entered into force[47]. The United States' intention with FATCA (Foreign Account Tax Compliance Act) is to tax all of the income of US taxpayers who hold bank accounts abroad in accordance with its tax law. FATCA is a form of unilateral US regulation that is applicable worldwide. It requires foreign financial institutions to forward information on all of the US accounts they manage to the US tax authorities, failing which the United States levies a large withholding tax on US payments made to these institutions or their clients.

Switzerland has also signed withholding tax agreements with the United Kingdom and Austria[48], which have enabled the regularisation of assets not declared in the past and ensure the taxation of all income in the future. These agreements came into force in 2013. Swiss financial institutions levy a lump-sum tax on the existing assets (past) as well as on the capital income and capital gains (future) of their British and Austrian clients and forward it to the tax authorities in the United Kingdom and in

[42] SR 196.1
[43] SR 351.1
[44] BBl 2014 5121
[45] SR 672.5
[46] Agreement of 26 October 2004 between the Swiss Confederation and the European Community providing for measures equivalent to those laid down in Council Directive 2003/48/EC on taxation of savings income in the form of interest payments; SR 0.641.926.81
[47] FATCA Act of 27 September 2013; SR 672.933.6
[48] SR 0.672.936.74; SR 0.672.916.33

Austria via the Federal Tax Administration (FTA). Instead of the withholding tax, British and Austrian clients may also opt to declare their assets and thus pay the tax directly to their country's tax authorities.

Finally, after international discussions on the automatic exchange of information (AEOI) grew in intensity, the Federal Council stated in 2013 that it was willing to actively collaborate, within the OECD, on developing a global AEOI standard designed to guarantee tax compliance. In 2014, Switzerland recognised the new international standard on the automatic exchange of information in tax matters adopted by the OECD and said it was ready to implement the AEOI with partner states, under certain conditions. By way of initial concrete measures, the Federal Council approved negotiation mandates with various partner states on 8 October 2014 (including the EU, USA and Australia) on the adoption of the AEOI and launched the consultation procedure on 14 January 2015 for two bills on the implementation of this standard. On 3 March 2015, Switzerland and Australia signed a joint declaration on the application of the AEOI in tax matters on a reciprocal basis. On 27 May 2015, Switzerland and the EU signed an agreement on the AEOI in tax matters. Finally, on 5 June 2015, the Federal Council submitted to Parliament its dispatches on the OECD/Council of Europe Convention and on the legal basis required for implementing the standard on the AEOI in tax matters. These dispatches are a follow-up to the consultation launched on 14 January 2015.

5.2.4 Developments in the fight against terrorism

On 12 December 2014, Parliament strengthened its anti-terrorism system by banning the terrorist organisations known as al-Qaeda and Islamic State and their associated organisations[49]. Under this new act, which came into force on 1 January 2015, any person within Switzerland who joins one of the targeted groups or organisations, provides it with human or material resources, organises propaganda that promotes it or its objectives, recruits supporters or encourages its activities in any other way is liable to a custodial sentence not exceeding five years or a monetary penalty. The act also includes a provision on confiscation.

The bans supplement the existing system by implementing the international sanctions contained in the relevant Security Council resolutions.

5.2.5 Developments in the fight against cybercrime

Switzerland has recognised the problems both of cybercrime in itself and of its connections with money laundering. Predicate offences to money laundering increasingly consist of property offences committed using computer-based technologies. Attached to the Federal Office of Police (fedpol), the Cybercrime Coordination Unit Switzerland (CYCO) identified, together with federal and cantonal partner authorities, the various modi operandi within the area of cybercrime and classified them according to different phenomena. The knowledge obtained from this has been made available to the offices concerned for the purposes of performing analyses and establishing types of offences in the area of money laundering. In particular, new cybercrime phenomena related to money laundering that are detected by MROS itself or reported to it by financial intermediaries are included in CYCO's typology. This collaboration between CYCO and MROS is facilitated and encouraged by the fact that the two structures are part of the Federal Office of Police (fedpol). In this way, MROS is kept informed at all times of the latest developments and new phenomena observed in respect of cyber offences which potentially constitute predicate offences to money laundering. For its part, CYCO is immediately aware of the latest developments regarding cybercrime related to money laundering. This not only facilitates coordination of the fight against money laundering but also ensures that MROS carries out its analysis and sorting tasks while taking account of the latest developments in the very dynamic area of cybercrime. Furthermore, the constant exchange between MROS and CYCO on the latest modi operandi of cybercriminals as well as the gains in terms of knowledge and skills that ensue also benefit financial intermediaries by keeping them aware at all times of the risks presented by cybercrime and its new approaches. The knowledge obtained on the scale of cybercrime and on its typology make it possible to draw up a national assessment of this phenomenon, or in other words, to gain an overview of cyber offences as potential predicate offences to money laundering and, on that basis, to set priorities and identify the need for action at an early stage.

[49] The Federal Act of 12 December 2014 on the Prohibition of al-Qaeda and Islamic State and Associated Organisations (SR 122)

5.2.6 Other developments in the legal framework concerning the fight against financial crime

Swiss Criminal Code – limitation periods
The limitation periods provided for in Article 97 paragraph 1 letter c of the SCC for serious misdemeanours, i.e. misdemeanours carrying a custodial sentence not exceeding three years, have been increased from seven to ten years (as of 1 January 2014). Money laundering (on its own, Art. 305bis para. 1 of the SCC) is one such misdemeanour. The limitation period for money laundering in more serious cases (Art. 305bis para. 2 of the SCC) remains unchanged (fifteen years).

Swiss Criminal Procedure Code (CrimPC)[50]
The Swiss Criminal Procedure Code was drawn up to increase the effectiveness of criminal prosecution throughout Switzerland. In force since 1 January 2011, the CrimPC unified the procedural rules at the federal and cantonal levels and thus replaced the 26 cantonal procedure codes and the federal procedure code that coexisted until 2011. In particular, Article 24 of the CrimPC provides for federal jurisdiction for the prosecution of certain offences in connection with organised crime, bribery, money laundering and terrorist financing whenever the criminal acts have, to substantial extent, been committed abroad or in several cantons with no single canton being the clear focus of the criminal activity. Moreover, it no longer provides for the sharing of the preliminary proceedings between the prosecutor and the examining judge, but makes the public prosecutor solely responsible for conducting all proceedings, i.e. from the preliminary proceedings to supporting the prosecution. It establishes possibilities for agreement between the defendant and the public prosecutor and strengthens the rights to a proper defence and certain rights of victims.

Federal Act of 6 October 2000 on the Surveillance of Postal and Telecommunications Traffic (SPTA)[51]
Under the existing act, surveillance measures can already be ordered for the purpose of investigating an offence such as money laundering (Art. 269 para. 2 of the CrimPC) and the new act currently being developed does not modify this surveillance. The main objective of the total revision of the SPTA is to enable the surveillance of persons strongly suspected of having committed serious offences while also respecting the basic rights of the persons concerned and adapting surveillance possibilities to the technological developments of recent years. The Federal Council adopted the corresponding dispatch and bill on 27 February 2013 and submitted them to Parliament.[52]

Bill on the VOSTRA criminal records information system
The bill on the VOSTRA criminal records information system provides for the creation of a criminal convictions register for companies in which their convictions and ongoing criminal proceedings will be recorded. In this way, courts will be able to take previous convictions into account when determining sentences for repeated offences. Companies will also be able to present an extract of their entry in the criminal convictions register as evidence of their good reputation in their relations with the authorities or other economic players. The entry of companies in the criminal convictions register will require the development of a new database. On 20 June 2014, the Federal Council adopted the dispatch accompanying the bill on the criminal convictions register and submitted it to Parliament[53].

Bill on Intelligence Service (IntSA)
On 27 November 2009, the Federal Council instructed the DDPS to prepare a new act on the intelligence service. The act will form the overall legal basis for the Federal Intelligence Service (FIS) and will replace the Federal Act of 21 March 1997 on Measures to Safeguard Internal Security (ISA)[54] and the Federal Act of 3 October 2008 on Responsibilities in the Area of the Civilian Intelligence Service (CivISA)[55].

On 19 February 2014, the Federal Council approved the draft of the new act on the intelligence service and the corresponding dispatch for the attention of Parliament.[56] The bill includes provisions on the introduction of new measures on information gathering in the areas of terrorism, espionage, proliferation of nuclear, chemical or biological weapons and attacks on critical infrastructure, as well as on

[50] SR 312.0
[51] SR 780.1
[52] BBl 2013 2483
[53] BBl 2014 5525
[54] SR 120
[55] SR 121
[56] BBl 2014 2029

the protection of Switzerland's essential interests. If the bill is adopted, and provided a referendum is not called, the act could enter into force on 1 January 2016.

5.3 Institutional framework for combating money laundering and terrorist financing

In practice, risk mitigation is ensured primarily by the institutional players that perform their tasks in the areas of the prevention, detection and suppression of money laundering and terrorist financing based on the legal and procedural resources available to them. In particular, these include financial intermediaries, which are the first line of operational defence in the fight against money laundering and terrorist financing, supervisory bodies and authorities, as well as the competent administrative, judicial and criminal prosecution authorities at federal and cantonal level.

The provisions of Articles 29 and 29*a* of the AMLA and Article 30 of the ACLA specifically allow for the exchange of information between public authorities in the form of administrative or mutual legal assistance.

5.3.1 Financial intermediaries

The financial intermediaries category comprises not only banks, insurers, securities dealers, stock exchanges and investment funds (banking sector), but also the non-banking sector and casinos (Art. 2 of the AMLA). Banking sector financial intermediaries are subject to the AMLA, have to obtain authorisation from FINMA before commencing their activity and are directly under FINMA supervision (Art. 3 of the Federal Act of 8 November 1934 on Banks and Savings Banks [BankA][57], Art. 3 and Art. 10 of the Federal Act of 24 March 1995 on Stock Exchanges and Securities Trading [SESTA][58], Art. 4 of the Federal Act of 17 December 2004 on the Oversight of Insurance Companies [IOA][59], Art. 13 of the CISA and Art. 12 of the AMLA).

Financial intermediaries in the para-banking sector that operate on a professional basis are also required to obtain authorisation from FINMA or join an SRO before commencing their activity (Art. 14 of the AMLA). In the non-banking sector, subjection to the AMLA is not linked to specific occupations or fields but rather to the professional practice of financial intermediation, an activity where money laundering and terrorist financing can be encountered. It can thus happen that two people who are in the same field (e.g. two fiduciaries) but perform different activities within that field do not have the same status: one can be subject to the AMLA while the other is not.

The AMLA gives a non-exhaustive list of financial intermediation activities that are subject to the Act. Moreover, the AMLA contains a general clause which states that financial intermediaries are persons who, on a professional basis, accept or hold on deposit assets belonging to others or who assist in the investment or transfer of such assets (Art. 2 para. 3 of the AMLA). The Federal Council Ordinance of 18 November 2009 on the Professional Practice of Financial Intermediation (PFIO)[60] sets out the criteria for being considered a financial intermediary pursuant to Article 2 paragraph 3 of the AMLA, specifically defining the requirements regarding the professional nature of financial intermediation.

In short, those subject to the AMLA in the non-banking sector are asset managers, credit institutions, particularly those offering financial leasing, commodities brokers (in the case of stock exchange trading for third parties), traders in banknotes, coins and precious metals, bureaux de change, money transmitters, investment fund distributors and representatives, securities dealers not subject to the SESTA, formal and actual executive organs of non-operative companies established under the laws of Switzerland or of a foreign country, as well as lawyers and notaries performing financial intermediation in addition to their conventional activities.

Anyone who goes from performing an activity on a non-professional to a professional basis has two months to join an SRO or obtain authorisation from FINMA. The financial intermediary is prohibited from establishing new business relations until an SRO has been joined or authorisation has been granted (Art. 11 of the PFIO).

[57] SR 952.0
[58] SR 954.1
[59] SR 961.01
[60] SR 955.071

Finally, casinos have to obtain a licence (Art. 10 ff. of the Federal Act of 18 December 1998 on Gambling and Gambling Casinos [GamblA][61]) and are subject to the direct supervision of the Federal Gaming Board (FGB; Art. 12 of the AMLA).

5.3.2 Supervisory bodies and authorities

5.3.2.1 Swiss Financial Market Supervisory Authority (FINMA)

The Federal Act of 22 June 2007 on Federal Financial Market Supervision (FINMASA)[62] came into effect on 1 January 2009. This Act aims to place the state supervision of banks, insurers, stock exchanges, securities dealers and other financial intermediaries under the aegis of a single authority in Switzerland. The three supervisory authorities which previously existed in these areas, i.e. the Swiss Federal Banking Commission (SFBC), the Federal Office of Private Insurance (FOPI) and the Anti-Money Laundering Control Authority (AMLCA), were thus merged to form the Swiss Financial Market Supervisory Authority (FINMA). The primary aim of this new institutional organisation is to strengthen financial market supervision.

FINMA is structured as an institution under public law. It has functional, institutional and financial independence, as well as a modern management structure with a Board of Directors, Executive Board and external auditor. To counterbalance FINMA's independence, it has been made accountable to and is subject to the overall political supervision of the Federal Assembly.

In addition to organisational issues regarding FINMA as an institution, the FINMASA also sets out principles governing financial market regulation, liability rules and harmonised supervisory instruments and sanctions. The FINMASA therefore functions as an umbrella law for the other laws governing financial market supervision. Nevertheless, the legal mandate conferred on the supervisory authority remains unchanged and takes account of the specific features of the various areas of supervision. Banks, securities dealers, stock exchanges, insurers and collective investment schemes must thus continue to satisfy the applicable legal criteria. The self-regulation system provided for under the AMLA and the SESTA is likewise maintained.

As a result of this new organisation, the former anti-money laundering ordinances of the SFBC, FOPI and AMLCA became anti-money laundering ordinances of FINMA from 1 January 2009, before eventually being harmonised and integrated into the FINMA Anti-Money Laundering Ordinance of 8 December 2010 (AMLO-FINMA)[63], which came into effect on 1 January 2011. The AMLO-FINMA had to be revised after the Federal Act for Implementing the Revised FATF Recommendations of 2012 was adopted by Parliament on 12 December 2014. A hearing on the proposed revision of the ordinance was held from 11 February to 7 April 2015. It is planned for the revised ordinance to come into force on 1 January 2016.

5.3.2.2 Federal Gaming Board (FGB)

An independent federal administrative authority, the FGB is administratively affiliated to the Federal Department of Justice and Police (FDJP). It has a permanent Secretariat, which is currently comprised of around 40 people. The FGB began its work when the GamblA took effect, i.e. on 1 April 2000. The FGB is tasked with enforcing the legislation on casinos, including the provisions to combat money laundering and terrorist financing, granting licences and seeing to the operation and taxation of casinos.

The FGB directly supervises casinos and ensures that the legal provisions are complied with. Concerning compliance with the provisions to combat money laundering and terrorist financing, the FGB performs the following tasks:

- Verification of all changes to internal AMLA directives and AMLA procedures made by casinos (the FGB may prohibit a change)
- Checking of casino staff members' AMLA training
- Onsite verification of the documentation prepared by casinos on their clients (client files), particularly with regard to their duty to verify the identity of clients, determine the beneficial

[61] SR 935.52
[62] SR 965.1
[63] SR 955.033.0

owner, register transactions and perform specific clarifications, as well as their duty to report to MROS
- Analysis of annual reports on the implementation of AMLA measures by casinos
- Checking of all changes concerning shareholders (with a minimum stake of 5%), participation holders and major business partners (the FGB has to give its approval before changes are made)
- Checking of all changes concerning casino management members and persons holding key positions (e.g. AMLA officers)
- Periodic review of the good reputation of casino employees
- Close monitoring of the financial situation of casinos

In the event of an irregularity or violation of the GamblA, the FGB orders the measures necessary to rectify the irregularity or restore legal order. During the investigation, it may take provisional measures, namely suspend the licence (Art. 50 of the GamblA). In the case of an infringement of the licence or a final judgment which generates a profit, an administrative fine of up to three times this profit may be imposed against the guilty casino. If no profit was generated or it cannot be ascertained or estimated, the fine can be up to 20% of the previous year's gaming turnover (Art. 51 of the GamblA).

The FGB withdraws the licence if certain essential conditions for granting it are no longer met, if the casino seriously or repeatedly violates the GamblA, its implementing provisions or the licence, or if the casino uses the licence for unlawful purposes (Art. 19 paras. 1 and 2 of the GamblA). In less serious cases, the FGB can suspend the licence, restrict it or subject it to additional charges and conditions (Art. 19 para. 3 of the GamblA).

Anyone who deliberately fails to meet the AMLA due diligence requirements provided for in the GamblA is guilty of a misdemeanour and liable to imprisonment for no more than one year or a fine not exceeding CHF 1 million. In serious cases, the penalty is a period of penal servitude not exceeding five years or at least one year of imprisonment. In the event of negligence, the penalty is a fine not exceeding CHF 500,000 (Art. 55 of the GamblA).

The FGB thus has a broad and dissuasive range of sanctions that can be applied in a differentiated manner depending on the offences and breaches committed by a casino.

5.3.2.3 Self-regulatory organisations (SROs)

With regard to combating money laundering and terrorist financing, the AMLA makes provision not only for supervision performed directly by FINMA, but also the possibility for certain financial intermediaries to be supervised by an SRO. SROs are supervisory bodies in keeping with the definition given in the glossary that accompanies the FATF recommendations. Their task consists in drawing up regulations that set out precisely how compliance is to be achieved with the obligations arising from the AMLA (Art. 24 ff. of the AMLA). They also have to check that affiliated financial intermediaries fulfil their obligations (Art. 25 para. 3 letter b of the AMLA) and impose appropriate penalties if this is not the case (Art. 25 para. 3 letter c of the AMLA). SROs themselves are subject to supervision by FINMA. FINMA is thus responsible for recognising SROs or withdrawing such recognition, approving the regulations issued by them and ensuring that they enforce them (Art. 18 para. 1 letters a to d of the AMLA). In practice, FINMA performs all audits onsite itself, with the exception of the SRO of the Swiss Bar Association and of the Swiss Notary Association.

FINMA actively and directly supervises recognised SROs. Depending on their membership structure, organisation and supervision policy, FINMA draws up risk profiles for the SROs and assigns them to various risk categories. An SRO's risk category determines the intensity and frequency of the supervisory tools applied to it. FINMA recognises an SRO subject to certain conditions being met, and it is subject to supervision by FINMA from the date on which it is recognised. The supervisory tools include periodic onsite supervisory reviews, regular bilateral supervisory consultations and analysis of SROs' annual reports. Once a year, each SRO receives an assessment letter detailing its weaknesses and the action that needs to be taken. FINMA also organises meetings with all SROs twice a year as a forum for discussing general challenges in the operational implementation of the AMLA. At present, 11 SROs supervise approximately 6,200 financial intermediaries operating essentially as asset managers, fiduciaries, payment service providers, lending and leasing businesses, and bureaux de change.

5.3.3 Federal authorities involved in combating money laundering and terrorist financing

5.3.3.1 Federal Department of Finance (FDF)

The FDF plans and executes Federal Council decisions on resources, finances, personnel, buildings and IT. Its tasks are directly related to the effectiveness of the welfare state and Switzerland as a business location. The FDF offices involved in combating money laundering and terrorist financing are the State Secretariat for International Financial Matters (SIF), the Federal Tax Administration (FTA), the Federal Customs Administration (FCA) and Legal Services within the department's General Secretariat.

State Secretariat for International Financial Matters (SIF). Created by the Federal Council on 1 March 2010, SIF includes certain divisions of the Federal Finance Administration (FFA), primarily the Monetary Affairs and International Finance Division, and the FTA's former International Division. SIF is responsible for the coordination and strategic management of international financial, monetary and tax matters, especially in the area of combating money laundering and terrorist financing (see CGMF). It seeks to strengthen Switzerland's international position with regard to financial and tax matters. It defends Switzerland's interests in international financial and tax matters, and leads the Swiss delegation within the framework of international negotiations in these areas. The State Secretariat is also tasked with safeguarding Switzerland's interests in the International Monetary Fund and in the OECD's Financial Stability Board, as well as with actively participating in international efforts to combat financial crime, including within the scope of the FATF. Moreover, it is responsible for analysing developments in the financial markets in Switzerland and abroad, and further developing legislation applicable to the financial sector.

Federal Customs Administration (FCA). The FCA is essentially charged with performing security and tax-related tasks at the border. Its two operating units are the Border Guard and Civil Customs. The FCA has its own investigative and prosecuting body comprised of members from the two operating units who have special training focused on investigative techniques and criminal legislation. Concerning anti-money laundering, the FCA has expertise in the cross-border transfer of cash. Moreover, the FCA is competent to prosecute certain customs offences, primarily associated with indirect taxation, given that they are considered predicate offences to money laundering under the legislation.

Federal Tax Administration (FTA). The FTA is the Confederation's competence centre for tax matters. Together with its partners, it makes an important contribution to the financing for public tasks. Its field of activity covers value added tax, direct federal tax, withholding tax, stamp duty, casino tax and military service exemption tax.

FDF General Secretariat (GS-FDF). Legal Services within the GS-FDF prosecutes and punishes certain violations of the criminal provisions of the FINMASA and the AMLA, primarily violation of the duty of disclosure (Art. 37 of the AMLA), and other financial market laws such as the SESTA and the BankA. It initiates administrative criminal proceedings in the event of a criminal complaint or if it is aware by other means that there are sufficient grounds for suspecting that an offence was committed in its area of responsibility. Most of the criminal complaints are filed by FINMA.

5.3.3.2 Federal Department of Justice and Police (FDJP)

In the Federal Department of Justice and Police, the Federal Office of Justice (FOJ) and the Federal Office of Police (fedpol) are in charge of issues regarding the prevention, detection and suppression of money laundering and terrorist financing. Within fedpol, the Money Laundering Reporting Office Switzerland (MROS) and the Federal Criminal Police (FCP) are particularly worthy of mention.

FOJ – Criminal Law Division. The FOJ's Criminal Law Division is responsible for preparing criminal law and law of criminal procedure legislation, and seeing it through. Furthermore, it contributes to the work of international organisations and working groups that deal with criminal law matters. The FOJ's *Division for International Legal Assistance* primarily sees to mutual legal assistance in criminal matters. Its main assignments include general (residual) responsibility with regard to mutual assistance in civil, criminal and even administrative matters, and it has the authority to negotiate international agreements in these areas. The division is divided into the following units:

1) Mutual Assistance Unit I: Seizure and Handover of Assets
2) Mutual Assistance Unit II: Obtaining Evidence and Service of Documents

3) Extraditions Unit
4) International Treaties Unit

Federal Commercial Registry Office (FCRO). The FOJ is also responsible for legislative affairs concerning company law. Moreover, it has a certain amount of authority with regard to the application of the law, particularly in the area of the commercial register. The competent unit within the FOJ is the FCRO. The commercial register is a database maintained by the state. It is public and contains all important facts for legal entities pursuing an economic activity. It ensures the security and transparency of legal transactions. It contains all data that has to be published by law, particularly the identity of the responsible bodies and authorised representatives. Depending on the legal form, all of the partners or members are listed (general partnership, limited partnership, limited liability company).

The cantons are tasked with organising and maintaining the commercial register. The competent cantonal offices verify the data supplied before registering it. The FCRO performs high-level supervision tasks. It is responsible for approving entries in the cantonal registers and seeing to publication in the Swiss Official Gazette of Commerce (SOGC). It also manages the Central Business Names Index, Zefix, which contains the entries for all companies registered in Switzerland, accompanied by the main identification details. Zefix is available online (www.zefix.ch) and has links to the cantonal commercial registries.

Federal Office of Police (fedpol). Fedpol's tasks include criminal investigations, security duties and administrative policing. It also coordinates certain police tasks and provides support to its federal and cantonal partners. From a police standpoint, special units of the Federal Police are responsible for money laundering and terrorist financing cases.

Federal Criminal Police (FCP). The FCP conducts police investigations under the leadership of the Office of the Attorney General of Switzerland (OAG). These are characterised by their great complexity and their international and interdisciplinary nature. They include matters related to terrorist activity and terrorist financing, economic crime, organised crime, state security and mutual assistance. The FCP's specialist units prepare targeted analytical reports on selected topics and regularly analyse money laundering convictions in Switzerland. The office's international tasks are performed by the International Police Co-Operation Main Division.

Money Laundering Reporting Office Switzerland (MROS). MROS receives and analyses the suspicious activity reports transmitted by financial intermediaries. MROS thus functions as a relay and filter between financial intermediaries and law enforcement agencies in Switzerland, forwarding the suspicious activity reports it receives to them if it deems this necessary after in-depth analysis. Administratively attached to fedpol, MROS plays the role of national FIU at the international level and as such is a member of the Egmont Group. As a member of this group, MROS can quickly exchange financial information directly with other FIUs in accordance with the conditions set out in the AMLA. Furthermore, it is required to operate a database of all suspicious activity reports received. Consequently, MROS has a comprehensive database and a body of information and statistics that enable it to perform analyses and inform other competent authorities, financial intermediaries and the public about threats and their development. Similarly, MROS uses information which has been rendered anonymous to raise awareness and train financial intermediaries, with which it maintains relationships of trust.

5.3.3.3 Federal Department of Home Affairs (FDHA)

The competent units for combating money laundering and terrorist financing within the FDHA are the General Secretariat, with its Legal and Supervision of Foundations Division, which supervises so-called classical foundations, and the Occupational Pension Supervisory Commission (OPSC), tasked with the supervision of cantonal and regional supervisory authorities for occupational pension foundations.

5.3.3.4 Federal Department of Foreign Affairs (FDFA)

The FDFA assists the offices responsible for regulation, supervision and criminal prosecution, and works together with them to ensure a coherent policy for combating money laundering and terrorist financing both in Switzerland and internationally. The organisational units at head office and the network of Swiss embassies are involved. With over 100 representations around the world, this network ensures contact and the flow of information between authorities with regard to the detection, prevention and suppression of money laundering and terrorist financing.

5.3.3.5 Federal Department of Economic Affairs, Education and Research (EAER)

Within the EAER, the State Secretariat for Economic Affairs (SECO) is responsible for implementing international sanctions, including the financial sanction measures imposed on al-Qaeda and the Taliban provided for by resolution 1267 (1999) and subsequent resolutions adopted by the Security Council as well as those associated with preventing the financing of proliferation (resolutions 1718, 1737 and subsequent resolutions).

5.3.3.6 Federal Department of Defence, Civil Protection and Sport (DDPS)

Attached to the DDPS, the Federal Intelligence Service (FIS) keeps a close eye on strategic developments and threats, compiles situation assessments and issues alerts and warnings in the event of emerging crises or unusual developments. It provides the appropriate authorities with information and findings which are relevant for safeguarding the internal and external security of Switzerland and its citizens as well as for enforcing laws and ensuring compliance with international obligations.

The legal basis for the FIS is formed primarily by the ISA, which tasks the federal government, and specifically the FIS, with the following key functions in relation to internal security: implementation of preventive measures for detecting early on and combating threats posed by terrorism, illegal intelligence, violent extremism and proliferation. Moreover, within the framework of the fight against terrorism, the FIS implements measures for the early detection and prevention of terrorist financing in compliance with the applicable legal basis and with the help of the resources available to it for this purpose. Finally, it collaborates closely with the other federal and cantonal units involved, as well as with foreign authorities responsible for similar tasks.

5.3.3.7 Office of the Attorney General of Switzerland (OAG)

The OAG is first and foremost the Confederation's investigation and prosecution authority. It has the authority to prosecute criminal acts which fall under federal jurisdiction. The OAG is the Swiss criminal prosecution authority in the event of money laundering or terrorist financing offences discovered in Switzerland that to a substantial extent were committed abroad or were committed in several cantons with no single canton being the clear focus of the criminal activity (Art. 24 of the CrimPC). The OAG's headquarters are in Bern. It also has branch offices in Lausanne, Zurich and Lugano, which are charged with the prosecution of offences in their respective linguistic region.

The OAG defined a new strategy in 2014 to increase the effectiveness of anti-money laundering investigations: a unit (Centralised Processing of Suspected Money Laundering Reports) comprised of prosecutors, legal experts, financial analysts and a secretariat, representing the three Swiss languages, systematically analyses all MROS suspicious activity reports as well as money laundering complaints and accusations. This unit's mission is to deal with the suspected money laundering reports submitted to it in a uniform and optimal manner and to assign resources to the investigators according to the priorities identified.

5.3.4 Cantonal authorities involved in combating money laundering and terrorist financing

5.3.4.1 Cantonal police forces

Switzerland's federalism is also reflected in its police structures. The cantonal and communal police forces are responsible for maintaining public order and security on their territory. In principle, the 26 cantons also have sovereignty for police matters and jurisdiction, and they are responsible for recruiting, training and equipping their police forces. Consequently, Switzerland has numerous police organisations that are regulated at local level: aside from the cantonal police forces, around a hundred cities, towns and larger communes have their own local police force.

5.3.4.2 Cantonal justice and police departments

The cantonal prosecution authorities are responsible for prosecuting money laundering and terrorist financing offences when the conditions for assigning authority to the Confederation are not met. Against this backdrop, the cantons have a specific institutional body for preventing and coordinating the fight against organised crime and economic crime. The Conference of Cantonal Justice and Police Directors (CCJPD) is tasked with this through its Commission for Organised Crime and Economic Crime, which is comprised of members of cantonal governments and experienced prosecutors with

management functions, the Attorney General of Switzerland, a representative of the Federal Criminal Court and a representative of fedpol. In the operational area of prosecution, the cantons are supported by numerous directives issued by this Commission to ensure uniform and efficient practices (e.g. the procedure for seized property, standard timeframes for banks in the case of decisions to publish documents by the prosecution authorities, etc.). The Commission for Organised Crime and Economic Crime provides the cantons in particular with an up-to-date list of lawyers specialised in the area and thereby contributes to speedy coordination of the various procedures.

5.3.5 Commissions and groups specialised in combating money laundering, terrorist financing and organised crime

The CGMF mentioned in the introduction is the main group specialised in combating money laundering and terrorist financing. The following groups are also worthy of mention in this chapter:

Terrorism interdepartmental working group. The FDFA (Directorate of Public International Law, DIL) leads the interdepartmental working group on terrorism (IDWG on terrorism), which brings together the various units within the Federal Administration responsible for terrorism-related matters. It is headed by the Swiss Counter-Terrorism Coordinator. The two key tasks of this group are the coordination of terrorism-related topics within the Federal Administration and information on the activities of the main international counter-terrorism organisations and institutions.

Assets of politically exposed persons (PEPs) interdepartmental working group. The FDFA regularly chairs an interdepartmental meeting on foreign PEPs' assets in Switzerland proven or suspected to be of suspicious origin. The group serves primarily as an early warning platform, particularly through the external network. It thereby offers the Federal Administration's various offices the possibility of exchanging financial information in a bid to ensure better coordination of their efforts to combat abuse of Switzerland's financial centre and find solutions for the problem of the restitution of illicitly obtained assets. Switzerland's strategy in relation to the freezing, confiscation and restitution of illicitly acquired assets of politically exposed persons (asset recovery) was developed within the framework of this group.

Interdepartmental working group on combating corruption (IDWG on combating corruption). The IDWG on combating corruption was set up following a Federal Council decision of 19 December 2008 based on the recommendations made by GRECO. This IDWG is chaired by the FDFA. Its mandate is to work towards preventing corruption. Its primary task consists in developing concerted national strategies and Switzerland's stances on international anti-corruption topics, particularly within the framework of the implementation of the three international conventions for combating corruption ratified by Switzerland (see section 5.2.2.2). The IDWG not only includes representatives of the Federal Administration offices concerned (FOJ, SECO, DIL, Federal Office of Personnel, armasuisse, etc.) and the OAG, it also actively involves representatives of the private sector (trade associations), the cantons, cities and civil society (think tanks, NGOs, academic institutions). The IDWG holds plenary meetings twice per year, while its core group meets every two months. As part of its mandate, the IDWG organises thematic workshops on topics such as transparency regarding the financing of political parties, commodity trading and corruption and corporate responsibility. Moreover, it takes care of awareness raising and training for Swiss diplomats abroad, directors of Swiss export promotion agencies and employees of the Federal Administration and SMEs with regard to preventing corruption. Every four years, it submits a report to the Federal Council on the main challenges in Switzerland and internationally in the fight against corruption and makes recommendations for the Federal Council on the measures to be taken in this area.

6 General analysis of the threat of money laundering and terrorist financing

6.1 Context and potential threat

It is difficult to say precisely how much capital of criminal origin is injected into the normal economic cycle worldwide each year. The most cautious experts estimate that the proportion is 2% to 5% of global gross domestic product per year, with most of the assets destined to be laundered through the financial sector in particular[64]. Although it is also difficult to say whether the proportion of capital laundered worldwide is possibly increasing more quickly than global GDP, recent analyses suggest an upward trend in the volume of capital of criminal origin channelled into the financial sectors of 20

[64] IMF 1996, 1998, 2001; UNODC 2011; Schneider 2012

OECD member countries, with the proportion nearing an average of 2% of GDP per year and reaching 3.5% to 4% for certain countries[65]. Against the backdrop of this upward trend, money laundering associated with multi-faceted forms of economic crime is especially significant, primarily criminal activity constituting various types of fraud and online fraud in particular[66]. For this emerging form of crime, a financial centre's various sectors serve above all as channels for transmitting the profits arising from this criminal activity. At the same time, however, the financial sector offers sector-specific possibilities for economic crimes such as investment scams, stock price manipulation and insider trading.

Money laundering and terrorist financing are a form of financial crime that is developing with the growing internationalisation of economic and financial transactions. Technological progress is favouring this development, particularly advances in terms of communication and the internet that facilitate capital mobility and thus give rise to new criminal opportunities for money laundering and terrorist financing, some of which are even beyond or on the fringes of financial intermediation. Consequently, it is obvious that there is a worldwide rise in the number of crimes leading to money laundering and terrorist financing activity involving several jurisdictions at the same time. This means that the effectiveness of efforts to combat money laundering and terrorist financing depends more than ever before on the quality of cooperation between the jurisdictions concerned and the state's ability to adapt its regulations according to the emerging threats with a transnational biais, making increasing use of new technologies. Against this backdrop and given the significance of its largely integrated and global financial sector, Switzerland is facing a growing potential risk, thereby confirming its long-term exposure to the risks of money laundering and terrorist financing such as the money laundering risks associated with drug trafficking as well as the emerging threat of money laundering linked to cybercrime. Nevertheless, because of the significance of the financial sector and the high degree of internationalisation, financial intermediaries in Switzerland have gained extensive experience in combating money laundering and terrorist financing and therefore have the knowledge necessary to combat these forms of crime effectively.

6.2 Money laundering

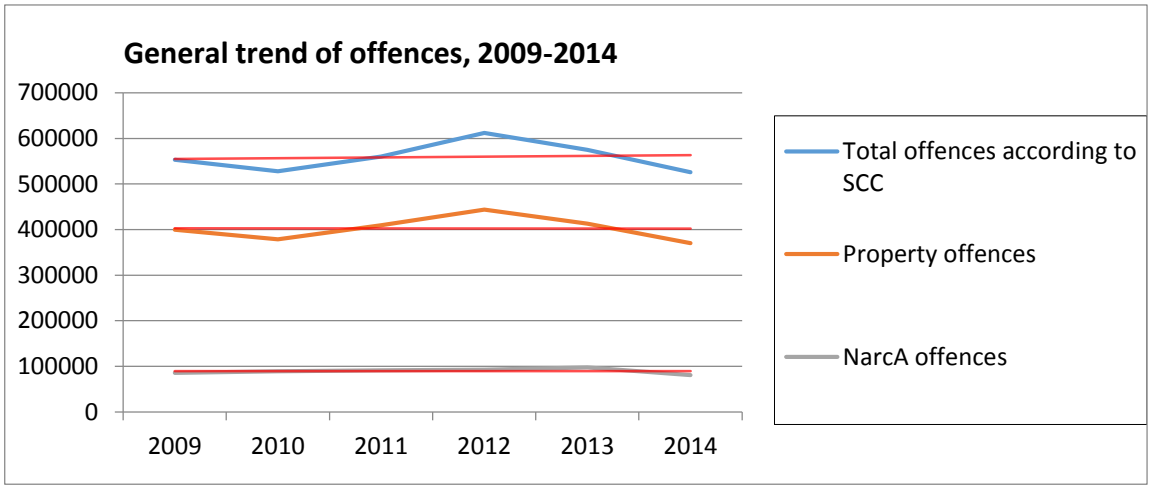
6.2.1 Significance and development of the potential threat

The trend regarding the amount of assets generated through crimes committed domestically and abroad gives a more precise idea of the extent of the potential threat as determined by the context. At the same time, the qualification and evolution of the types of offences make it possible to get a more exact picture of the real threat, identifying the offences for which money laundering is probably carried out.

Since 2004, Switzerland has gradually moved from a particularly low crime rate and stabilised at a rate similar to that of most Western European countries according to police statistics and national victimisation surveys[67]. Overall, the crime rate has risen only slightly since the 2009 consolidation of crime statistics in Switzerland, particularly with regard to fraudulent property offences such as scams and misappropriation, as well as offences associated with drug trafficking[68]. Switzerland's crime rate nevertheless remains low by international standards.

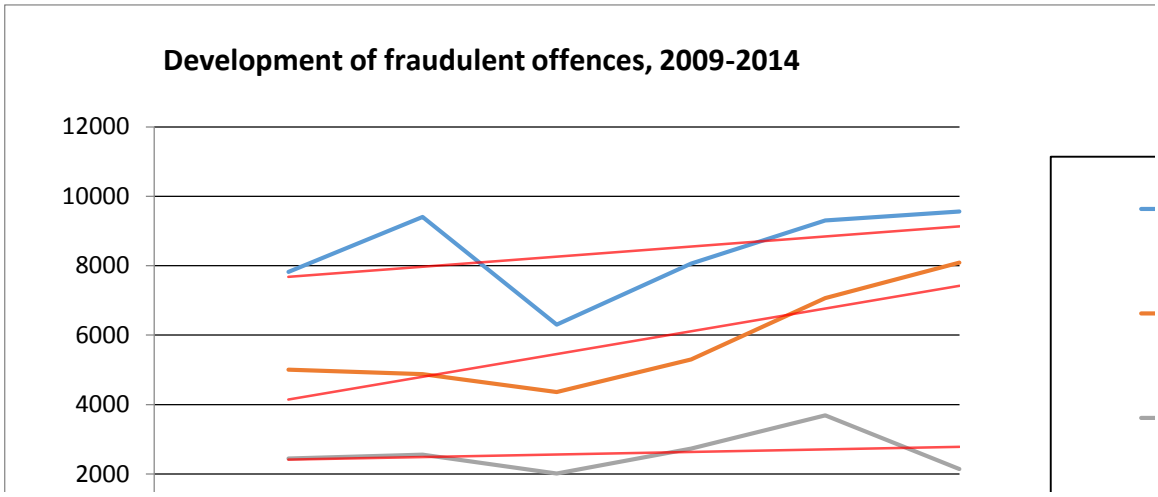
Figure 4: General trend of crimes reported to the police, 2009-2014

[65] Schneider 2010
[66] Unger 2007; Global Money Laundering and Terrorist Financing Threat Assessment, FATF 2010
[67] Killias et al. 2011
[68] Police Crime Statistics (PCS) 2013



Source: FSO, Police Crime Statistics (PCS), 2009-2014

Figure 5: Trend of fraudulent crimes reported to the police and money laundering reports, 2009-2014



Source: FSO, Police Crime Statistics (PCS), 2009-2014

These statistics show a slight increase in absolute terms in the assets derived from felonies committed in Switzerland that are put back into circulation, primarily fraudulent property offences such as scams and misappropriation, and offences against the NarcA (Figures 4 and 5).

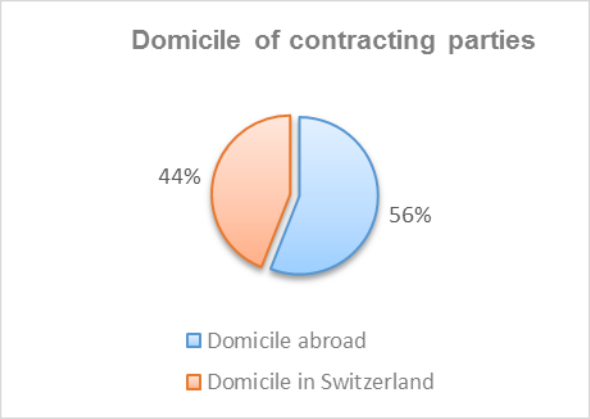
In parallel with the general increase in the amount of assets of criminal origin put into circulation worldwide, recent estimates suggest that the volume of capital of criminal origin injected from abroad into the financial sectors of 20 OECD member countries is rising[69]. On this basis and in view of its high degree of internationalisation, it can be expected that assets of criminal origin from foreign jurisdictions will become increasingly significant for the Swiss financial sector.

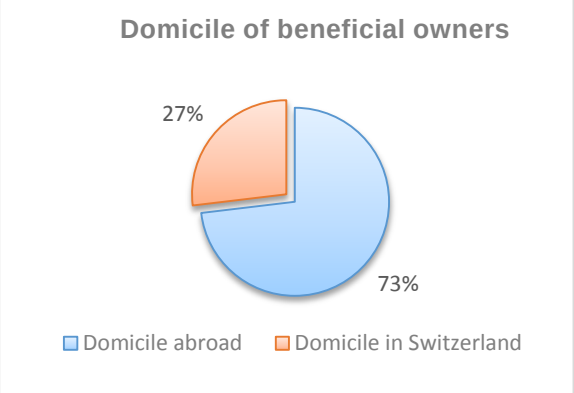
In the absence of money laundering conviction statistics that would make it possible to differentiate between predicate offences to money laundering committed in Switzerland and those committed abroad, it is difficult to determine both the trend and the proportion of assets in Switzerland generated through foreign crimes. Nevertheless, an analysis of the suspicious activity reports for the past decade based on the contracting party's place of domicile suggests that, in the case of Switzerland, most (56%) of the predicate offences to money laundering are committed abroad or that the resources for them (in the sense of preparatory actions) are mobilised abroad (Figure 6). By way of comparison, Singapore's national risk assessment states that foreign predicate offences constitute 34% of all money laundering convictions[70]. An analysis of suspicious activity reports based on the place of domicile of the beneficial owners (BOs) of the business relationships reported to MROS between 2004

[69] Schneider 2010
[70] Singapore National Money Laundering and Terrorist Financing Risk Assessment Report 2013

and 2014 points to an even greater proportion of 73% of predicate offences were committed abroad (Figure 7).

Figures 6 and 7: Domicile of contracting parities and beneficial owners involved in suspicious activity reports submitted to MROS between 2004 and 2014

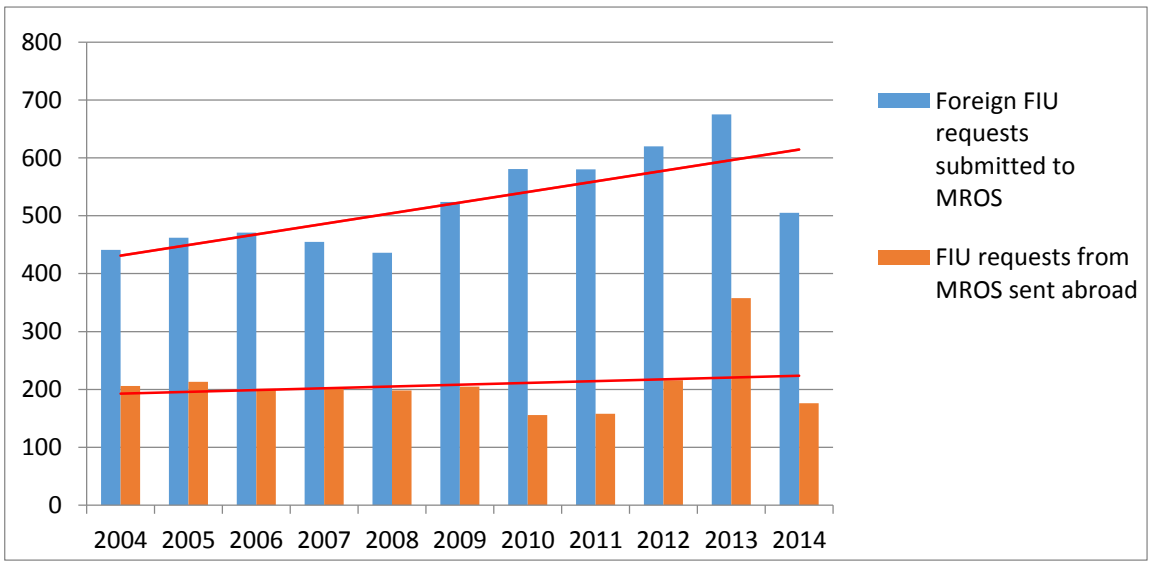




Source: MROS[71]

Beyond the effect of greater international cooperation over the past decade, the assumption that a larger proportion of the assets of criminal origin injected into the Swiss financial circuit is derived from foreign felonies can also be supported by the growing number of requests for financial information submitted to Switzerland by foreign FIUs that are part of the Egmont Group between 2004 and 2014 (Figure 8).

Figure 8: Trend of international exchanges of financial information between MROS and other Financial Intelligence Units (FIUs)

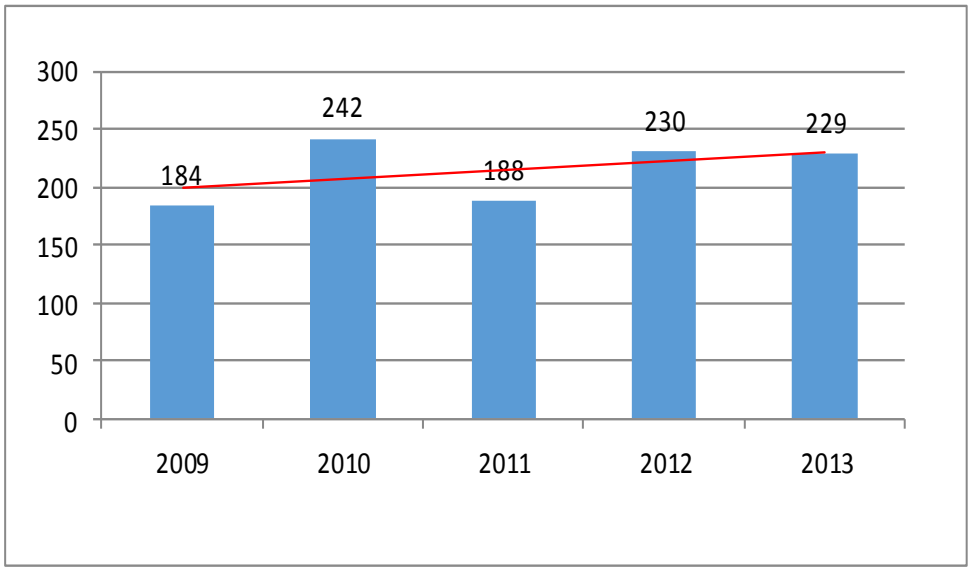


Switzerland's financial sector stands out for the amount of assets derived from foreign felonies or felonies based on foreign resources and support structures relative to the assets derived from felonies committed in Switzerland (Figures 6, 7, 8).

Supporting a growing potential threat, an investigation of the real threat from the specific offence of money laundering in Switzerland, i.e. the development of the number of convictions in accordance with Article 305bis and 305ter paragraph 1 of the SCC, also shows an upward trend since 2009. In parallel, convictions for a lack of due care in accordance with Article 305ter paragraph 1 of the SCC have stabilised at a very low level compared with the money laundering convictions in accordance with Article 305bis paragraph 1 of the SCC (Figure 9).

[71] The figures and tables without a specific source are based on data gathered by MROS

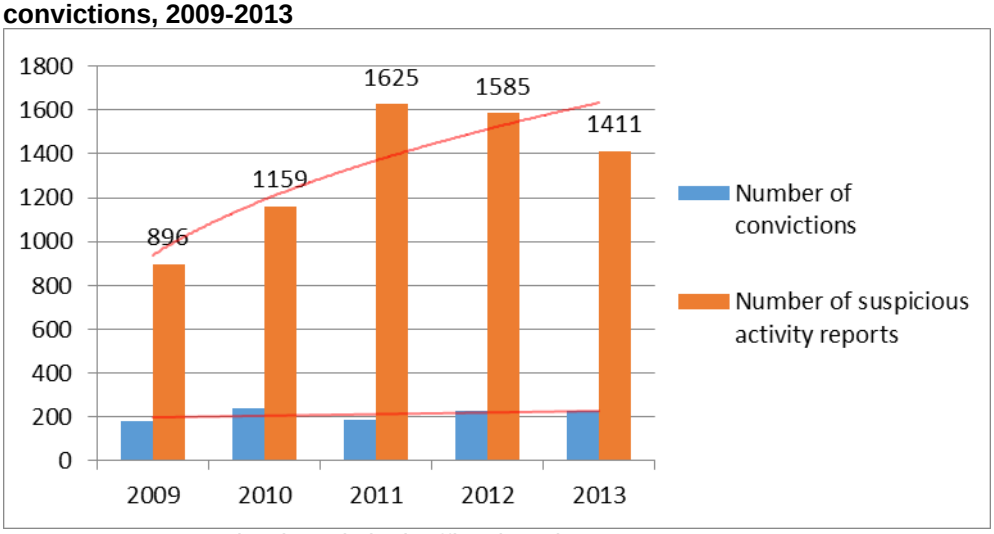
Figure 9: Trend of the number of money laundering convictions in accordance with Article 305bis of the SCC, 2009-2013



Source: FSO

The trend towards a rise in the real threat suggested by the growing number of money laundering convictions in Switzerland is borne out by the proportionally greater increase in suspicious activity reports submitted to MROS relative to the number of convictions for the same period. Against this backdrop, it is worth noting that the longer-term increase in suspicious activity reports is accompanied by a proportional rise in the amounts involved. This proportionality points to a real increase in the long-term threat that goes beyond the scope of the succession of legislative and regulatory amendments aimed at strengthening the system (Figure 10).

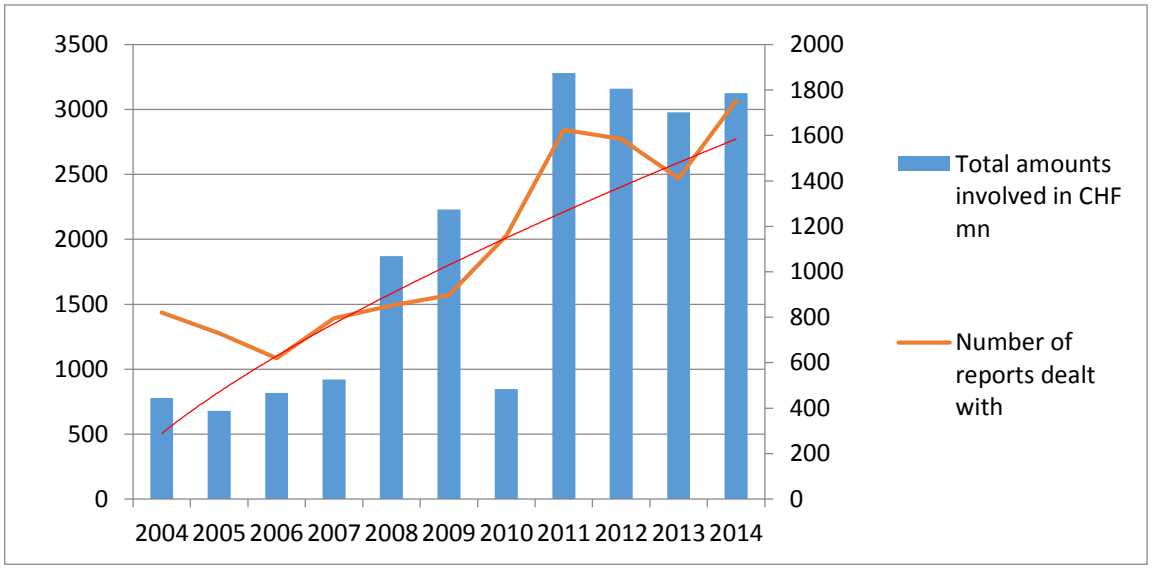
Figure 10: Comparative trend of number of suspicious activity reports and money laundering convictions, 2009-2013



Source: MROS, Federal Statistical Office (FSO)

At the same time, the analysis shows the effect of the legislative adjustments linked to the implementation of the FATF recommendations and the measures taken within the framework of the events associated with the Arab Spring. On this basis, it can be expected that the recent legislative amendments will also lead initially to a greater increase in the number of suspicious activity reports submitted to MROS and then the number will stabilise at a higher level.

Figure 11: Comparative trend of number of suspicious activity reports and total amounts involved per year in CHF mn, 2004-2014



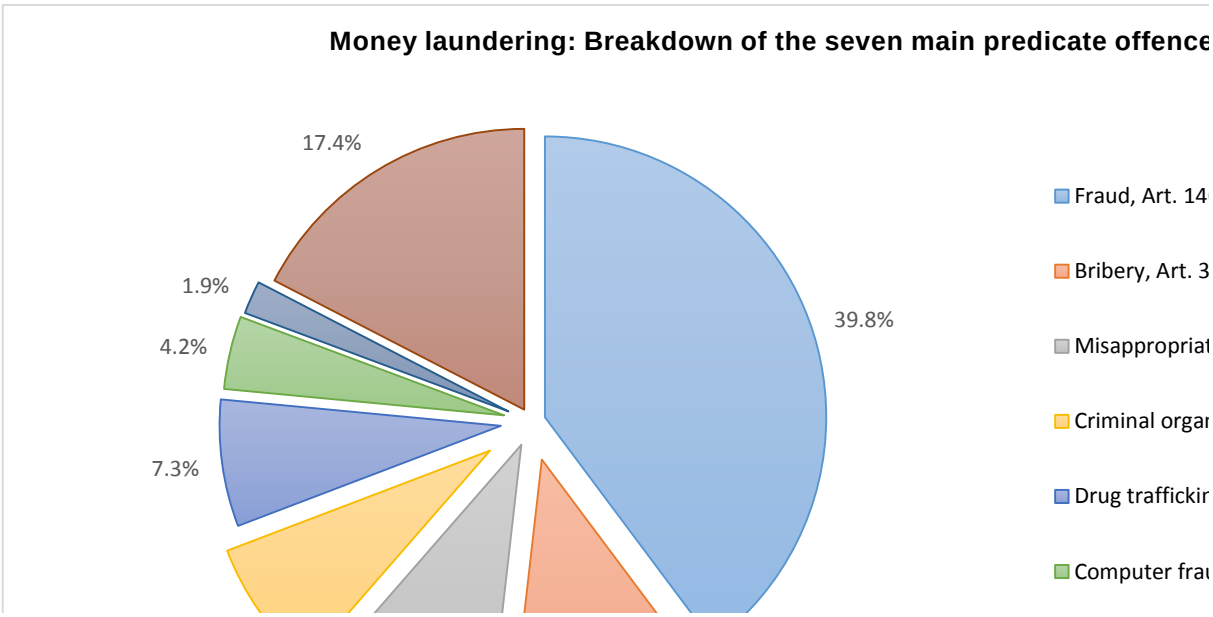
The growing number of money laundering convictions and an analysis of the suspicious activity reports submitted to MROS show not only the higher overall effectiveness of Switzerland's system but also a real increase in the threat. The greater increase in the number of suspicious activity reports relative to the milder increase in the number of convictions can be explained either by the rise in certain key predicate offences or else by a change in the modus operandi of the most significant predicate offences, making them more difficult to detect and suppress (Figures 9, 10, 11).

6.2.2 Identification of the real threat

Unlike the reporting systems used in other countries, in Switzerland the motivation for a suspicious activity report submitted by financial intermediaries to MROS is based on a prior independent analysis of the risk that the business relationship in question is used for money laundering purposes. Consequently, the data in the MROS suspicious activity report database is not derived from an automatic suspicion identification procedure but rather primarily from suspicions established by financial intermediaries based on their own analyses. As such, the MROS database can be considered as the most representative quantitative approximation available in Switzerland regarding the real threat present in the financial sector. Nevertheless, it is necessary to correct the real threat identified in this manner, given that it unfolds outside the scope of financial intermediation defined by the AMLA and depending on the increased detection difficulty there may be.

Identification of the key threats
An analysis of the suspicious activity reports submitted to MROS between 2004 and 2014 shows the following breakdown of the suspected predicate offences identified (Figure 12).

Figure 12: Identification and significance of the seven key suspected predicate offences, 2004-2014



An analysis of the real threat demonstrates a variable degree of internationalisation for the different suspected predicate offences (Table 2). The degree of internationalisation reveals significant vulnerability depending on the predicate offence in question, firstly in terms of the probability of detection and especially regarding the likelihood that the money laundering associated with it is effectively sanctioned and the assets confiscated. The transnational dimension tends to increase particularly with regard to money laundering activity following misappropriation and criminal mismanagement. This vulnerability is even greater with regard to money laundering associated with participation in a criminal organisation and is greatest of all for money laundering activity following bribery. Moreover, property predicate offences tend to be committed online.

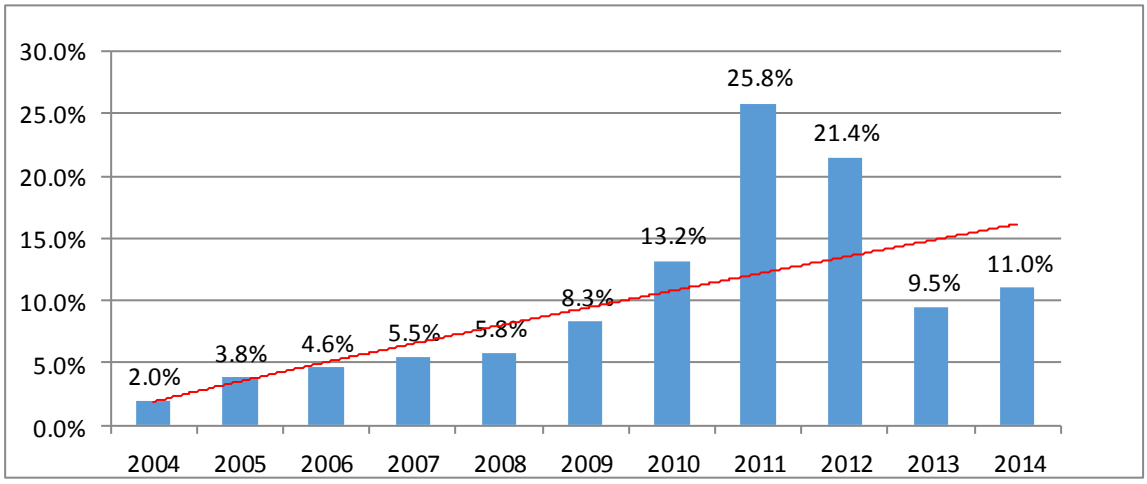
Table 2: Domicile of the main players for the key suspected predicate offences

	Domicile of main player	
	Switzerland	Abroad
All predicate offences	44.0%	56.0%
Fraud (Art. 146 of the SCC)	42.6%	57.4%
Misappropriation (Art. 138 of the SCC)	37.9%	62.1%
Criminal mismanagement (Art. 159 of the SCC)	28.2%	71.8%
Criminal organisation (Art. 260ter of the SCC)	20.9%	79.1%
Bribery (Art. 322^{septies} of the SCC)	9.1%	90.9%

Third-party money laundering

An analysis of the suspicious activity reports between 2004 and 2014 also shows that approximately 10% of suspected offences concern money laundering itself, without it being possible to identify a more specific predicate offence. The relative increase in basic money laundering compared with all suspected predicate offences suggests that a growing proportion of money laundering activity in Switzerland concerns the last stage of the process, i.e. integration (stage III). In this final stage, it is often difficult to support an initial suspicion and link the assets concerned to a specific felony. This stage often features a high degree of complexity involving a variety of legal structures and mobilising a range of economic players who make the transactions and operations undertaken seem plausible. Furthermore, the increase in the suspected offence of money laundering could suggest that a growing proportion of international money laundering activity is in the hands of criminal networks and intermediaries specialised in money laundering, i.e. third-party money laundering, (Figure 13).

Figure 13: Trend of the suspected offence of money laundering, 2004-2014 (without a specific known predicate offence)



The threats that are potentially underestimated include predicate offences to money laundering where financial intermediation in accordance with the AMLA plays a less important role, as well as newly introduced predicate offences that have not yet generated their full impact.

Street crime

The predicate offences for which criminals use economic channels other than financial intermediation as defined in the AMLA generally concern funds and assets derived from street crime in Switzerland, particularly drug trafficking[72] in violation of the Federal Act of 3 October 1951 on Narcotics and Psychotropic Substances (NarcA)[73], theft (Art. 139 of the SCC) and trafficking in human beings (Art. 182 of the SCC). If not spent directly, the assets derived from street crime, including drug trafficking profits, are often laundered through the local economy. However, abuse of the local economy in Switzerland for laundering assets derived from this form of crime constitutes a specific vulnerability given that few cases are detected via financial intermediation. Only money transmitters regularly submit suspicious activity reports regarding the threat of money laundering associated with local drug trafficking.

New stock-market-related predicate offences

The newly introduced predicate offences include counterfeiting of goods (Art. 155 of the SCC), product piracy (Art. 67 of the Federal Act of 9 October 1992 on Copyright and Neighbouring Rights, CopA[74]), insider trading and price manipulation (Art. 40 para. 2 and Art. 40*a* para. 2 of the SESTA). The last two did not become predicate offences to money laundering until 1 May 2013. Consequently, it is not yet possible to comment on the significance of money laundering associated with these predicate offences. However, it is obvious from the few cases reported to MROS that money laundering activity linked to these newly introduced offences often has widespread international ramifications, suggesting that usually the laundering rather than the predicate offence itself is performed in the Swiss financial sector. Moreover, the reported cases suggest that financial instruments traded outside of the regular stock exchange are particularly vulnerable.

Tax-related predicate offences: Existing offence in the case of indirect taxation and new predicate offence associated with serious tax crimes (direct taxation)

Article 14 paragraph 4 of the ACLA makes provision for a predicate offence to qualified tax fraud regarding fraud in relation to administrative services and charges committed in organised gangs (customs contraband). The FCA has not brought criminal proceedings since this provision entered into force in 2009. Nevertheless, 50 to 60 requests for international mutual legal assistance have been submitted based on facts that could constitute the predicate offence provided for in Article 14 paragraph 4 of the ACLA, particularly VAT carousel fraud[75]. The FOJ delegated the review of all of

[72] See the analytical report on money laundering rulings handed down in Switzerland, Federal Office of Police (fedpol), 2014

[73] SR 812.121

[74] SR 231.1

[75] A VAT carousel generally involves the cross-border trade in goods conducted with a view to enabling a company to deduct input tax without VAT ever being paid. The pseudo companies then disappear without paying the booked VAT to the tax authorities and the buyers of the goods sell them while profiting from the input tax deduction. It is referred to as a carousel when this fraud mechanism is repeated several times with the same merchandise.

these mutual legal assistance requests to the FCA, which responded on the basis of Article 14 paragraph 4 of the ACLA. However, this legal assessment has never yet been considered by the Federal Criminal Court or Federal Supreme Court, as all of the requests dealt with were admissible because they also included simple tax evasion, which authorises the granting of mutual legal assistance by virtue of the Anti-Fraud Agreement[76] or the Convention Implementing the Schengen Agreement[77].

During the period under review, MROS likewise received around 40 suspicious activity reports concerning VAT fraud of this type committed in various European countries; case law treats this as fraud in accordance with Article 146 of the SCC.

Following the FATF's international standards, serious tax crimes were introduced as predicate offences to money laundering in 2012. The corresponding implementing legislation (Federal Act of 12 December 2014 for Implementing the Revised FATF Recommendations of 2012) introduced a serious crime in direct taxation (Art. 305bis para. 1 and 1bis of the SCC) and extended Article 14 para. 4 of the ACLA beyond customs contraband in order to cover other indirect taxes levied by the Confederation in addition to customs duties and VAT upon importation. The pertinent provisions will not enter into force until 1 January 2016. Consequently, no data is available as yet to assess the real threat of money laundering resulting from serious tax crimes, particularly with regard to direct taxation.

6.2.3 Analysis of the key threats

Property predicate offences

In 2014, fraud was still the most significant predicate offence to money laundering in absolute terms in Switzerland. Relative to the other predicate offences, fraud cases have been trending downwards since 2010. In reality, this downward trend can be explained by the fact that a growing proportion of fraud is now committed online (Figure 14). Internationally, the phenomenon of online fraud is constantly on the rise[78]. This new form of cybercrime has specific features, particularly regarding the modus operandi, and therefore differs fundamentally from conventional property offences. Moreover, cybercrime is often transnational in nature and is frequently highly complex in technical terms. This trend is also visible in Switzerland.

For this reason, CYCO, which is attached to fedpol, drew up structural tables together with its service partners to describe the specific characteristics of the various cybercrime phenomena that can give rise to money laundering activity. The phenomenon of cyber fraud[79] essentially takes the following forms: false international transfer orders[80], fraudulent online shops[81], false real estate advertisements[82], fictitious transport companies[83], false requests for assistance[84], false payment confirmations[85], advance payment scams[86], false phone calls from Microsoft[87], romance scams[88] and

[76] Cooperation Agreement of 26 October 2004 between the European Community and its Member States, of the one part, and the Swiss Confederation, of the other part, to combat fraud and any other illegal activity to the detriment of their financial interests; SR 0.351.926.81

[77] Agreement of 26 October 2004 between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis; SR 0.362.31

[78] FATF, Global Money Laundering and Terrorist Financing Threat Assessment, 2010

[79] Online fraud misdemeanours. In 2013 alone, CYCO received 2,257 reports concerning online fraud, representing 40% of the reports regarding property offences committed online. See the annual report of the Cybercrime Coordination Unit Switzerland (CYCO), 2013, p. 12.

[80] The perpetrator pretends to be a superior or client and prompts a company's employee to make an international transfer

[81] The online shop does not deliver the merchandise ordered or else delivers lower-value goods or counterfeits

[82] False real estate advertisements prompt the victim to transfer a housing deposit in advance

[83] False transport companies are used as trusted third parties for dispatching merchandise

[84] The perpetrator sends requests for financial assistance to the victim's e-mail contacts

[85] The perpetrator sends the seller (the victim) false payment confirmations, imitating company e-mail addresses or inventing the e-mail addresses of fictitious companies

[86] Mostly by sending spam, the perpetrators seek partners to pay fees in order to release a large sum of money

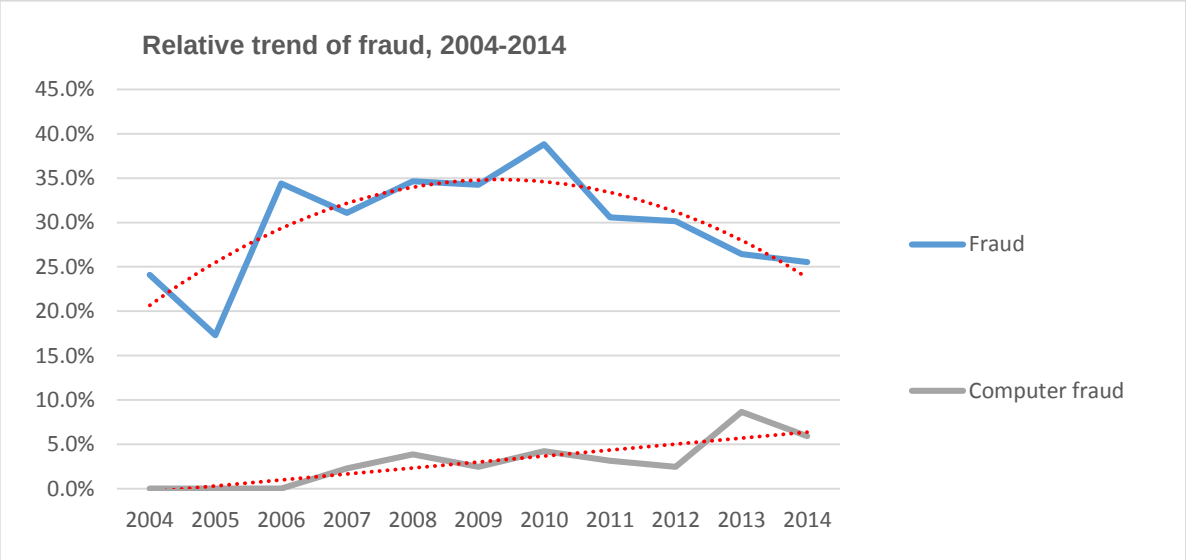
[87] The perpetrator pretends on the telephone to be a Microsoft employee and performs harmful actions on the victim's computer

[88] Feigned romantic intentions followed by a request for money

phishing[89]. Hacking[90], cybersquatting[91] or the use of malware[92] can also give rise to money laundering activity in that these contribute to fraud or another crime being committed. In parallel to cyber fraud, other property offences can be predicate offences to money laundering, particularly extortion (Art. 156 of the SCC) committed with the help of malware, DoS/DDoS[93] attacks or sextortion[94].

Against the backdrop of these new forms of crime, the MROS statistics show an upward trend for predicate offences to money laundering in the shape of online fraud committed by means of computer fraud (Art. 147 of the SCC). The money laundering activity most commonly found in association with these offences is fraud linked to fraudulent online sales of goods or services and phishing. The apparent decline in conventional fraud as a predicate offence is accompanied by a steady increase in suspicious activity reports regarding the specific offence of computer fraud. In this context, it is probable that the phenomenon is not yet fully reflected in the figures derived only from an analysis of suspicious activity reports. Because of the technology used in fraud and other property offences committed online, it is more difficult to identify the alleged perpetrators, who, moreover, are usually abroad. In addition, the reporting rate for cyber fraud is particularly low in Switzerland at 11.9%[95]. It is thus likely that the level of predicate offences to money laundering involving fraudulent property offences is actually stable or even rising because of cyber fraud.

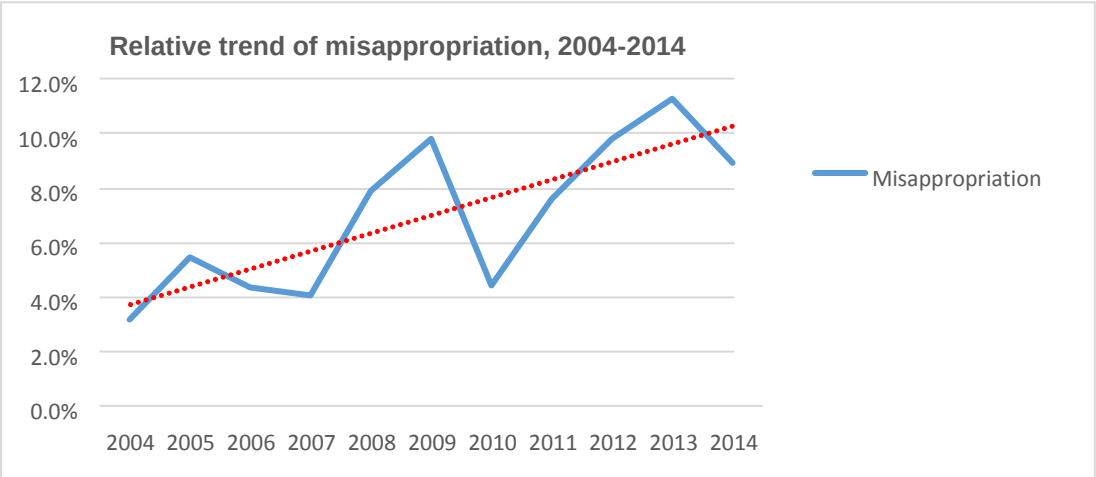
Figure 14: Trend of fraud and computer fraud relative to other suspected predicate offences in percentage terms, 2004-2014



At the same, the predicate offence involving misappropriation is clearly rising in relation to all suspected predicate offences, with a relative increase of 4% to 10% (Figure 15). This predicate offence to money laundering has become more internationalised, just like the predicate offence of criminal mismanagement, given that the misappropriation of funds intended for different forms of financial investment is frequently involved.

Figure 15: Trend of misappropriation relative to other suspected predicate offences in percentage terms, 2004-2014

[89] Method for obtaining personal data, particularly bank details. In 2013, CYCO received 2,208 phishing reports, representing 39% of the reports regarding property offences committed online. See the annual report of the Cybercrime Coordination Unit Switzerland (CYCO), 2013, p. 12.
[90] Unauthorised access to a third-party IT system
[91] Registration of domain names to which the owner is not entitled in reality or which can be confounded with the names of companies, authorities, brands or individuals
[92] IT program that executes harmful functions
[93] Deliberate attacks on a computer, server or network with a view to making them unavailable
[94] Blackmail using sex videos of the victim
[95] Killias et al. 2011



The vulnerabilities associated with the threats arising from fraudulent predicate offences lie primarily in the detection and suppression difficulties linked with new technologies and their growing transnational nature involving several jurisdictions.

An analysis of suspicious activity reports suggests a major upward trend for the predicate offence of bribery of foreign public officials in accordance with Article 322^{septies} of the SCC and a slight increase for the predicate offence of support for and participation in a criminal organisation (Art. 260ter of the SCC). The main feature of these predicate offences is that the primary acts, i.e. the bribery itself or the various felonies committed by a criminal organisation, and some of the secondary acts, such as laundering activity by intermediaries, occur in foreign jurisdictions.

Bribery of foreign public officials (Art. 322^{septies} of the SCC)
Switzerland has a particularly low corruption index by international standards, indicating that its vulnerability to potential threats associated with money laundering is limited.

Table 3: Corruption index for Switzerland, 2013-2014

	Transparency International Corruption Perception Index (TI CPI)
2013	85/100
2014	86/100

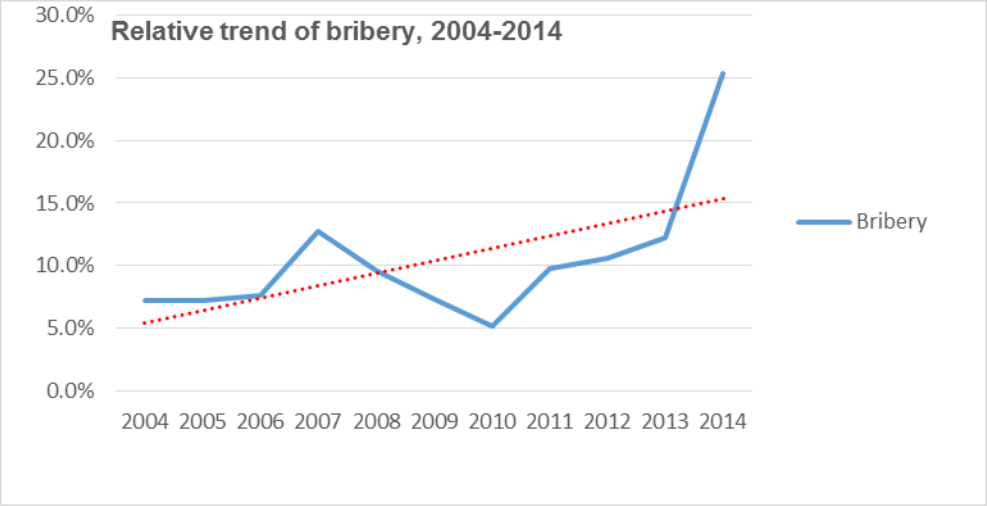
Source: Transparency International 2015

Suspicions of money laundering activity associated with the bribery of Swiss public officials or the acceptance of bribes by such officials in accordance with Articles 322ter and 322^{quater} of the SCC are rare, suggesting a low real threat for money laundering activity following bribery in Switzerland. This is confirmed by the corruption perception index for Switzerland (Table 3). Nevertheless, the potential threat linked with bribery in Switzerland is possibly underestimated, mainly given the presence of a large number of multinationals and international sporting federations. Bribery between private players is not a predicate offence to money laundering, however, and it is not prosecuted ex officio in Switzerland[96].

Based on the model of money laundering in stages, the threat for Switzerland's financial sector is found primarily in the layering and integration (stages II and III) of assets derived from bribery, enabling the bribed person to freely dispose of them for consumption and reinvestment purposes. At the same time, an analysis of the nationality of BOs shows parallel financial flows involving both the active players, who are usually nationals of OECD member countries, and the passive bribery players domiciled in jurisdictions with high corruption levels. Another share of the assets derived from bribery in foreign jurisdictions that can possibly be in Switzerland concerns the proceeds from advantages unduly gained from active bribery. The financial intermediaries concerned by suspicious activity reports regarding bribery are concentrated almost exclusively in Switzerland's large financial centres, i.e. the cantons of Geneva, Zurich and Ticino.

[96] Articles 1 and 2 of the UCA (however, see the Federal Council's bill mentioned in section 5.2.2.2 aimed at private bribery being prosecuted ex officio)

Figure 16: Trend of bribery performed abroad relative to other suspected predicate offences in percentage terms, 2004-2014



The upward trend for bribery committed abroad, i.e. a relative increase of 5% to 25% since 2004 (Figure 16), and giving rise to money laundering activity in Switzerland corresponds to the intensification and internationalisation of illicit global financial flows, including flows of funds arising from bribery[97]. Even if the general upward trend for Switzerland is confirmed from year to year[98], the overall analysis shows that the threat associated with this predicate offence is highly volatile, suggesting that it is particularly sensitive to political changes and events that can occur in the jurisdictions concerned. Some of the threat associated with misappropriation and criminal mismanagement probably overlaps with kleptocracy leading to bribery itself, often involving the same group of players. Moreover, part of the increase can also be explained by the fact that financial intermediaries have greater access to names and information on foreign bribery affairs through various media and databases.

Participation in and support for a criminal organisation (Art. 260ter of the SCC)

Organised crime takes different forms in Switzerland in terms of both structure and scope. Going from serial burglaries to money laundering, the range of offences also includes drug trafficking and human trafficking[99]. On the one hand, the basic criminal activity directly poses a threat to citizens' security; on the other, organised crime constitutes an ever-present threat for the legal economy and political institutions. From a legal standpoint in Switzerland, the aforementioned forms of organised crime are assessed differently depending on their level and type of organisation. The predicate offence under consideration here concerns exclusively the most serious form of organised crime, legally constituting the offence of participating in or supporting a criminal organisation in accordance with Article 260ter of the SCC and usually coming under the authority of the OAG (Figure 17). According to Federal Supreme Court case law, certain terrorist organisations and kleptocratic regimes are also deemed to be criminal organisations from a legal standpoint[100].

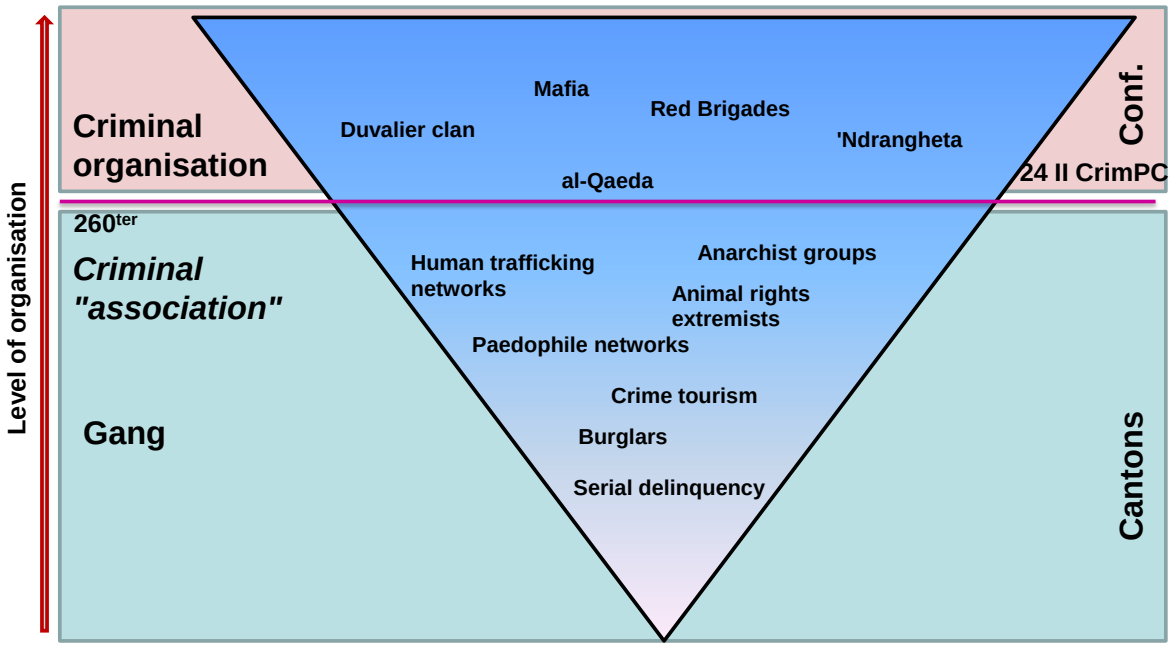
Figure 17: Legal distinction between the constituent elements of Article 260ter of the SCC and criminal activity in organised gangs

[97] Global Financial Integrity, "Illicit Financial Flows from Developing Countries 2001-2010", 2012; it should be noted that only around 3% of the illicit financial flows directly concern bribery

[98] Annual report of the Federal Office of Police (fedpol), 2013, Statistics 2013, p. 4

[99] 2013 annual report of the Federal Office of Police (fedpol), May 2014

[100] Federal Criminal Court case law, which has remained unchanged since 1999, has qualified seven groups as terrorist criminal organisations in accordance with Article 260ter of the SCC. See decision of 21 October 2002 (1A.174/2002), decision of 15 November 2002 (1A.194/2002), decisions of the Swiss Federal Supreme Court 128 II 355 ff and 125 II 569 ff, decision of 5 April 2005 (1A.50/2005), decisions of the Swiss Federal Supreme Court 131 II 235 ff and decision of 25 October 2012 (1C.470/2012).

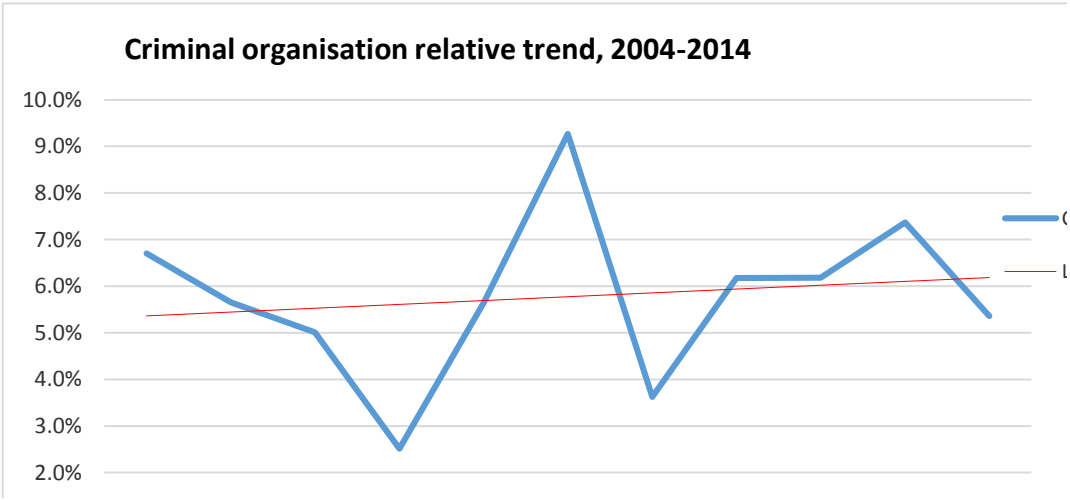


Source: fedpol

A large proportion of criminal organisations' activities in Switzerland is certainly attributable to drug trafficking, and the leadership structures are often in other European countries[101]. At the same time, certain increasingly internationalised criminal organisations are tending to diversify their criminal activity and can use their territorial presence in Switzerland to launder the organised crime gains obtained from other jurisdictions, particularly with the help of commercial enterprises and service providers operating essentially in the financial and real estate sectors, as well as in the restaurant trade[102]. Geographically, the threat associated with criminal organisations active in neighbouring European countries seems higher, suggesting that these have a greater territorial footing in Switzerland than other criminal organisations. Conversely, money laundering performed by criminal organisations operating outside of Europe is detected less frequently and could thus be underestimated.

According to an analysis of the suspicious activity reports concerning possible participation in a criminal organisation, the associated money laundering activity is rising somewhat (Figure 18). This primarily concerns Switzerland's main financial centres, i.e. the cantons of Zurich, Geneva and Ticino, as well as the cantons of Bern and St. Gallen to a lesser extent.

Figure 18: Trend of the felony of participation in and support for a criminal organisation relative to other suspected predicate offences in percentage terms, 2004-2014



[101] See the analytical report on money laundering rulings handed down in Switzerland, Federal Office of Police (fedpol), 2014

[102] 2014 annual report of the Federal Office of Police (fedpol)

However, this slight increase in money laundering that could be associated with criminal organisations could also be explained by better access to information on certain persons' links with such organisations, principally in electronic media.

6.2.4 Overall risk evaluation

Complexity
The level of complexity of a predicate offence to money laundering increases the vulnerability of the system for combating the threat of money laundering. In this regard, the threats associated with the key predicate offences have varying degrees of complexity, leading to different vulnerabilities depending on the threat identified.

Legal structures such as domiciliary companies, trusts and foundations reduce the transparency of the economic background of capital flows associated with a given business relationship, thereby diminishing the probability of being able to identify the actual BOs of the assets involved. Consequently, the involvement of domiciliary companies can give an indication of the complexity level of the money laundering threats identified. With regard to such indication, the predicate offence of fraud has a similar level of complexity to that of all the threats measured. In contrast, an analysis of the significance of domiciliary companies' involvement in bribery-related predicate offences suggests a much higher degree of complexity. This analysis also shows a higher level of complexity relative to money laundering activity associated with participation in a criminal organisation (Table 4).

Table 4: Level of complexity: involvement of domiciliary companies, 2004-2014

	Involvement of domiciliary companies
All predicate offences	17.1%
Fraud	16.5%
Bribery	38.1%
Criminal organisation	22.6%

An analysis of predicate offences according to the number of players involved also suggests a higher level of complexity for bribery-related predicate offences committed abroad. In 51.5% of cases linked to bribery committed abroad, more than three players are involved, while the percentage is 43.7% for fraud-related money laundering.

Sums of money involved
The amount of money involved is an additional indication of vulnerability relative to the key threats identified. Bribery-related predicate offences have a significantly higher vulnerability level in terms of the sums of money involved. The predicate offence concerning participation in a criminal organisation also has a high vulnerability level in terms of the amount of money concerned (Table 5).

Table 5: Comparison of median values (in CHF thousands) and average values (in CHF millions) for the three key predicate offences, 2004-2014

	Median value of amounts involved in CHF thousands	Average value of amounts involved in CHF millions
All predicate offences	0.970	1.674
Fraud	2.843	1.259
Bribery	70.681	3.993
Criminal organisation	18.524	1.488

Moreover, it can be assumed that criminal activity involving bribery and participation in a criminal organisation has a higher vulnerability level not only because of its greater complexity and the sums of money involved, but also with regard to the potential consequences of these two threats in terms of the reputation of the financial sector as a whole both institutionally and systemically.

Geographical distribution
An analysis of the threats by country reveals a significant European dimension in neighbouring and Mediterranean countries. With regard to the risk associated with bribery (committed abroad) and participation in a criminal organisation, Switzerland is generally exposed both to Europe and to non-European jurisdictions. Outside of Europe, some Eurasian, African and Latin American countries carry

an increased risk. Concerning the projections for total illicit financial flows internationally, the potential threat from Southeast Asia and certain Latin American and African countries in particular seems to be underestimated, especially in terms of the threats associated with bribery and participation in a criminal organisation[103]. Statistics from the Swiss National Bank also point to the same upward trend in the general flows from these regions.

Convictions and international mutual assistance

Between 2003 and 2013, 15% of the total money laundering convictions in Switzerland originated from a suspicious activity report transmitted by MROS to a criminal prosecution authority. In contrast, the percentage of money laundering convictions originally triggered by an MROS report is close to 50% in the cantons of Zurich, Geneva and Ticino, as well as at federal level. An analysis of money laundering convictions by jurisdiction shows that most money laundering affairs in Switzerland are dealt with by cantonal prosecution authorities, primarily the cantons of Zurich, Geneva, Ticino, Vaud, Bern and Basel Stadt, which together account for two thirds of convictions (Table 6).

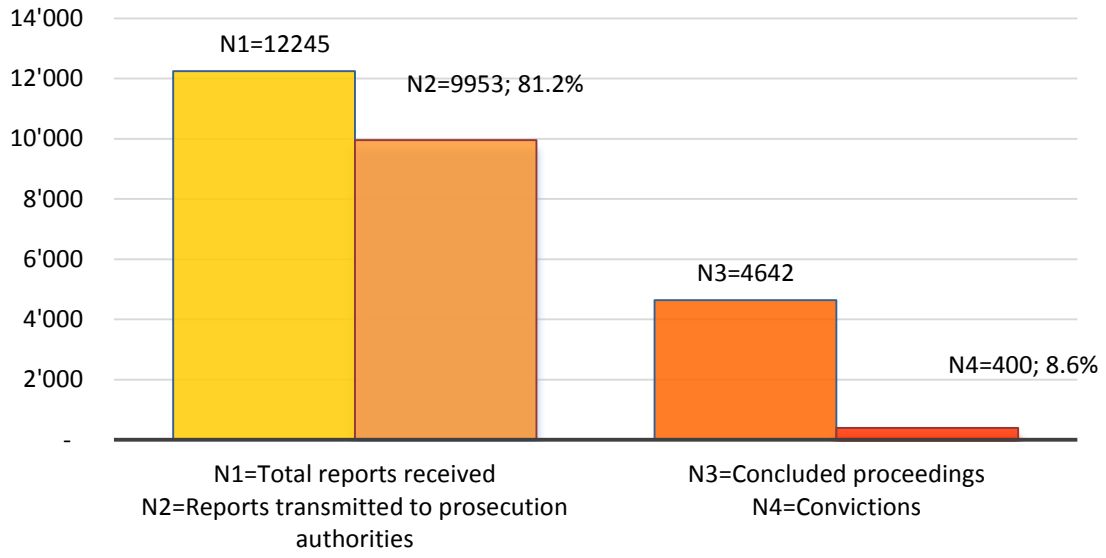
Table 6: Number of money laundering convictions under Article 305bis of the SCC according to the competent prosecution authorities, 2009-2013

	Number of convictions	Percentage
Office of the Attorney General of Switzerland (OAG)	**36**	**3.4%**
Prosecution authorities of ZH, BE, BS, GE, VD, TI	**714**	**66.5%**
Other cantonal prosecution authorities	**323**	**30.1%**
Total	**1073**	**100%**

Source: FSO

Between 2004 and 2014, 8.6% (N_4=400) of concluded criminal proceedings (N_3=4,642) at federal and cantonal level triggered by a suspicious activity report transmitted by MROS (N_2=9,953) resulted in a money laundering conviction (Figure 19). The convictions concerned primarily money laundering following fraud, misappropriation and violations of the NarcA. In contrast, the number of convictions in Switzerland for money laundering associated with participation in a criminal organisation or following bribery abroad was low.

Figure 19: Number of money laundering convictions triggered by a suspicious activity report, 2004-2014



According to the Office of the Attorney General of Switzerland and the offices of the cantonal prosecutors, international mutual assistance plays a particularly crucial role in money laundering affairs when the defendants are not domiciled in Switzerland or when it is necessary to establish or

[103] Global Financial Integrity, "Illicit Financial Flows from Developing Countries 2001-2010", 2012

confirm the existence of a predicate offence to money laundering committed abroad. In such cases, it is often decided to discontinue the proceedings, especially when letters rogatory sent abroad in a bid to establish or confirm a predicate offence committed abroad associated with financial transactions carried out in Switzerland are not executed or when foreign criminal proceedings are abandoned. These complex proceedings with transnational ramifications and requiring international mutual assistance have an average duration of three to five years.

The competent authorities in Switzerland, primarily the FOJ, deal with an average of 250 to 300 requests for international mutual assistance in money laundering matters every year. The requests for international mutual assistance in money laundering matters sent to Switzerland have been on an upward trend since 2007 (Figure 20). Most of these requests are from neighbouring countries and other European countries. They are essentially requests for evidence and, in approximately 20% of cases, are related to existing proceedings in Switzerland.

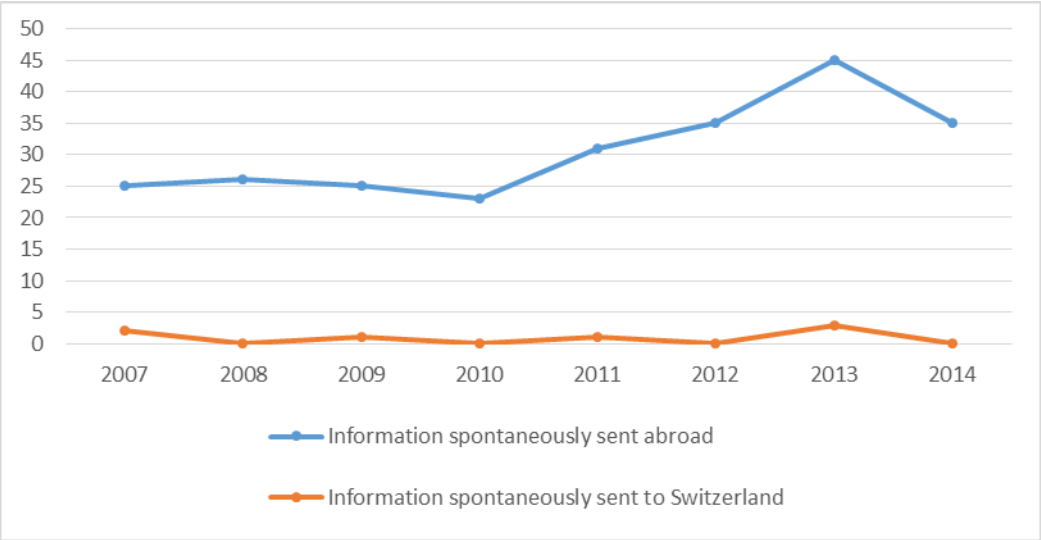
The number of extradition requests received and submitted is three to five per year. Switzerland receives two to three requests for funds to be remitted per year.

Figure 20: Trend of international mutual assistance requests dealt with, 2006-2014

Source: FOJ

Under Article 67*a* of the IMAC, it is possible for Swiss criminal prosecution bodies to transmit information spontaneously to their foreign counterparts in support of ongoing criminal proceedings abroad or in view of the possible initiation of such proceedings (Figure 21). In certain cases, the suspension of proceedings is ordered in Switzerland while awaiting an official international mutual assistance request from a foreign counterpart and the possible outcome of foreign proceedings. There are also five to ten requests for foreign authorities to take over prosecution within the framework of international mutual assistance.

Figure 21: Number of times information is transmitted spontaneously under Article 67*a* of the IMAC, 2007-2014

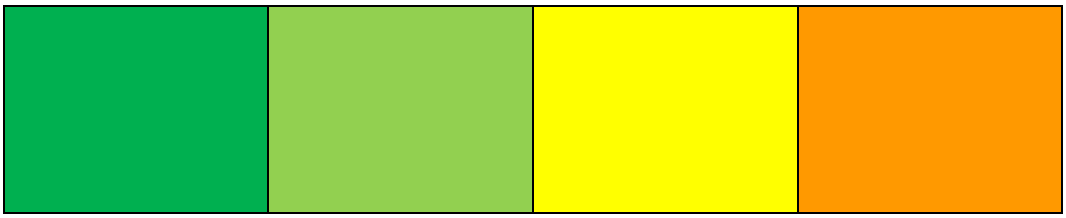


Source: FOJ

Conclusion

The main threats for the Swiss financial sector in terms of predicate offences to money laundering are fraud, misappropriation, bribery and participation in a criminal organisation. In fifth place, we find money laundering linked to street crime, primarily offences against the NarcA, the profits from which are usually laundered by being reinjected into the local economy. Fraud accounts for around a third of the real threat, bribery approximately 15%, participation in a criminal organisation at least 10%, and misappropriation and criminal mismanagement combined at least 10%. An analysis of predicate offences also suggests that some money laundering activity at the international level is performed by specialists. The criminal pattern for fraud-related offences has a more local or regional dimension. At the same time, with regard to the threat arising from fraudulent predicate offences, the predicate offences of computer fraud, particularly phishing, misappropriation and criminal mismanagement are more transnational in nature. The threats associated with bribery and participation in a criminal organisation are even more internationalised, with both a European and non-European dimension. Moreover, the threats associated with bribery and participation in a criminal organisation have a higher vulnerability level because of the greater complexity, which makes it more difficult to detect and suppress them. Furthermore, the threats associated with bribery and participation in a criminal organisation expose the Swiss financial sector to greater vulnerability because of the larger sums of money involved and more significant potential consequences in terms of reputation both institutionally and systemically.

Threats				
			Fraud **Computer fraud** **Misappropriation** **Criminal mismanagement**	
			Bribery (committed abroad) **Criminal organisation**	
		Drug trafficking **Street crime**		



Vulnerabilities

6.3 Terrorist financing

Analysis of the potential threat

Even though Switzerland is neither a priority nor specific target for terrorist groups, particularly Jihadists, an attack could nevertheless be carried out at any time in Switzerland or on Swiss interests abroad[104]. Against the current backdrop of more intense competition between Islamic State and al-Qaeda for domination of the Jihadist movement, both of these organisations could seek to promote themselves by possibly carrying out attacks with a major symbolic impact. As it is not insulated from this general environment, Switzerland could also be the target of such an attack, or serve as a rear base for planning and executing it in terms of financial and logistical support.

Concerning terrorist financing, there are two main forms of potential threat for Switzerland: firstly, the raising of funds and other assets from residents to finance terrorist activities; and secondly, the use of the financial sector to pool the assets from different foreign sources in order to transmit them to foreign locations for terrorist purposes. In this regard, the potential threat of terrorist financing concerns primarily the financing of terrorist activities that are carried out abroad but use the Swiss financial sector as a transition point. More generally, the threat thus concerns the financing of preparatory measures as well as, in a broader sense, logistical support for an organisation or terrorist network from Swiss territory[105].

Analysis of the real threat

The suspicious activity reports transmitted to MROS provide the most consolidated indication available of this threat level in Switzerland over the long term. It is worth noting that some of the financial flows associated with terrorist financing do not come under financial intermediation and therefore are not captured by quantitative measures.

Relative to the total suspicious activity reports transmitted to MROS as part of the AMLA system, suspicions of terrorist financing account for only a small portion of the reports dealt with. Between 2004 and 2014, a total of 141 suspicious business relationships were reported, representing 1.1% of the total 12,224 money laundering suspicious activity reports received during the period in question (Table 7). MROS thus receives an average of 13 reports concerning suspected terrorist financing per year. The number of international mutual assistance requests for terrorist financing is two or three per year.

In keeping with the nature of terrorist financing activities, which generally call for small amounts of money, the median value reported is around CHF 250 per terrorist financing case, whereas the median value for suspicions of money laundering is significantly higher at CHF 1,000 (Table 7).

Table 7: Comparison of suspicious activity reports concerning money laundering and terrorist financing, 2004-2014

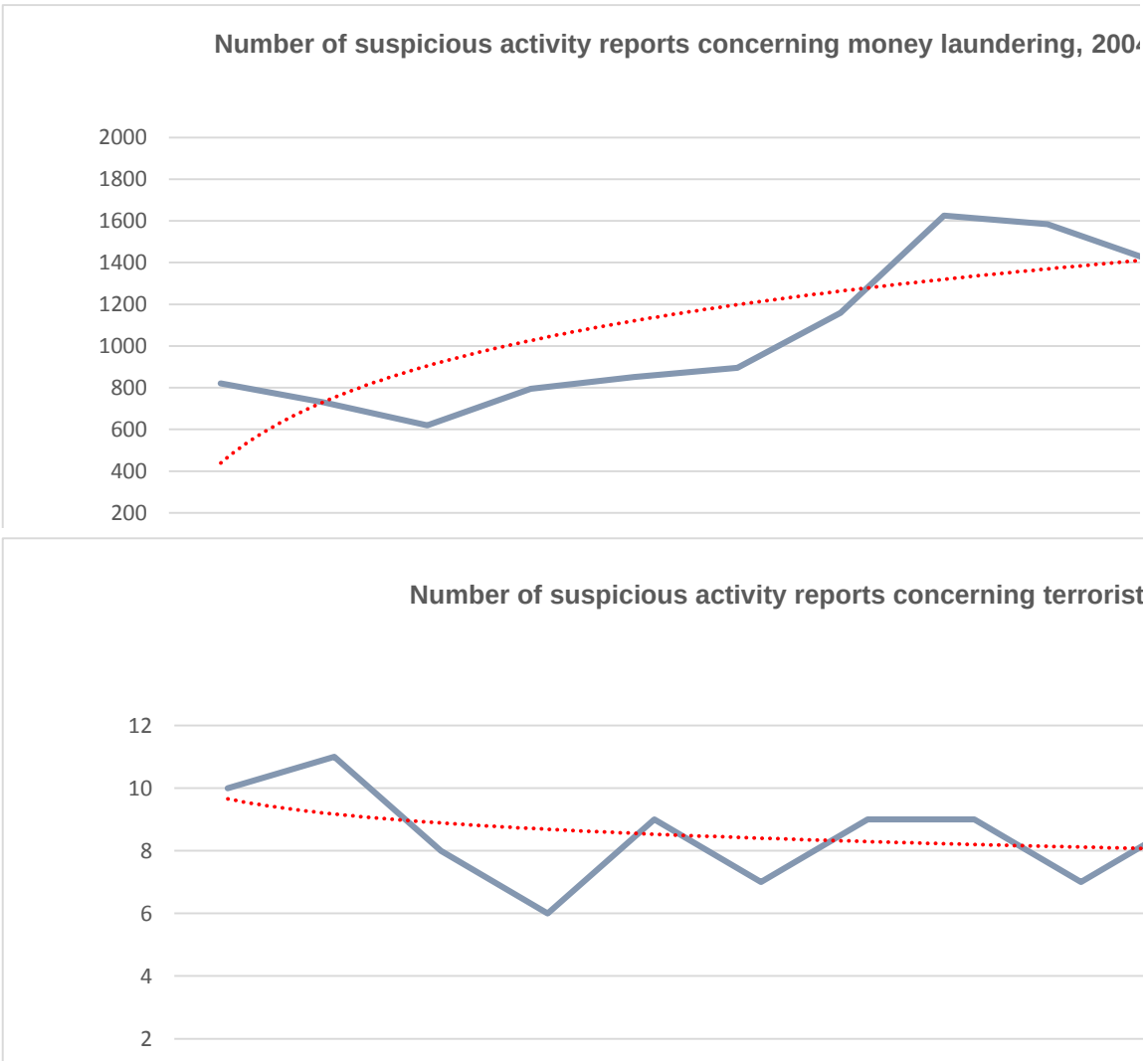
	Terrorist financing	Money laundering
Number of suspicious activity reports	141 (1.1%)	12,083 (98.9%)
Median value	~250 francs	~1,000 francs

Moreover, unlike the increase seen in Switzerland for money laundering suspicious activity reports, the number of cases for suspected terrorist financing is not very high and remained stable for the

[104] Situation report of the Federal Intelligence Service (FIS), 2014, p. 25
[105] 2013 annual report of the Federal Office of Police (fedpol), pp. 43-44

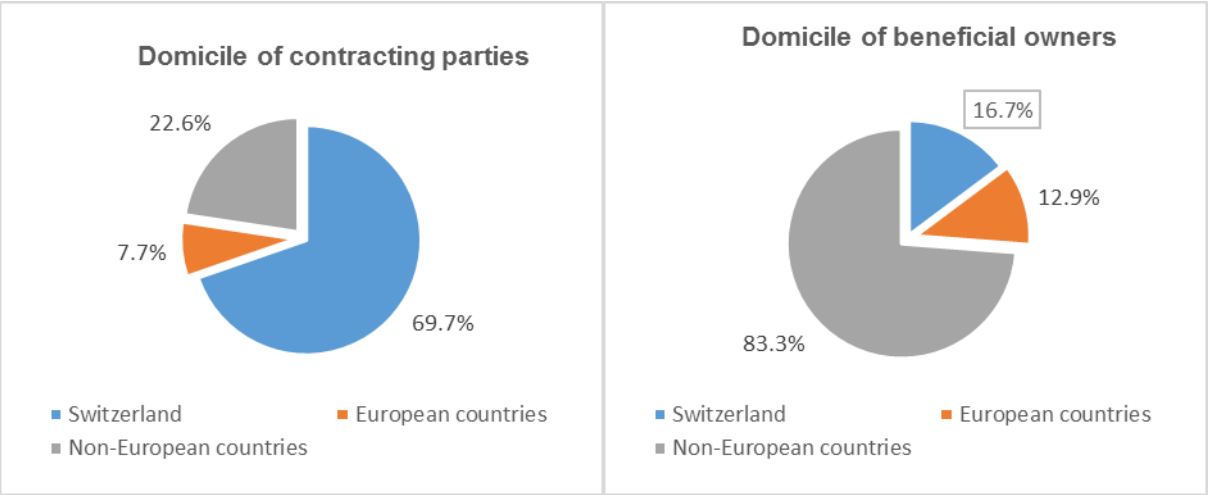
entire period examined (Figures 22 and 23). The more significant year-on-year fluctuations can be explained mainly by the complexity of certain cases, sometimes giving rise to several business relationship reports from financial intermediaries for a given case. However, the number of terrorist financing suspicious activity reports tended to rise during the three years following the 9/11 attacks, before settling at its current level.

Figures 22 and 23: Comparative trend of suspicious activity reports concerning money laundering and terrorist financing, 2004-2014



An analysis of the suspicious activity reports for 2004 to 2014 shows that the business relationship contracting parties were domiciled in Switzerland in more than two thirds of cases. In contrast, the BOs were domiciled abroad in the vast majority of cases, more specifically outside of Europe (Figures 24 and 25).

Figures 24 and 25: Domicile of contracting parties and beneficial owners for terrorist financing suspicious activity reports



Based on the information currently available, the general trend observed internationally of terrorist organisations obtaining financing through the procurement of forged identity documents – an activity often linked to human trafficking – cannot be demonstrated for Switzerland. More generally, there is no indication in the case of Switzerland that the funds used for possible terrorist financing purposes are more of criminal than legal origin. Nevertheless, there is an exception in the form of the collection of mandatory "donations" organised within certain diaspora communities, which is comparable to the extortion of funds that can be used to finance possible terrorist acts and activities.

6.3.1 Alternative financial circuits outside of financial intermediation

Alongside the method of collecting and transmitting money and assets through financial services subject to the AMLA, it is worth noting that alternative fund transmission methods, such as *hawala*[106] systems and physical fund transfer methods, may be used in Switzerland to finance possible terrorist acts. These transmission methods are particularly attractive because of their confidential nature. Given that they leave very little in terms of a paper trail, they are more difficult to detect and thus constitute a major obstacle for the establishment of evidence in legal proceedings. On this basis, it is probable that alternative transfer methods are used in Switzerland at least as frequently as regular financial services to collect and transmit funds and assets for the possible purpose of terrorist financing[107]. However, according to current knowledge of the players involved in this analysis, it is not possible to quantify the significance of these methods of collecting and transmitting funds and assets.

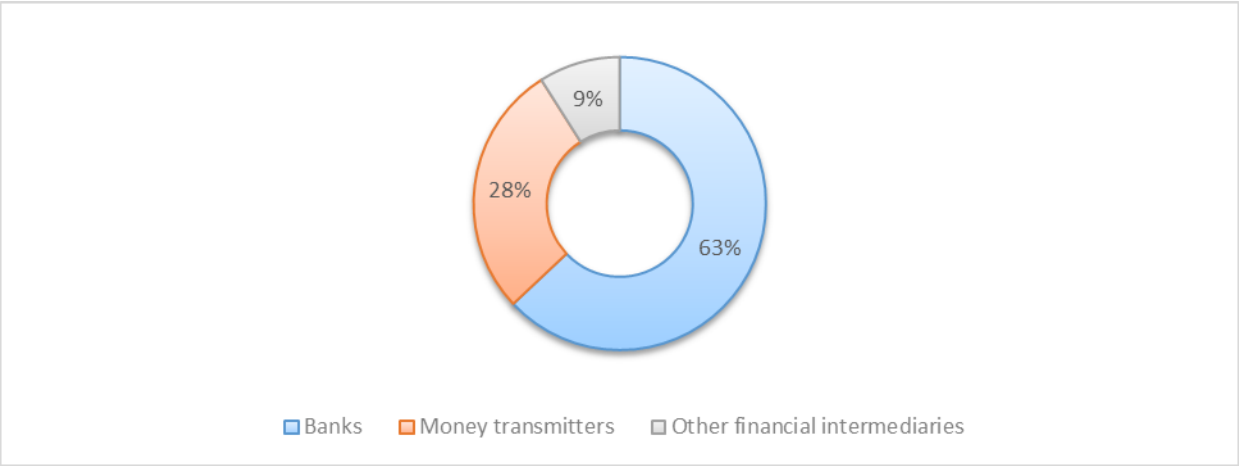
6.3.2 Types of financial intermediary used and reasons for detection

Between 2004 and 2014, the vast majority of the terrorist financing suspicious activity reports sent to MROS were from banks and money transmitters (Figure 26) in the large financial centres of Zurich and Geneva, as well as the cantons of Bern and Basel Stadt.

Figure 26: Types of financial intermediary used in terrorist financing suspicious activity reports, 2004-2014

[106] The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing, FATF 2013

[107] Silvia Martens, Muslimische Wohltätigkeit in der Schweiz, 2013



The complexity of the cases reported is low or average: between 2004 and 2014, more than three natural persons or legal entities were involved in 41.9% of cases and domiciliary companies were rarely used. This low level of complexity in terms of the number of players involved is consistent with both the means of collecting funds and assets and the relay and redistribution function set up by terrorist groups for various logistical reasons.

One method of financing possible terrorist activities observed during the period analysed consisted in taking out financial credits. More recently, rare cases involving the use of prepaid credit cards were reported. Given the appeal of this method of payment for terrorist financing in terms of ease of use transnationally and anonymity and the growing diversification and significance of electronic means of payment and fund transfer both worldwide and in Switzerland, these methods of payment will probably be used for terrorist financing purposes more often in the future.

The cases reported vary with regard to the sums of money involved, although less than CHF 10,000 was involved in around 75% of the cases. Nevertheless, the total involved exceeded CHF 1,000,000 in a limited number of suspicious cases. Given the small sums of money generally involved, detection based on a gap between the client's economic profile and the transaction is less probable. An analysis of the reasons for detection shows the large proportion of the reported cases triggered by third-party information and newspaper articles (Figure 27). Financial intermediaries use a whole range of sources for meeting their due diligence requirements in terms of terrorist financing. Along with consulting public sources such as the internet, financial intermediaries seek mainly to identify clients who could be on lists of people under embargo or identified as terrorists by international and foreign authorities[108]. The same information comes particularly from the compliance databases of private providers such as World-Check, which are often used by financial intermediaries to assess the risks associated with their clients. With regard to the lists of names, financial intermediaries make a huge effort to distinguish between true and false positives. There are a great many cases of false positives triggered by an apparent correspondence with a name on one of these lists. Most of the time, as it happens, the information available is limited to a simple name, linked to an often imprecise date of birth, for which many homonyms exist. Aware that their names are in databases, the holders of assets suspected of being used for terrorist financing could in certain cases anticipate a possible asset freeze by emptying their accounts.

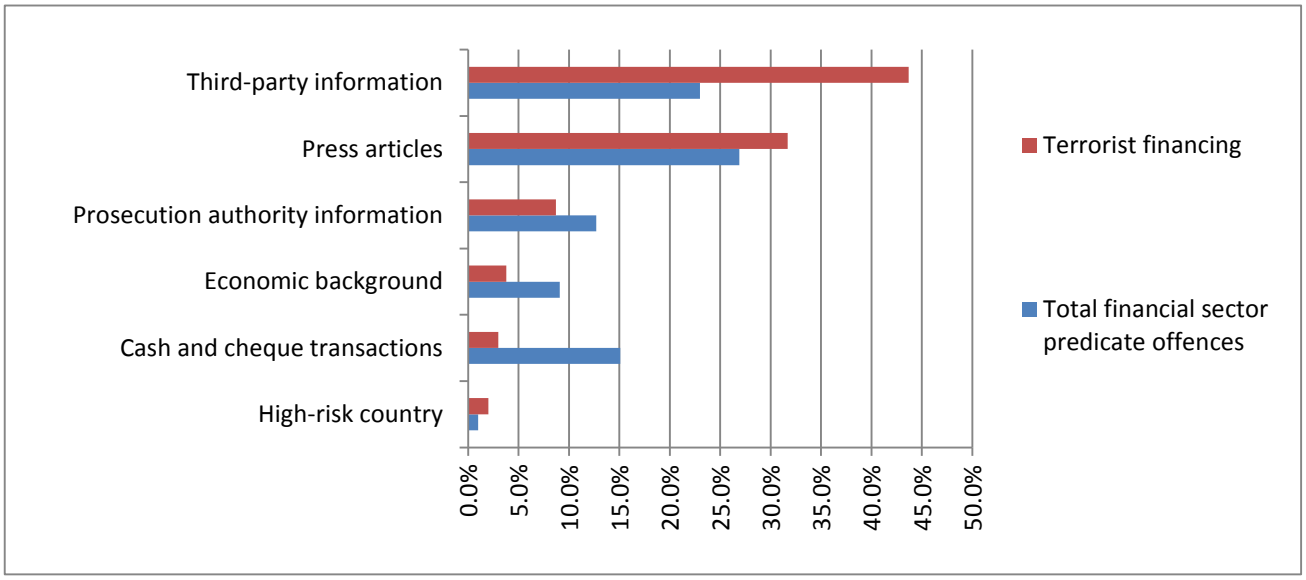
In general, more extensive transaction monitoring concerning doubts about the client's economic background or the origin of funds, or more generally the client's behaviour, does not play a direct role in terrorist financing suspicious activity reports. In the event of doubts about the economic background or unusual transactions for the client's profile, financial intermediaries prefer to subject suspicious cases to more detailed monitoring and in-house management rather than submit a suspicious activity report until the case can possibly be linked to an official list or an actual terrorist event[109]. This scenario applies particularly for persons and entities designated by the Office of Foreign Assets

[108] Financial intermediaries systematically refer to sanction lists, particularly those drawn up by SECO, including the measures ordered by the Federal Council and the United Nations Security Council within the framework of resolution 1267 (1999), those of the United States via the various Bush lists, and EU lists. In contrast, the use of other databases and lists such as those of World-Check varies according to the financial intermediaries, particularly depending on the different database operating costs and the ensuing verification measures.

[109] In compliance with Article 14 of the AMLO-FINMA

Control (OFAC) in the United States and clients from uncooperative territories or countries in application of FATF recommendation 19, which requires financial intermediaries to apply enhanced due diligence measures to clients associated with an uncooperative territory or country. Moreover, the increasingly generalised use of computerised detection systems, especially in the case of small structures in the money transmitting sector, could cause a possible increase in the number of suspicious activity reports in the future.

Figure 27: Trigger for terrorist financing suspicious activity reports sent to MROS, 2004-2014



6.3.3 Involvement of non-profit organisations and commercial enterprises

Since the attacks of 11 September 2001, international bodies have been highlighting the significance of the potential threat posed by the non-profit organisation (NPO) sector in combating terrorist financing globally[110]. In this regard, an analysis of the terrorist financing suspicious activity reports sent to MROS shows that NPOs do indeed play a role in Switzerland. The involvement of such organisations in possible instances of terrorist financing is apparent in 17.4% of the cases reported. However, in contrast to the assumption of more generalised involvement of NPOs, most of the suspicions in Switzerland concern a limited number of recurring organisations (see section 7.2.2. Non-profit organisations). Most of the NPOs mentioned in suspicious activity reports are Islamic charitable organisations with a nationalistic or global focus, organisations affiliated or linked to known ethno-nationalistic organisations and political exile organisations. The most exposed NPOs are those operating in conflict zones, where terrorist organisations are active on the ground and where there is a significant threat of terrorist acts.

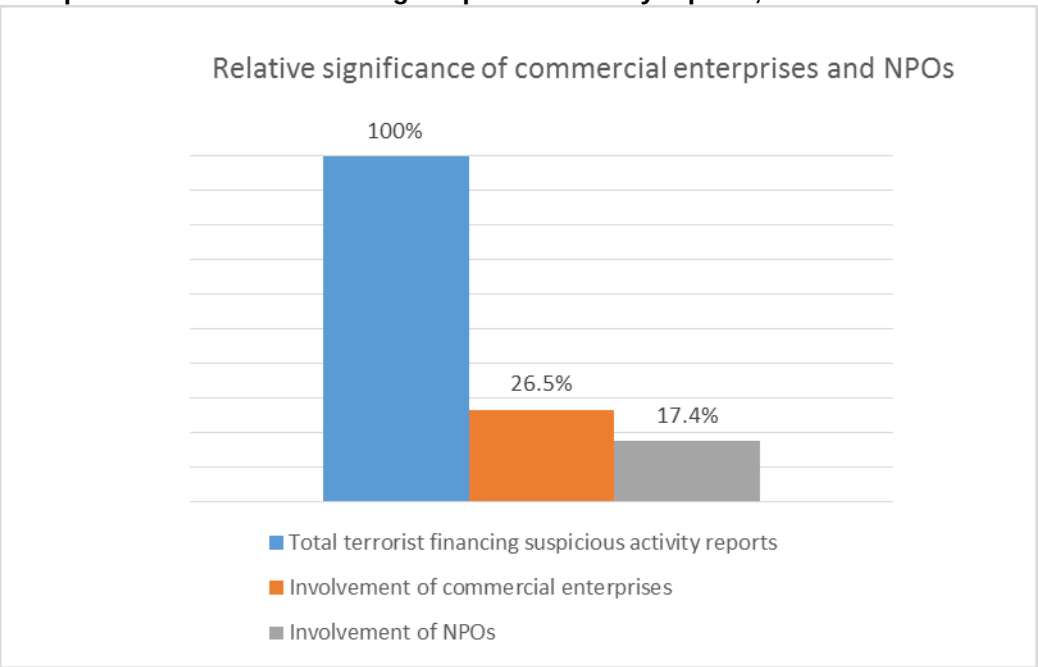
The main vulnerability regarding non-profit organisations in Switzerland lies in their ability to mix the destinations and actual use of the assets involved, most of which are used for humanitarian or political purposes. Furthermore, unlike the attention financial intermediaries pay to domiciliary companies, the BO does not have to be determined for NPOs provided they do not deviate from the purpose stated in their articles of association. In any case, the funds collected are often transferred and distributed subsequently to other organisations and foundations that are no longer under the direct control of the organisation that initially collected the funds. Against this backdrop, the main threat lies in the financing of complex quasi-state groups that combine several structures, some of which may be used for terrorist purposes, through NPOs in Switzerland. This threat could prove to be higher if the presumed destination of the assets in question concerned territories where the relevant organisations have total or partial territorial power – depending on the extent to which the state's power and authority have been lost – or organisations that are part of legitimate governments. In this scenario, the end use of the funds collected in or channelled through Switzerland remains non-specific at the time of collection or transmission. Insofar as the funds collected are actually used for terrorist purposes, they are essentially used for financing logistical and ideological bases of terrorist organisations by making

[110] See FATF recommendation 8, Best Practices. Combating the Abuse of Non-Profit-Organizations, FATF 2013; European Union Terrorism Situation and Trend Report, EUROPOL 2014

infrastructure available in Switzerland and abroad and creating networks, particularly for propaganda and recruitment purposes.

Aside from the use of these organisations, the suspicious activity reports also show that commercial enterprises are possibly used for terrorist financing purposes in more than 25% of suspicious cases (Figure 28). At the same time, the international mutual assistance requests submitted to Switzerland suggest in a certain number of cases that domiciliary companies set up for charitable investment purposes actually finance terrorist organisations.

Figure 28: Comparison of the significance of the involvement of NPOs and commercial enterprises in terrorist financing suspicious activity reports, 2004-2014



The considerable involvement of commercial enterprises in Swiss suspicious cases is consistent with the global trend of terrorist organisations using the vulnerabilities inherent in the international trade system to transfer funds and other assets (Figure 27)[111]. Commercial enterprises can thus serve for transferring the funds and assets collected by mixing them with legitimate assets arising from trade or for using some of the profits for terrorist financing activities. In Switzerland, most of the companies reported are small or medium in size and operate in the area of international merchandise trade or international transport.

Typologies

A. A financial intermediary reported to MROS a business relationship with a foundation supposedly close to an organisation notorious for its terrorist activities. More specifically, the foundation's purpose is to finance a television station whose editorial policy is clearly close to the ideas defended by the terrorist organisation. However, it was not possible for a sufficient financing link to be established between the foundation and the organisation's paramilitary bodies given that the terrorist organisation in question has several components, including political branches that were apparently independent from the paramilitary bodies.

B. A financial intermediary reported a business relationship with a person who seemed to be identical to someone on a foreign state's list of individuals suspected of financing terrorism or participating in a terrorist organisation. In this case, the name and nationality were identical, with the exception of an additional middle name that was not mentioned on the list. Based on transaction analysis and other pertinent information and circumstances, MROS concluded that the person in question was not the individual designated by the foreign state.

C. Several financial intermediaries reported to MROS business relationships with a religious charitable association recently designated by a foreign state's treasury department. According to its articles of association, the funds collected were intended for orphans and people in need in a given conflict zone. The association in question transferred funds to several local foundations. In this context, the legal proceedings were unable to establish that the funds distributed in this way were not used for

[111] CTITF Report Working Group Report 2009, p. 11

humanitarian purposes even though the relevant foundations were reputed to be ideologically close to a political movement involved in terrorist activities in said conflict zone.

6.3.4 Exchange of information and collaboration between players directly involved in combating terrorist financing

In the area of combating terrorist financing, the rapid exchange of the information received is essential. To this end, the different players in the Swiss system collaborate closely so that all necessary information is gathered and analysed as a whole. Thus, in addition to the financial intermediaries who have a duty to report suspicions of terrorist financing, the FIS, MROS, the FOJ and the OAG contribute primarily to the efficient processing of information relating to suspicions of terrorist financing within the scope of their respective powers. Information concerning terrorist financing is exchanged regularly by the FIS with national partners and international partner services both bilaterally and multilaterally. In terms of processing information, FIS bilateral exchanges with partner services at the international level are particularly important. To this end, written requests for information that are sent and received are processed rapidly, in urgent situations on the same day. In addition, the FIS takes part in international meetings of terrorism experts from intelligence services and forwards the corresponding expert reports in the appropriate format to the interested partners in Switzerland. In addition to the cantons, the most important partners of the FIS at the national level are MROS and the Border Guard. In the context of criminal investigations, between 2011 and 2014, 41 requests for mutual assistance in terrorism matters were made to Switzerland by different countries focusing on radical Islamic extremism, separatist organisations and extreme left-wing and right-wing terrorist organisations. Five of these requests specifically concerned terrorist financing. The Swiss authorities also submitted 37 requests for mutual assistance to different countries focusing mainly on radical Islamic extremism, separatist organisations and extreme left-wing terrorist organisations. Three of these requests specifically concerned terrorist financing.

In addition to concluding various bilateral agreements on strengthening police cooperation, Switzerland has sent police attachés to be stationed in several partner states in recent years [112]. The police attachés carry out operational and strategic functions to support criminal proceedings initiated in Switzerland and to ensure rapid and unimpeded forwarding of reliable information between Switzerland and the host countries. They are called upon to deal primarily with serious cross-border crime such as drug trafficking, organised crime, money laundering, human trafficking, terrorism and terrorist financing. In the context of current terrorist threats concerning Jihadist travel, the management of fedpol, FIS and of the FDFA State Secretariat have set up a task force (TETRA - TErrorist TRAvellers) with the aim of exchanging information effectively and coordinating all national efforts to combat the terrorist threat from Jihadist travellers.

There is also an operating working arrangement[113] with the USA which governs the setting up of joint investigation teams to combat terrorism and terrorist financing.

Evaluation

The risk of terrorist financing, in particular through financial intermediation, is limited in Switzerland. However, this risk can change rapidly. To address this threat, one can rely primarily, in criminal terms, on Article 260^{quinquies} of the SCC (financing terrorism) which punishes the direct and intentional financing of a violent crime. Under Article 260ter of the SCC, Swiss criminal law also prohibits support for a

[112] The legal foundations are enshrined in the Federal Act of 7 October 1994 on the Central Offices of the Federal Criminal Police and the joint police and customs cooperation centres with other countries (FCPCOA; SR 360). Police attachés are stationed in Brazil, Italy, Kosovo, Serbia, Thailand, the Czech Republic, the USA and at INTERPOL in France and Europol in the Netherlands. In addition, agreements on the representation of Swiss interests by a third party have been concluded with other major countries for the prosecution authorities, namely Malta, Slovenia, Macedonia, Albania, Bosnia and Herzegovina, Croatia, Montenegro, Indonesia, Cambodia, Malaysia, the Philippines, Poland, Slovakia, Hungary and Canada. Moreover, 15 foreign countries currently have liaison officers, police and customs officers, to represent their interests in Switzerland.

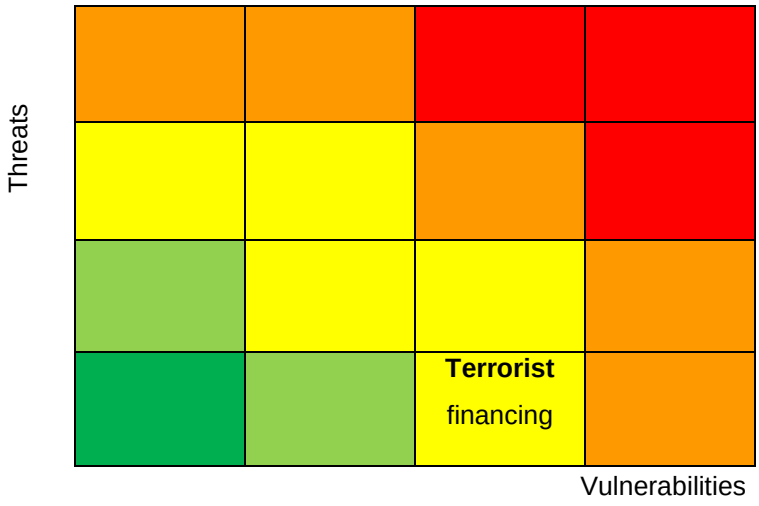
[113] Arrangement of 12 July 2006 between the Federal Department of Justice and Police of the Swiss Confederation and the Department of Justice of the United States of America acting for the Competent Law Enforcement Authorities of the Swiss Confederation and of the United States of America on the creation of joint investigation teams concerning the fight against terrorism and the financing of terrorism (SR 0.360.336.1).

criminal (terrorist) organisation, for example by financing it. Since Article 260^{quinquies} of the SCC was adopted in 2003, no judgment based on this criminal provision has been handed down. Article 260^{quinquies} of the SCC is a subsidiary regulation which is annulled by other provisions of the SCC in the case of the financing of a specific terrorist act or support for a criminal organisation. Where applicable, the perpetrator is guilty, as the instigator or accomplice, of other offences provided for by the SCC, in particular support for a criminal organisation (Art. 260ter SCC). That is how judgments based on Article 260ter SCC were imposed on people whose actions provided support for terrorist activities in terms of ideology and logistics. Prosecution of acts of support for terrorism can in addition be based on other provisions of the SCC, such as Article 259 (Public incitement to commit a felony or act of violence), Article 135 (Representations of acts of violence),[114] which prohibits in particular propaganda which incites terrorist violence, and Article 260bis, which makes provision for the criminal prosecution of preparatory acts, including serious assault and murder. Finally, Jihadist travellers can also be punished for foreign military service, in application of Article 94 of the Military Criminal Code (MCC)[115].

Viewed as a whole, the system to suppress terrorist financing seems to have proved its effectiveness up to now. Compliance with the due diligence obligations by financial intermediaries in particular has a preventive effect of major importance. Likewise, the cooperation of the different competent authorities when subsequently processing the information obtained also plays a central role in preventing the financing of terrorist activities in Switzerland.

Moreover, as already indicated in chapter 5.2.4, the Federal Act on the Prohibition of al-Qaeda, Islamic State and Associated Organisations came into effect on 1 January 2015 in response to the evolving international threat. This law not only prohibits all activities of the organisations concerned in Switzerland and abroad, but even punishes any act aimed at putting human or material resources at their disposal, for example, by recruiting followers or propaganda and fundraising campaigns.

Finally, the work to implement the 2005 Council of Europe Convention on the Prevention of Terrorism is under way. The adoption of provisions to prohibit acts preparatory to terrorist offences is being examined for the purpose of ratifying and implementing this convention. The effectiveness of these provisions will be assessed on the basis of the future case law concerning them.



7 Sectoral risk analysis

7.1 Main sectors subject to the AMLA

For those sectors whose financial intermediaries are subject to the provisions of the AMLA and thus also the duty to report any suspicious activity, the quantitative measurements are first and foremost based on the suspicious activity reports (SARs) submitted to MROS between 2004 and 2014. These measurements are supplemented by additional information (qualitative and quantitative) and analyses supplied by members of the CGMF, specifically the supervisory authorities, as well as the private-sector players consulted. The qualitative risk assessment is thus the product of the CGMF's overall

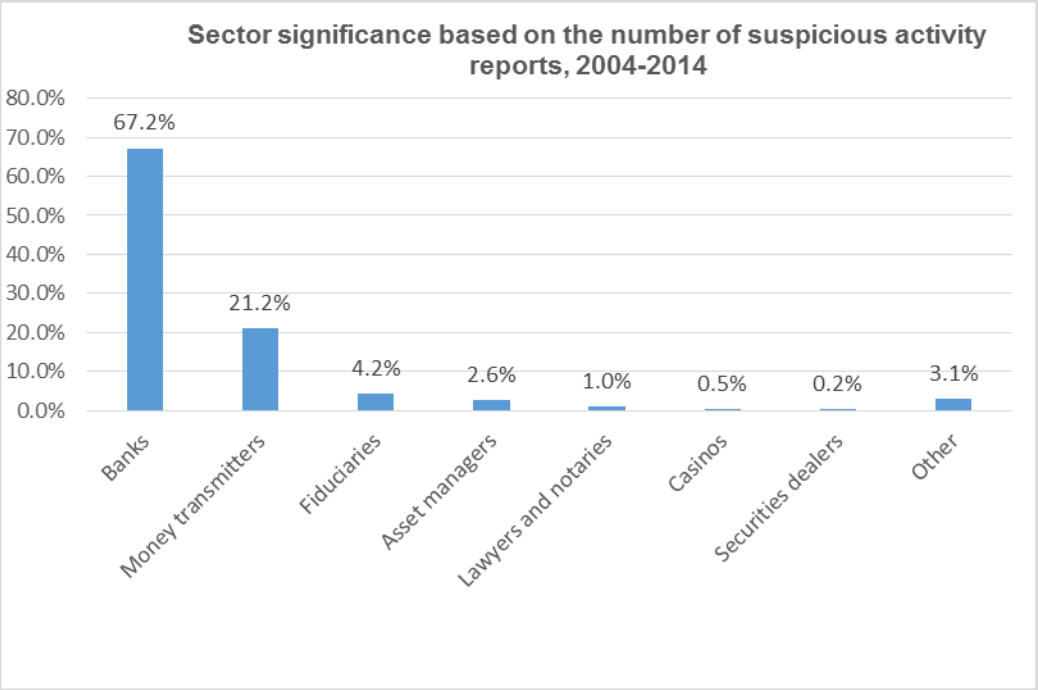
[114] Cf. Ruling from the Federal Criminal Court of 22 May 2014, SK 2013.39.
[115] SR 321.0

analysis of each sector, particularly in terms of their specific vulnerabilities and the appropriateness of the regulatory framework set up to address and mitigate the vulnerabilities identified.

An analysis of the origin of suspicious activity reports shows that five sectors are particularly concerned by the threat of money laundering and terrorist financing. Banking takes the lead in this respect, followed by money transmitters, fiduciaries, asset managers, and lawyers and notaries (Figure 29).

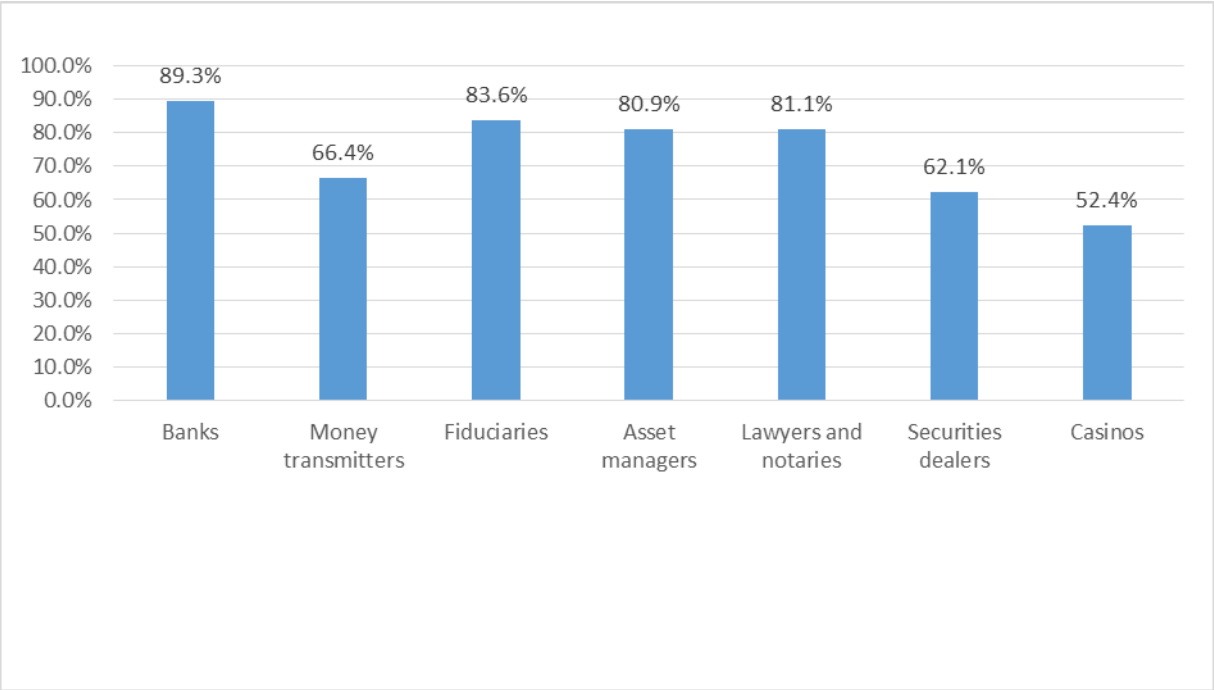
The majority of the suspicious activity reports from these sectors are filed by financial intermediaries operating in the country's three main financial centres, i.e. the cantons of Zurich, Geneva and Ticino. Suspicious activity reports are also submitted from the cantons of Bern and St. Gallen, as several financial institutions have centralised their compliance centres there.

Figure 29: Breakdown of suspicious activity reports submitted to MROS by business sector, 2004-2014



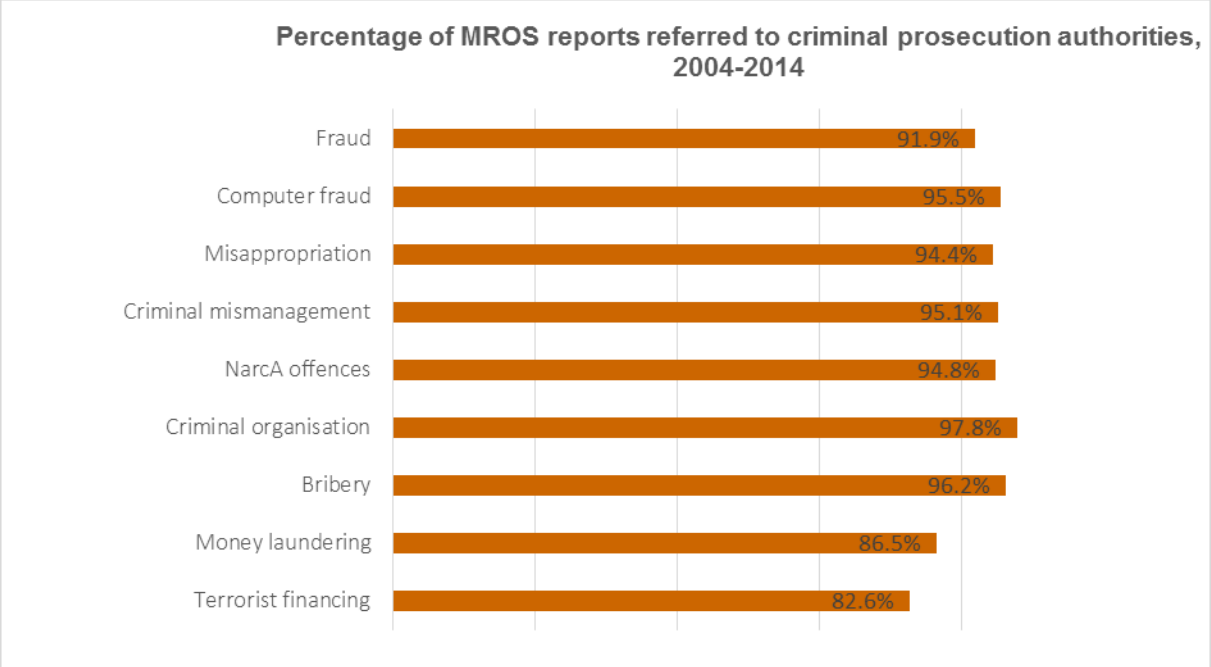
The referral rates to criminal prosecution authorities after analysis by MROS are quite similar for banks, fiduciaries, asset managers, and lawyers and notaries. However, the referral rates of reports from money transmitters, casinos and securities dealers are lower, suggesting that these sectors pose less of a threat (Figure 30).

Figure 30: Percentage of suspicious activity reports referred to criminal prosecution authorities by key business sector, 2004-2014



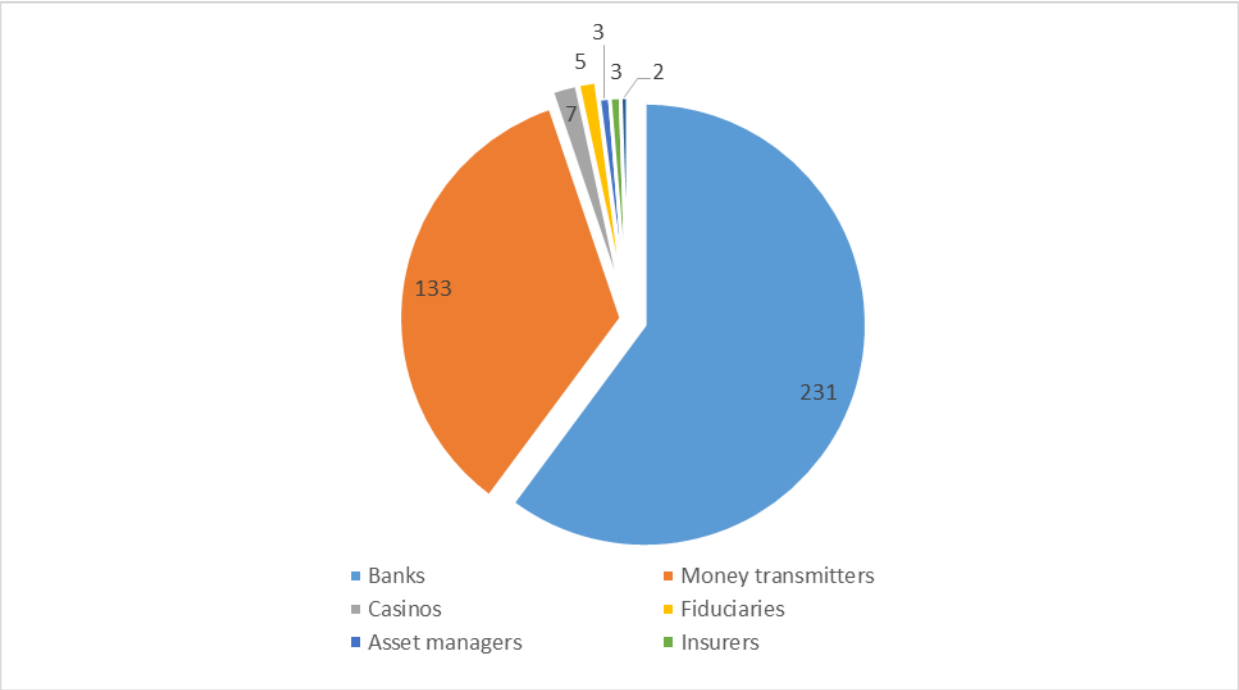
The high general rate of referral, at around 90%, is an indication of the quality of the analytical work done by the financial intermediaries. Regarding money laundering and terrorist financing offences, the referral rate is high, despite the greater difficulty in substantiating a suspicion. Moreover, the referral rates with regard to the main predicate offences reflect the equal treatment of all suspicious activity reports submitted to MROS (Figure 31).

Figure 31: Percentage of suspicious activity reports referred to criminal prosecution authorities, 2004-2014



The breakdown of the 400 money laundering convictions following a suspicious activity report forwarded by MROS to criminal prosecution authorities between 2004 and 2014 indicates the significance of the threat associated with banking and money transmitters (Figure 32).

Figure 32: Number of money laundering convictions following a suspicious activity report forwarded to criminal prosecution authorities, by business sector, 2004-2014



Most money laundering convictions in Switzerland that follow a suspicious activity report filed by banks or by asset managers and fiduciaries are in relation to fraud (including computer fraud), misappropriation and criminal mismanagement or, less frequently, participation in a criminal organisation. Convictions following a suspicious activity report from a money transmitter are in most cases related to drug trafficking or computer fraud. The few convictions linked to the insurance sector are mainly in relation to participation in a criminal organisation, while most of those concerning casinos are in relation to drug trafficking and misappropriation or criminal mismanagement.

7.1.1 Banks

Context

Switzerland's political and economic stability makes the financial services offered by its banks lastingly attractive to a diversified client base, with the banking sector holding a prominent global position across all financial activities[116]. Banking is an important element of the Swiss economy: in 2014, the gross value added generated by the financial sector as a whole made up 10.2% of the entire Swiss economy, and almost half of that came from banking. In terms of employment, 5.9% is generated by the financial sector, of which two thirds is in banking[117]. A large proportion of those working in banking are based abroad. This high rate of internationalisation in the banking sector depends largely on the global economy. Since 2010, the number of branches and representative offices of Swiss banks abroad with respect to the total number of banks in Switzerland has remained stable; in absolute terms, however, the number of banks operating in Switzerland has declined steadily since 2013[118].

Switzerland is home to two world-class financial centres whose levels of competitiveness and capacity rank them among the ten leading financial centres worldwide[119]. In 2012, total assets under management by the Swiss financial sector amounted to CHF 5,565 billion, corresponding to around 8.9% of worldwide assets under management. Given its close correlation with the global economic situation, this volume increased by more than 10% in 2013 to a total of CHF 6,316 billion.

Table 8: Growth in assets under management by the Swiss financial sector in 2008-2013 in CHF bn

	2008	2009	2010	2011	2012	2013
Assets under management	5,400	5,600	5,476	5,246	5,565	6,316

[116] World Bank, Worldwide Governance Indicators 1996-2012
[117] Federal Statistical Office (FSO) 2014, Swiss Bankers Association (SBA): Der Finanzplatz Schweiz und seine Bedeutung 2012
[118] Swiss National Bank (SNB), 2014
[119] The Global Financial Centres Index 15, 2014

Year-on-year change	-23.7%	+3.7%	-2.2%	-4.2%	+6.1%	+13.5%

Sources: Swiss National Bank (SNB) 2014; Swiss Bankers Association (SBA) 2013

Aside from its volume of assets under management, placing Switzerland among the world's leading financial centres, the banking sector also holds a large market share in cross-border wealth management. Indeed, many of Switzerland's wealth management banks focus their business model on providing cross-border services to private clients domiciled in other countries[120]. A review of the figures since 2008 shows a long-term increase in cross-border wealth under management in absolute terms. This volume stabilised in 2013 at CHF 2,300 billion, corresponding to around a quarter of total cross-border wealth under management worldwide (Table 9).

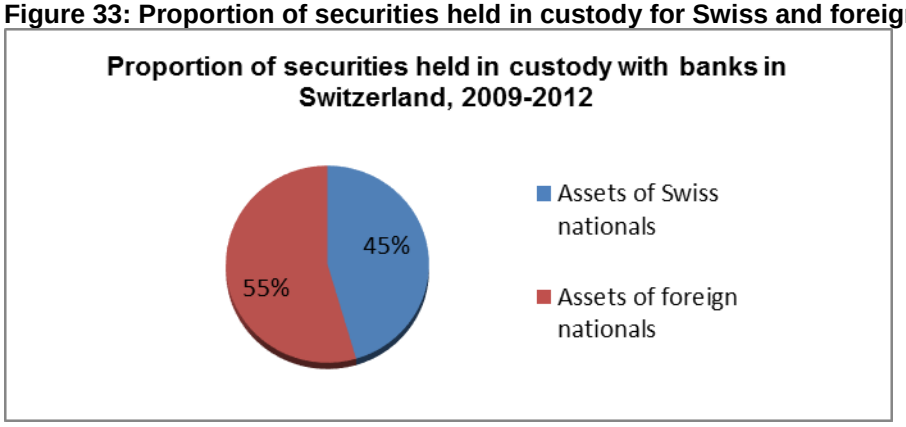
Table 9: Growth in cross-border wealth under management by the Swiss financial sector in 2008-2013

	2008	2013
Cross-border wealth under management in CHF bn	1,710	2,300

Source: Swiss National Bank (SNB), Swiss Bankers Association (SBA) 2013, The Boston Consulting Group 2014

Between 2009 and 2012, some 55% of the securities deposited with a Swiss bank belonged to foreign clients (Figure 33). In 2012, equities, bonds and collective investment schemes accounted for 95% of all assets held in Swiss custody accounts[121]. In 2009, two thirds of fixed-term deposits were held by foreign clients.[122]

Figure 33: Proportion of securities held in custody for Swiss and foreign nationals, 2009-2012



Source: Swiss National Bank (SNB) 2009-2012

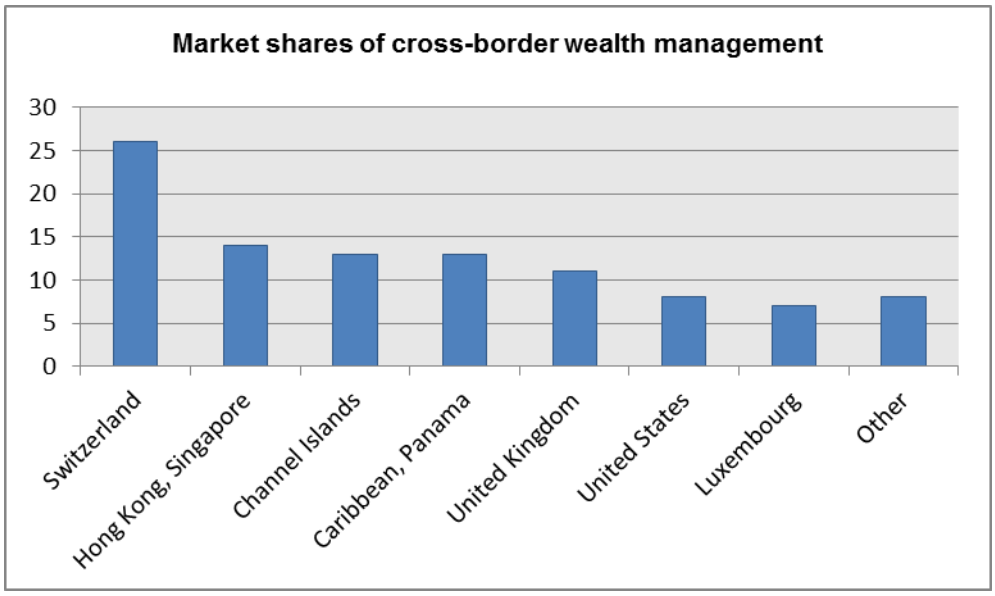
While there is a general uptrend internationally in the proportion of cross-border assets under management, Switzerland has stabilised its position in cross-border wealth management at a very high level (Figure 34).

Figure 34: Comparison of market shares of cross-border wealth management in international financial centres, 2012

[120] Statement by FINMA on the legal and reputational risks in the context of cross-border financial activities 2010

[121] Swiss Bankers Association (SBA), Wealth management – at a global level and in Switzerland 2013, p. 17

[122] Swiss Bankers Association (SBA), Wealth management – at a global level and in Switzerland 2011, p. 15



Source: Boston Consulting Group 2013

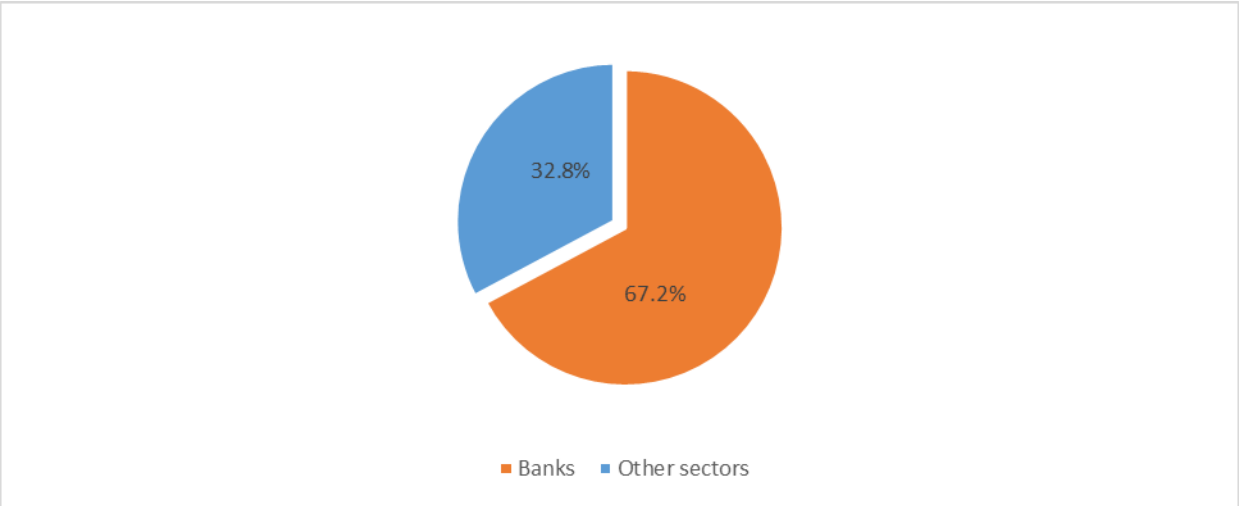
The Swiss banking sector still has substantial capacity to absorb and manage funds held by non-residents. The nature of cross-border management makes the banking sector vulnerable to being used for money laundering purposes. Cross-border management entails a dispersion of financial activities over various jurisdictions, i.e. the place of management, the place of residence of the person depositing the assets, and the financial instruments used. Using the powers delegated by clients residing abroad, the banks thus act as asset managers, performing various financial services in the name of and for the account of their clients, sometimes also by way of external intermediaries based in the client's country of domicile. In this type of management, the identification and continuous verification of the true BOs become more challenging, hampering efforts to detect and stop money laundering activities. This vulnerability is exacerbated by the diversification of financial activities carried out by clients and the financial institutions themselves, the multiplication of financial intermediaries involved, and the regulatory disparity between the legislation of different jurisdictions applicable to banks. In this respect, institutions with branches located abroad and foreign banks with branches in Switzerland have to manage the risks inherent to cross-border activities and implement a coordinated and cohesive system for combating money laundering and terrorist financing, while still complying with the various regulations applicable to the foreign jurisdictions concerned[123].

Key role of the banking sector in combating money laundering and terrorist financing

In Switzerland, all institutions holding a banking licence are subject to the provisions of the AMLA by virtue of Article 2 paragraph 2 of the AMLA. The significance of the threat of this sector being used for money laundering and terrorist financing purposes is reflected in the number of suspicious activity reports submitted MROS by banks between 2004 and 2014, i.e. 8,224 out of a total of 12,224 reports (Figure 35). The high number of reports filed by the banking sector is also due to increased risk awareness and the substantial resources devoted by the sector to identifying suspicious relationships or transactions.

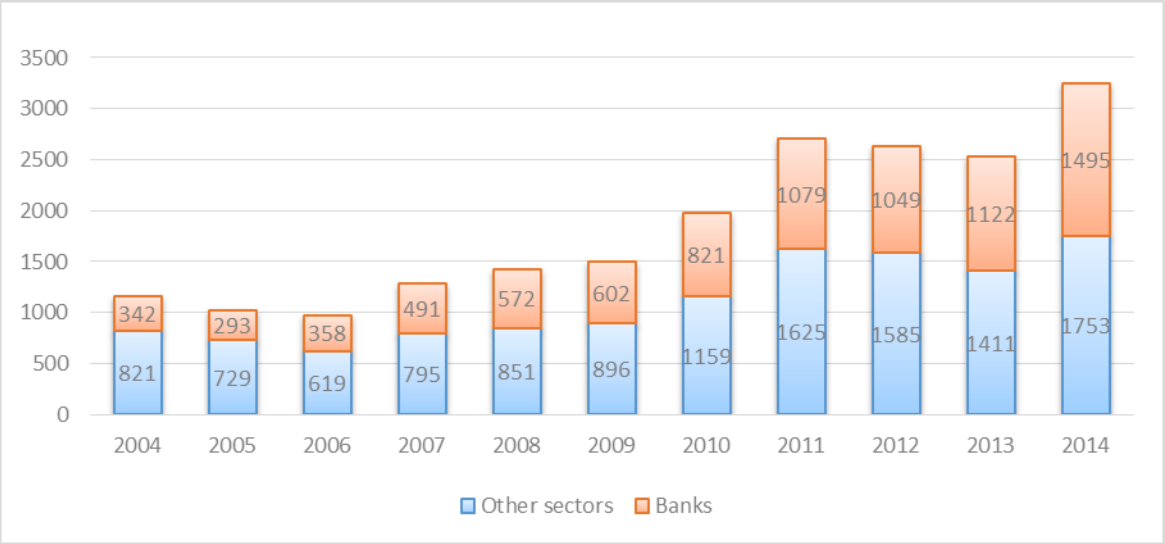
Figure 35: Proportion of suspicious activity reports originating in the banking sector, 2004-2014

[123] Swiss Bankers Association (SBA), Wealth management – at a global level and in Switzerland 2011, pp. 18-19



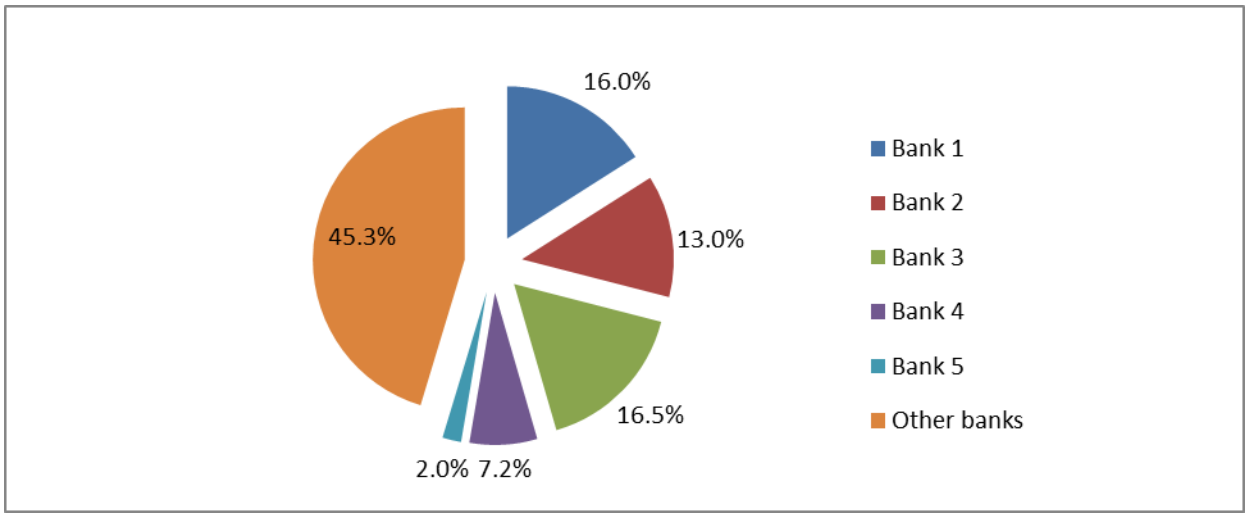
The dominant position of the banking sector in combating money laundering and terrorist financing is also evident in the growing proportion of suspicious activity reports filed by banks in comparison to the rest of the financial sector (Figure 36). This increase reflects the seriousness of the threat facing the sector, but also the extent of the resources deployed to detect suspicious cases and the sector's analytical capabilities.

Figure 36: Growth in the number of suspicious activity reports originating in the banking sector, 2004-2014



Of the 344 banks licensed by FINMA in 2014, five accounted for 54.7% of all the suspicious activity reports submitted. The high number of suspicious activity reports from these five institutions corresponds in many respects to their size in terms of turnover and market share. The remaining 45.3% of reports came from 179 banks (Figure 37).

Figure 37: Breakdown of suspicious activity reports within the banking sector, 2004-2014



An analysis of the due diligence activities by those banks accounting for some 45% of the suspicious activity reports filed with MROS gives an indication of the extent of the mechanisms for identifying suspicious relationships and the transaction monitoring tools set up by the sector as a whole to mitigate the risk of money laundering and terrorist financing in banking and for the Swiss financial sector in general.

At the same time, a more detailed analysis of the work involved in detecting and reporting to MROS by three of the five banks mentioned above illustrates the Swiss system for combating money laundering and the crucial role of financial intermediaries. The latter are an integral part of the system and bear huge responsibilities in this respect. It is the financial intermediaries who carry out detailed checks on their clients and the transactions performed. Highly efficient computerised verification systems have been set up to cross-check clients' names at regular intervals against various databases furnishing open-source information (World-Check, Factiva, etc.), thus detecting any names appearing in sanctions lists, ongoing criminal proceedings or convictions entered. If a match is found, the transactions of the clients in question are automatically blocked. Transactions are also monitored constantly by internal control systems. As a rule, clients are classified according to their business activity, domicile, status (e.g. PEP or relatives of a PEP) or assets. Each client is thus assigned a risk profile, which is recorded in the system. Therefore, if a client's transactions exceed a certain threshold defined by the bank, the case is reported to the Compliance department.

All cases detected are examined by the compliance officers, who clarify the client's position under the AMLA. The client's dossier is scrutinised so as to determine, for example, the plausibility of the transactions in question. Following this, the bank decides which cases constitute a situation that it is obliged to report to MROS. Cases not submitted under the duty to report (mandatory suspicious activity reports) are generally done so under the bank's right to report (voluntary suspicious activity reports).

Thus, the reports received by MROS have already passed an initial filter set up by the Swiss legislator with the financial intermediary, which is subject to supervision by FINMA. As a result, cases originating in the banking sector are of good quality. This is reflected in their high referral rate by MROS to the criminal prosecution authorities, as well as the high number of court convictions.

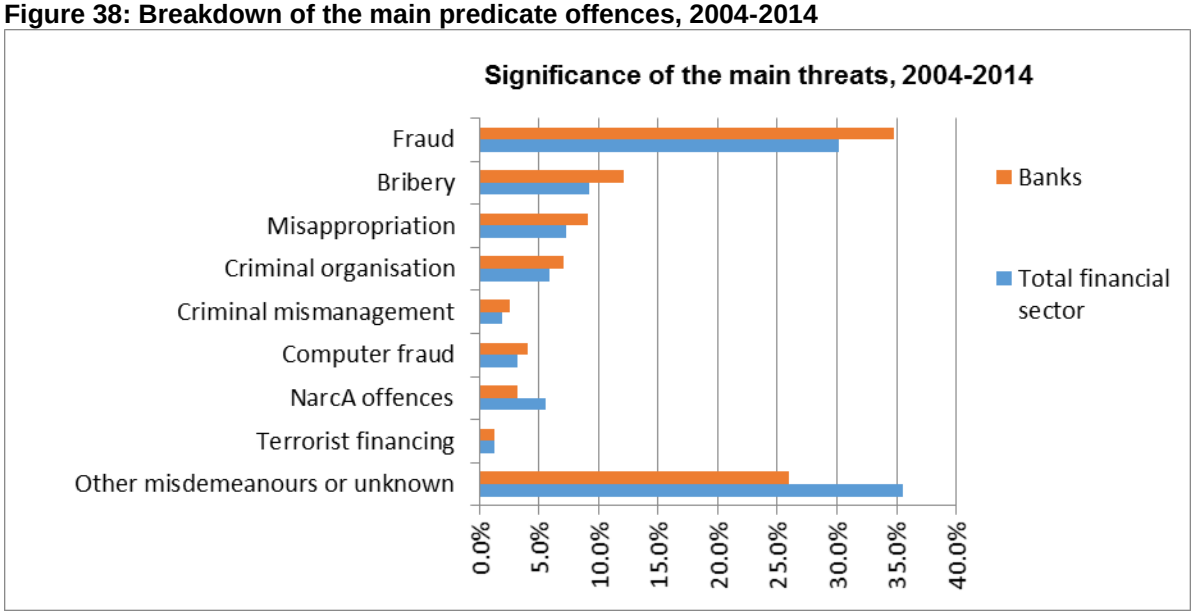
Table 10 (below) shows the Swiss system in operation, the objective being to raise the awareness and responsibility of all those involved, whether in the public or private sector, in a joint effort to combat money laundering and terrorist financing. These figures relate to the three banks filing the most suspicious activity reports with MROS in 2012 and 2013 (Figure 35).

Table 10: Filtering performed by the three banks submitting the most suspicious activity reports, 2012-2013

Year	Total number of transactions carried out by the three banks	Number of suspicious transactions analysed by the three banks	Number of SARs filed with MROS after analysis
2012	1.9 bn transactions	45,000 red flags	494
2013	2 bn transactions	47,000 red flags	511

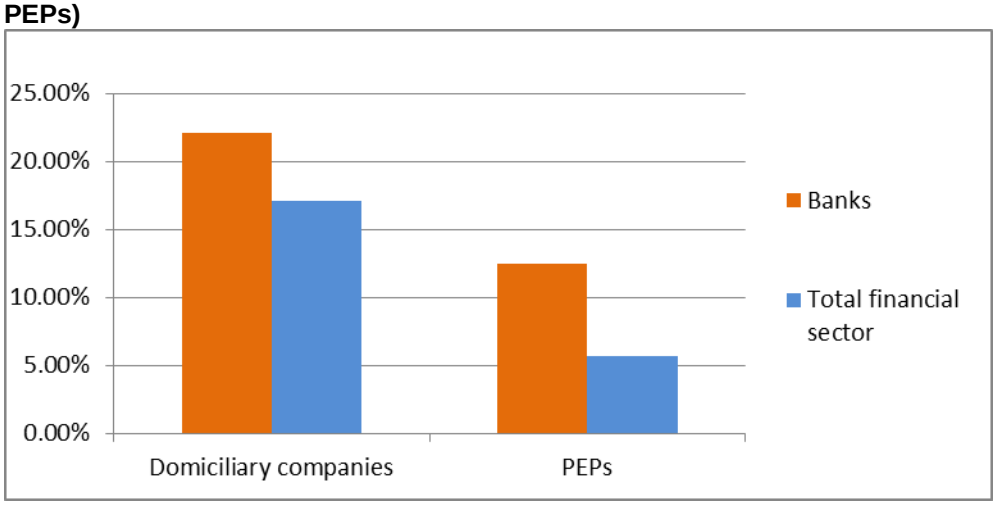
The banking sector is exposed to all predicate offences to money laundering as well as the threat of terrorist financing (Figure 38). Regarding the main threat factors, i.e. fraud, bribery and misappropriation as well as participation in a criminal organisation, the banking sector is more exposed than other sectors. However, with its sophisticated mechanisms to analyse and identify the risks, the banking sector is better placed than others to detect suspected predicate offences.

Figure 38: Breakdown of the main predicate offences, 2004-2014



Compared with the financial sector as a whole, banking sector clients pose a higher risk of using complex legal structures such as domiciliary companies and trusts. Also, bank clients include a higher proportion of PEPs (Figure 39).

Figure 39: Complexity of the business relationships reported (domiciliary companies and PEPs)



Risk factors

A risk assessment for the banking sector will depend on the nature of the banking activities performed by the various institutions and their respective clients. To this end, FINMA uses a range of risk factors to assess each bank's overall risk.

For private clients, the first risk factor is the total wealth under management. The money laundering process in this case seeks to maximise the volume of funds to be laundered rather than dividing them up. With regard to commercial clients, the risk is higher for unlisted companies, as these have lower levels of transparency and supervision than companies listed on a stock exchange. However, the risk is lower in the case of local companies operating in Switzerland than with foreign companies, for which information is more difficult to obtain.

All of the banking institutions offer each client a standard range of basic services such as account maintenance, payment services and credit/debit card services. The risk associated with such basic services increases only in relation to the number of other, more specific services the bank may offer a client. Similarly, credit services and transactions generally pose very little risk. For these, banks systematically perform additional checks, thereby reducing the sector's vulnerability in relation to such activities.

On the other hand, the risk posed by finance for international trade and exports is moderately high. Banks offering such services are more exposed to business relationships involving high-risk countries, particularly with regard to commodity trading. The main risk lies in the bank potentially being used to launder assets, i.e. on the basis of counterfeit or falsified securities, or to circumvent internationally imposed sanctions. As with other credit transactions, however, the risk can be mitigated by banks conducting additional systematic checks so as to minimise their financial and reputational risks.

As regards services that offer clients more discretion, the availability of numbered accounts and hold mail services constitutes a high risk for the sector. A request for discretion would suggest that the client wishes to avoid complete transparency, which may point to a possible criminal origin of at least some of the assets transferred using these services. Similarly, the sector faces a high risk in opening accounts and managing assets on behalf of legal structures such as foundations, domiciliary companies and trusts domiciled in offshore centres. Given that such structures are so easy to set up, their use in wealth management may be perfectly legitimate. On the other hand, assets of criminal origin are typically laundered using such legal structures. They offer a greater possibility of concealing the BO's identity and the origin of the associated assets, especially when these are transferred in stages across different legal structures and several jurisdictions, thereby facilitating fast transnational transactions involving large sums of money.

A higher risk is also incurred by some banks offering transitory accounts for foreign correspondent banks[124]. This risk is based on the different standards used for transactions and the lack of transparency regarding the identity of the parties involved in transactions carried out this way.

For the purpose of supervision, FINMA classifies banks into three major risk categories, based on the different activities carried out by the bank in question:

Category 1 (universal banks): High risk
This category covers banks that offer a complete range of banking services in Switzerland and abroad, including retail banking services and cross-border private banking, institutional asset management and international trade finance. These are invariably large banks (corresponding to at least the size of FINMA's category 3 banks)[125]. As regards wealth management, these banks have a large number of very wealthy clients with global financial operations requiring complex financial services, i.e. ultra-high-net-worth individuals (UHNWI), as well as many relationships involving PEPs. Due to their central position within the Swiss financial sector, the banks in this category also have other banks as clients, which then carry out transactions for their own account as correspondent banks. The high number of all sorts of private and commercial clients using standardised services along with UHNWI services poses an ongoing challenge for the Compliance departments of banks in this category, which are responsible for adherence to due diligence obligations, a task requiring huge coordination and technical resources.

Category 2 (private banking): Medium-to-high risk, depending on whether concentrating on the domestic or international market
This category concerns banking activities associated with wealth management for high-net-worth clients, i.e. private banking, often with the use of domiciliary companies and other legal structures. Furthermore, in managing such large fortunes, the banks in this category also operate in securities trading, whether for their own account or that of their clients. Some banks in this category have a mainly international client base, with variations in terms of origin and domicile, their clients' status (e.g. PEPs) and the extent of their transnational financial activities (cross-border private banking).

Category 3 (retail banks): Low-to-medium risk, depending on the type of client (retail banks: low risk) and products (international trade finance: medium risk)

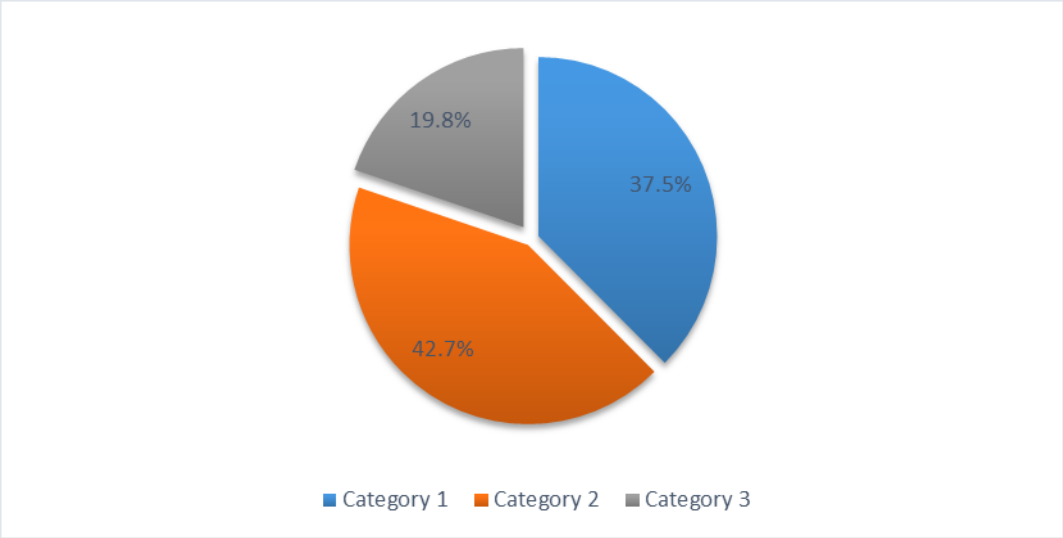
[124] Cf. Article 12 paragraph 3 of the AMLO-FINMA
[125] FINMA Circular 2011/2 "Capital buffer and capital planning – banks"

This category comprises banks in Switzerland offering standardised banking services (retail services) to private and commercial clients, mainly within Switzerland, such as payment services, business loans, consumer loans, mortgages and pension-related services. In 2014, around one third of banks subject to the AMLA in Switzerland fell under this category. Furthermore, a certain number of banks in this category also operate in trade finance.

Assessment of the real threat (based on suspicious activity reports)

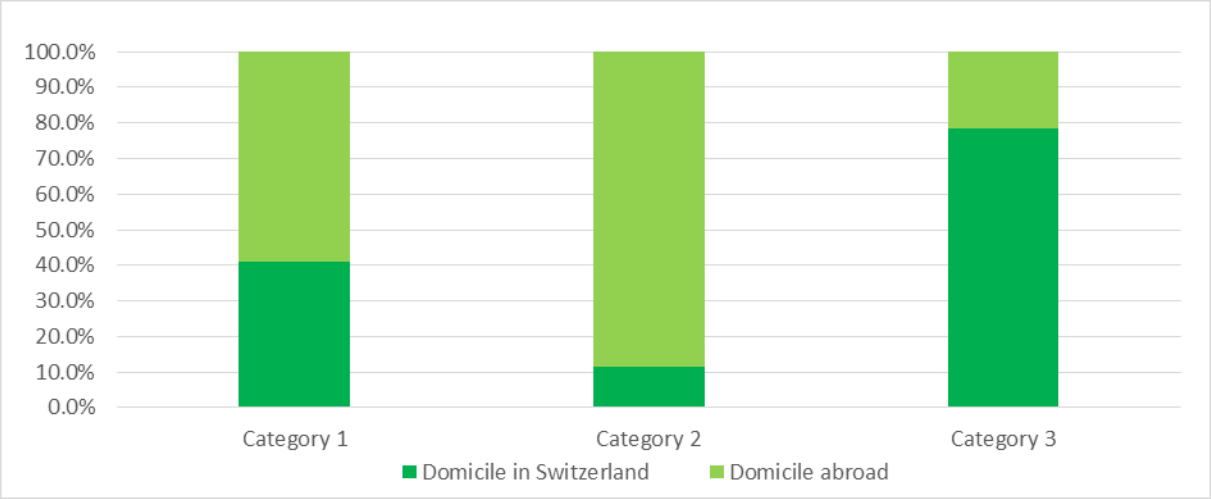
During the period under review, category 2 and 3 banks submitted significantly more suspicious activity reports than the other categories (Figure 40), largely explained by their size in terms of assets under management and market share.

Figure 40: Breakdown of suspicious activity reports submitted by the banking sector by risk category, 2004-2014



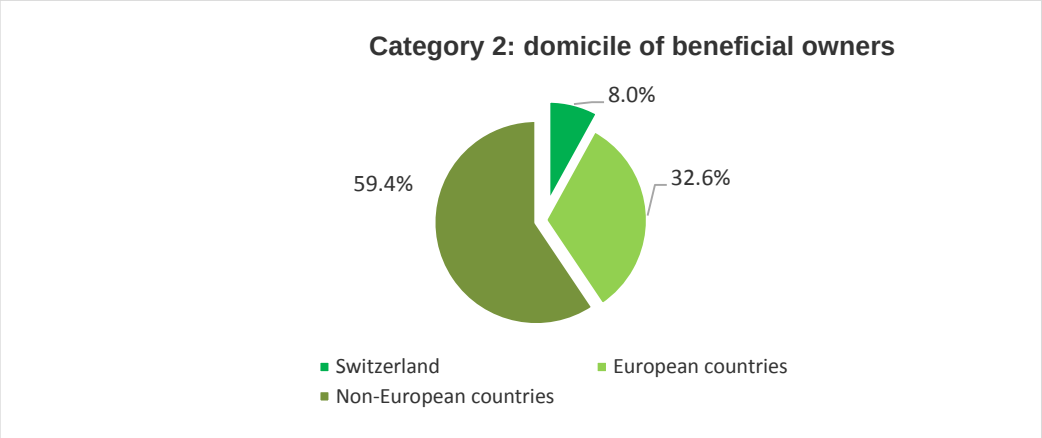
For category 2 banks, the vast majority of contracting parties concerned by suspicious activity reports have their legal domicile outside of Switzerland, often in a neighbouring country, i.e. Italy, France and Germany, or another European country (Figure 41).

Figure 41: Breakdown of the domicile of contracting parties by bank category, 2004-2014



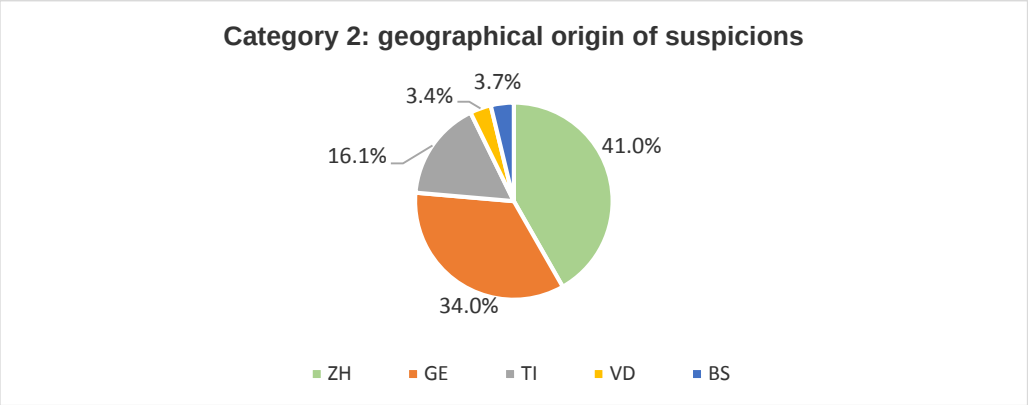
For category 2, most of the BOs concerned have their domicile outside of Europe (Figure 42). Foreign-controlled banks and branches of foreign banks in this category have a higher proportion of contracting parties and BOs domiciled outside of Europe. It is interesting to note that statistics from the Swiss National Bank also indicate an upward trend in the general flows from these regions.

Figure 42: Breakdown of the domicile of beneficial owners for category 2 banks, 2004-2014



Geographically, the cases reported for category 3 banks are distributed across all cantons. For categories 1 and 2, the cases reported tend to be concentrated in the financial centres of the cantons of Zurich, Geneva, Ticino, Vaud, Basel Stadt and Zug (Figure 43). Among the reports filed by category 2 banks, foreign-controlled banks and branches of foreign banks based in the canton of Geneva represent a particularly high proportion of reports submitted. In comparison, the number of reports filed by foreign-controlled banks or branches of foreign banks based in the canton of Ticino[126] is lower.

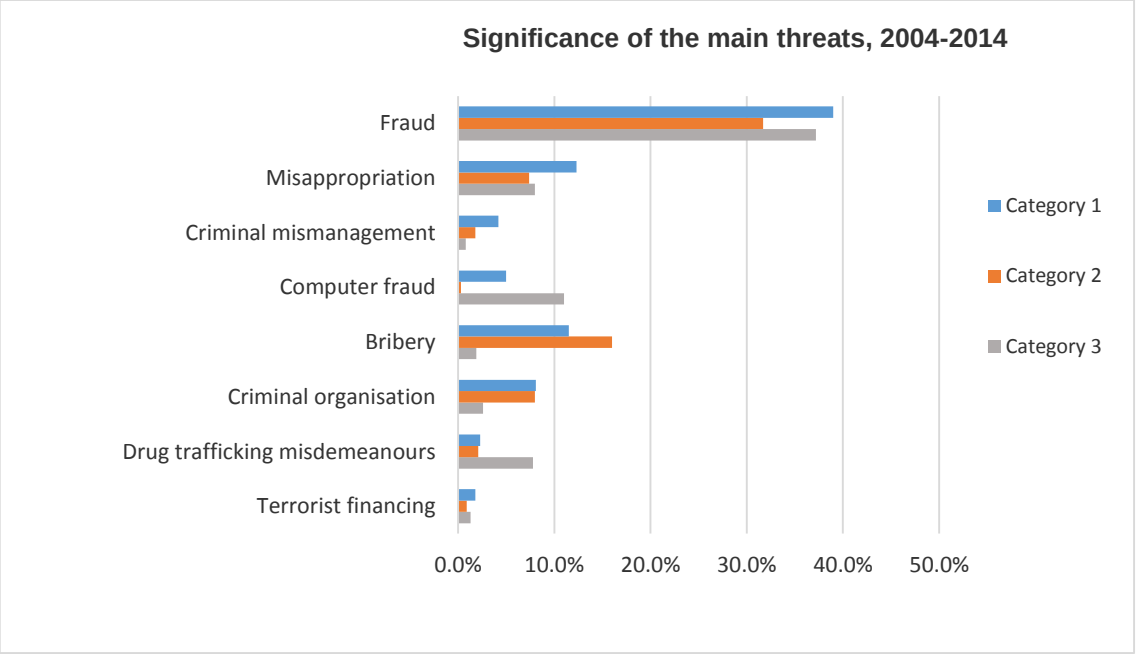
Figure 43: Breakdown of the geographical origin of suspicions within category 2 banks, 2004-2014



The three categories of banks also differ with regard to predicate offences. As with the financial sector as a whole, instances of money laundering associated with fraud or computer fraud pose the greatest threat to the banking sector, with banks in categories 1 and 3 most exposed to this risk. The threat of property predicate offences, primarily misappropriation and criminal mismanagement, which is more international in nature, is highest for category 1 banks. The risk of money laundering in association with acts of bribery is higher for category 2 banks, as is the risk of organised crime, which also concerns category 1 banks. The laundering of assets obtained through drug trafficking felonies committed in Switzerland mainly concerns category 3 banks (Figure 44).

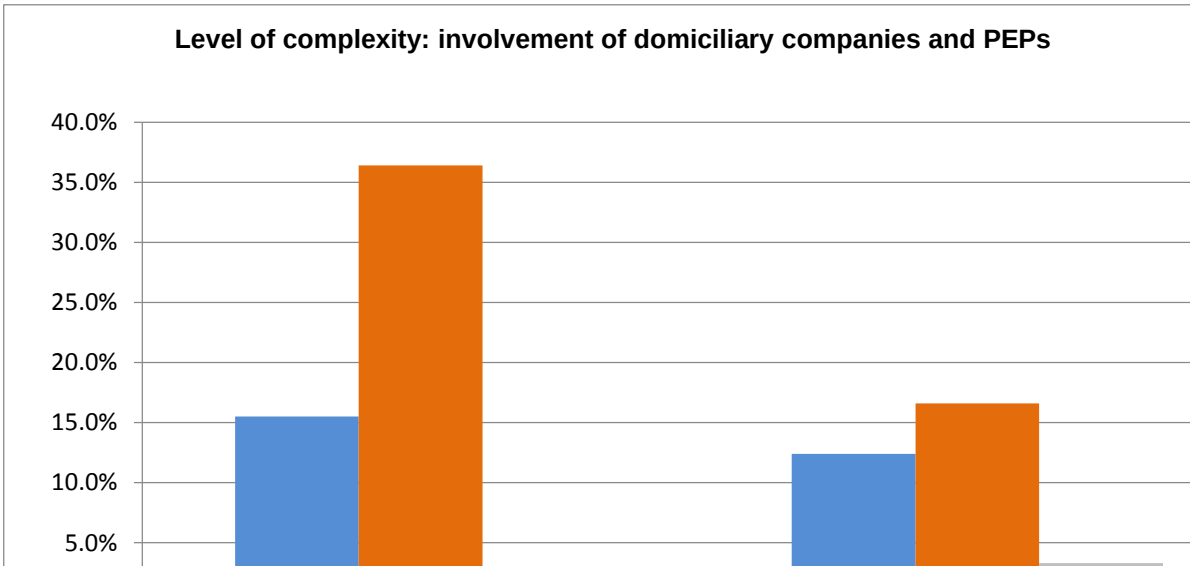
Figure 44: Breakdown of the main predicate offences by bank category, 2004-2014

[126] La piazza finanziaria ticinese, Associazione bancaria ticinese 2014



Regarding the involvement of domiciliary companies and PEPs in business relationships reported as suspicious, category 2 banks face the greatest risk, which is slightly higher for foreign-controlled banks or branches of foreign banks. Category 1 banks present a mixed picture regarding the risk associated with complex structures, while category 3 banks face a limited risk (Figure 45).

Figure 45: Complexity of the business relationships reported by bank category



In keeping with the huge resources deployed to detect suspicious cases and lower the sectoral risk, all three categories of banks have sophisticated detection systems, revealing a range of potential sources and grounds for suspicion, including those that require further checks of the economic background of clients. Categories 1 and 3 tend to find grounds for suspicion in the manner and means of payment, such as cash deposits or payments by cheque and the use of certain accounts such as transitory accounts. Category 2 banks more frequently mention media reports as their grounds for suspicion. For foreign-controlled banks or branches of foreign banks, the most common grounds for suspicion are in association with high-risk countries.

Typologies

A. A bank learned from a newspaper article that the father of one of its clients, a PEP, had been accused of bribery in a South American country. This businessman was suspected of accepting bribes in awarding public contracts in the oil business. Although the bank's client was not mentioned in the open sources available, the bank found some correlations between the information drawn from media

reports and its own transaction monitoring. It noted large inflows over a short period of time, deposits made by offshore companies and links to another person involved in the bribery case mentioned in the media. The analysis by MROS found that most of the funds credited to this relationship had been transferred to other accounts, the BO of which was the PEP's son. The bank thus suspected its client of acting as a straw man for his father. MROS forwarded the report to the Office of the Attorney General of Switzerland. An investigation covering several reports on the same case is ongoing.

B. The company X SA noted that it had made unexplained payments amounting to almost CHF 80,000 in favour of A, a person unknown to the company. In an attempt to clarify the situation, X SA informed A's bank of the account irregularities found. Further research by the bank revealed that some of the funds credited to A's accounts were transferred to an account held by B, a former accountant of X SA. Upon examining the account-opening documentation for both relationships, the bank concluded that B had opened an account in A's name and unlawfully transferred funds belonging to X SA, for whom she worked. The bank reported both relationships to MROS. The analysis by MROS revealed that B had committed similar acts a number of years beforehand in another country. The criminal prosecution authorities convicted A for repeated misappropriation, document forgery and money laundering.

C. In the late 1990s, a bank opened a business relationship in the name of a foreign organisation with the stated objective of assisting and supporting people affected by civil war or natural disasters. A number of years later, a systematic search carried out online and in other databases by the financial intermediary found that the organisation had embezzled funds to finance a movement that was on the official list of terrorist organisations. Moreover, MROS found that the leaders of the organisation were wanted by Interpol. As the Office of the Attorney General of Switzerland had already launched an investigation with regard to the terrorism-related facts, this report was forwarded and merged with the ongoing proceedings. The case is pending.

D. Person A contacted a close acquaintance B in relation to his intended purchase of a newspaper operation. In his letter, A said that he already had CHF 25,000 but that he needed another CHF 20,000. To enable him to make this purchase, B agreed to lend A CHF 10,000. The interested parties signed a partnership agreement, and B transferred the agreed funds to A's personal account. B subsequently learned from the media that the newspaper in question had not been for sale and contacted A's bank. The financial intermediary confirmed that A's account had indeed been credited with the sum of CHF 10,000 from B and that the funds had subsequently been quickly withdrawn in cash. The case was reported to MROS and then forwarded to the appropriate cantonal prosecution authorities. A was found guilty of fraud under Article 146 paragraph 1 of the Swiss Criminal Code.

E. The business relationship of company X, based in Switzerland and affiliated with group Y, was reported to MROS. The bank learned from newspaper reports that group Y was suspected of having orchestrated a large-scale case of VAT carousel fraud. According to reports, a large number of shell companies had been created and then liquidated to enable the sale of oil products, invoicing the VAT to domestic buyers but not declaring it to the tax authorities. It was reported that the director of company X was at the head of the entire operation and that criminal proceedings were ongoing against several persons abroad. Following enquiries with its counterparties abroad, MROS was able to narrow down its analysis and confirm the suspicions against company X. This new information led to MROS forwarding the case, initially closed, to the Office of the Attorney General of Switzerland. A preliminary investigation is now under way.

Assessment

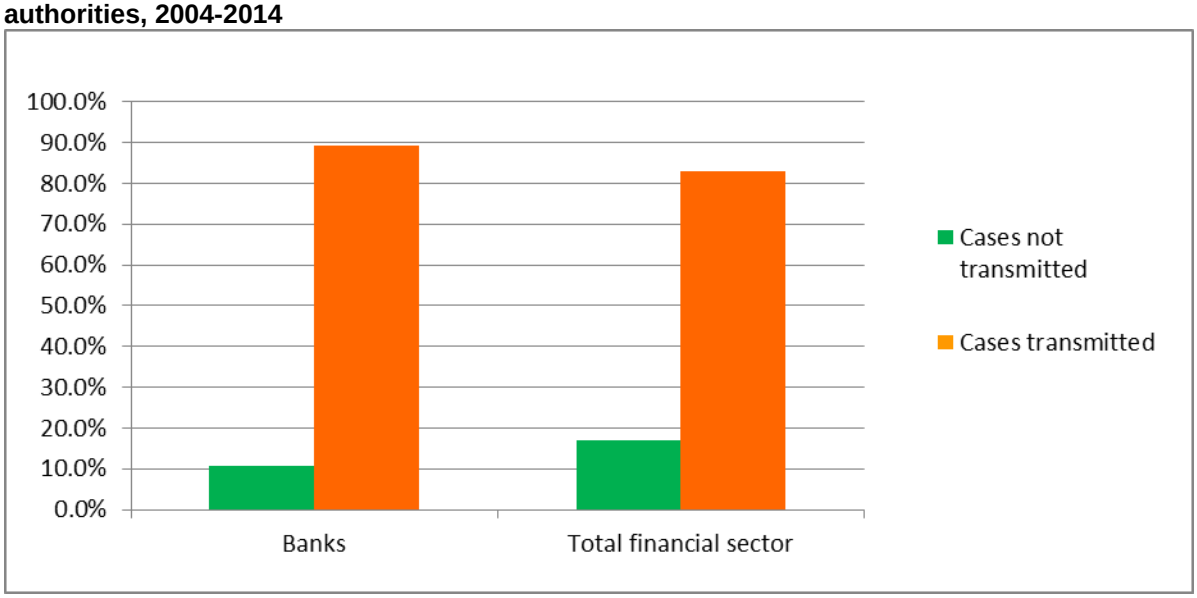
The banking sector's due diligence obligations are clearly defined in a set of binding rules, in the Agreement of 2008 on the Swiss Banks' Code of Conduct with regard to the Exercise of Due Diligence (CDB 08) and in the AMLO-FINMA. These rules govern, among other things, the conditions for verifying the identity of contracting parties and identification of the BO of assets and of legal entities, including legal structures, irrespective of their nature and place of incorporation, such as domiciliary companies, trusts and other fiduciary companies, corporations (corp.) and limited liability companies (LLC) (Art. 2, 3 and 4 of the CDB 08, Art. 12 para. 2 letter h of the AMLO-FINMA). In the special case of a trust, for which the BO cannot be formally identified because no single party has complete power over the assets, e.g. a discretionary trust, the bank must research and document the parties likely to be the true BO (point 43 para. 1 of the CDB 08). Their obligations regarding document retention are also clearly set out in the regulations and guarantee an appropriate paper trail.

In all cases, business relationships with PEPs are deemed to pose a higher risk (Art. 12 para. 3 of the AMLO-FINMA). In this respect, banks having a relationship with a foreign PEP are obliged to carry out additional clarifications regarding the origin of the client's wealth and the assets deposited, and to verify and document the plausibility of the economic background of any significant inflows.

As operating a bank requires a banking licence from FINMA[127], banking institutions are subject to FINMA's prudential supervision, depending on the risks facing creditors, investors, insured parties and the Swiss financial centre as a whole. Through this prudential supervision, together with its supervision of adherence to obligations, FINMA gains in-depth knowledge about the banks under its supervision, thereby reducing the risk of insufficient vigilance of money laundering and terrorist financing for the entire sector. Regarding FINMA's supervision of the banks' due diligence obligations in money laundering, audit firms play an essential role, with the responsibilities and minimum standard audit strategy defined by FINMA[128]. For each institution, FINMA determines the oversight concepts and the intensity of such oversight, depending on the specific risk factors applicable to the banking institutions concerned and the size of the banking institution. In addition to checking all the due diligence obligations, the following aspects should also be closely monitored each year: identification of the contracting party and the BO of new business relationships, periodic checks of existing relationships posing higher risks, e.g. PEPs, transactions with financial intermediaries that do not use a computerised transaction monitoring system. Effective since 2014, audit firms receive detailed audit standards to be implemented. Within the context of its risk-based oversight, FINMA has additional instruments at its discretionary disposal to verify banks' adherence to their due diligence obligations, e.g. supervisory reviews, which may include onsite audit visits, carried out independently by FINMA. In the case of a serious and long-standing breach of due diligence obligations, FINMA has a range of enforcement measures at its disposal to restore legal order, which may go as far as withdrawing the banking licence and banning a bank from operating.

Despite the seriousness of the threat, the various control mechanisms established by banking institutions and the risk-based regulatory framework play a decisive role in mitigating the risks of money laundering and terrorist financing for the Swiss financial sector as a whole, contributing to the efficiency of efforts to combat money laundering and terrorist financing in Switzerland. Thus, for the banking sector, the referral rate of suspicious activity reports to the criminal prosecution authorities is higher than for the other sectors (Figure 46).

Figure 46: Percentage of suspicious activity reports forwarded to criminal prosecution authorities, 2004-2014

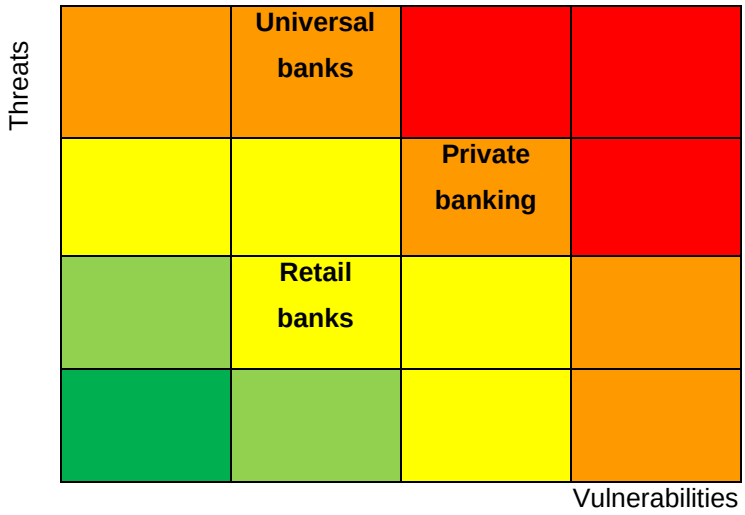


Suspicious activity reports submitted by the banking sector resulted in 231 money laundering convictions between 2004 and 2014, representing 57% of all convictions entered in Switzerland on the basis of suspicious activity reports. Faced with a serious threat, it must be said that the banking sector – with a range of internal and external measures to combat money laundering, taking a risk-based approach, implemented by the banks and the oversight authorities – is capable of reducing quite substantially the money laundering risks inherent to this sector. In this manner, and given their central role, the banks contribute significantly to lowering the risks of money laundering and terrorist financing in the Swiss financial sector.

[127] The minimum conditions for obtaining such a licence are set out in the BankA, specifically in Article 2 paragraphs 2, and in the SESTA and the associated ordinances

[128] FINMA Circular 2013/3 on Auditing

Regarding the financial services offered by banks in Switzerland, the mechanisms to combat money laundering and terrorist financing will be supplemented by the implementation of new legislative provisions introduced with the revised FATF recommendations, particularly measures to improve the transparency of legal entities, tighter obligations for financial intermediaries to identify the physical BOs of legal entities, and an extension of the definition of PEPs to also include domestic PEPs and PEPs of intergovernmental organisations. Therefore, in light of the provisions and controls provided under the AMLA, which are applicable to all players in the sector, and given the density of the checks performed by the banks themselves, the vulnerabilities of this sector are appropriately addressed and do not require any additional measures.



7.1.2 Securities dealers

In Switzerland, any natural persons or legal entities trading in securities on a professional basis are deemed to be financial intermediaries as defined in the AMLA (Art. 2 para. 2 letter d of the AMLA, FINMA Circular 2011/1 on Financial Intermediation under the AMLA and Art. 5 para. 3 of the PFIO). In 2014, there were 71 independent dealers falling under this category. These financial intermediaries trade primarily in listed financial instruments, whether for their own account or for the account of others and, to this end, may create and offer derivative financial products. In principle, financial intermediaries operating exclusively in securities trading for their own account run a low risk of being used for money laundering purposes. However, the risk is higher where they perform trading operations for the account of third parties and with respect to the nature of the financial instruments traded, particularly their degree of regulation. The risk is lessened where financial transactions associated with trading are performed across a number of different banking institutions and each one deploys adequate resources to meet its due diligence obligations.

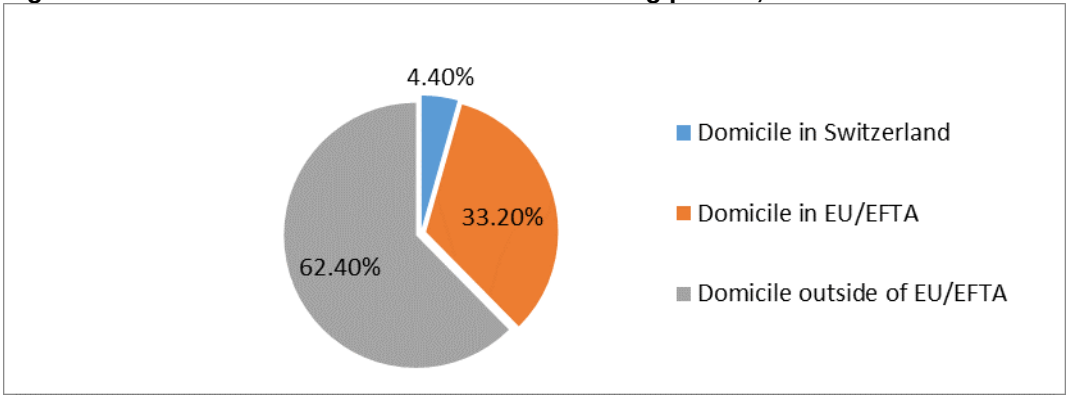
In the interests of market integrity, the standard stock exchange system in Switzerland is subject to a set of regulations and self-regulatory requirements, all of which lower considerably the risk of money laundering by verifying the economic plausibility of transactions (Art. 5 of the SESTA)[129]. In principle, based on current regulations, each transaction in listed securities is entered in the order book kept by the stock exchange and also in the dealer's securities journal (Art. 5 para. 2 and Art. 15 paras. 1 and 2 of the SESTA and also FINMA Circular 2008/4 on Securities Journals). The regulations also comprise an obligation on the dealer to disclose any listed securities traded off the official stock exchange or prior to their being fully paid up in the case of shareholdings of at least 3% (FINMA Circular 2008/4, Margin no. 22). Furthermore, securities dealers are required to record in the order book the ordering party of the transaction (FINMA Circular 2008/4, Margin no. 38). According to their due diligence

[129] In Switzerland, the standard stock exchange is a public limited company with the name SIX Swiss Exchange SA. It is subject to supervision by FINMA, which specifies the code of conduct on the market in its Circular 2013/8. The stock exchange has an autonomous body that verifies adherence to the regulations and may issue sanctions in the event of any breaches of the rules (SIX Exchange Regulation).

obligations under the AMLA, they must know the identity of the BO of the transactions carried out (Art. 32 of the AMLO-FINMA), thereby guaranteeing the paper trail.

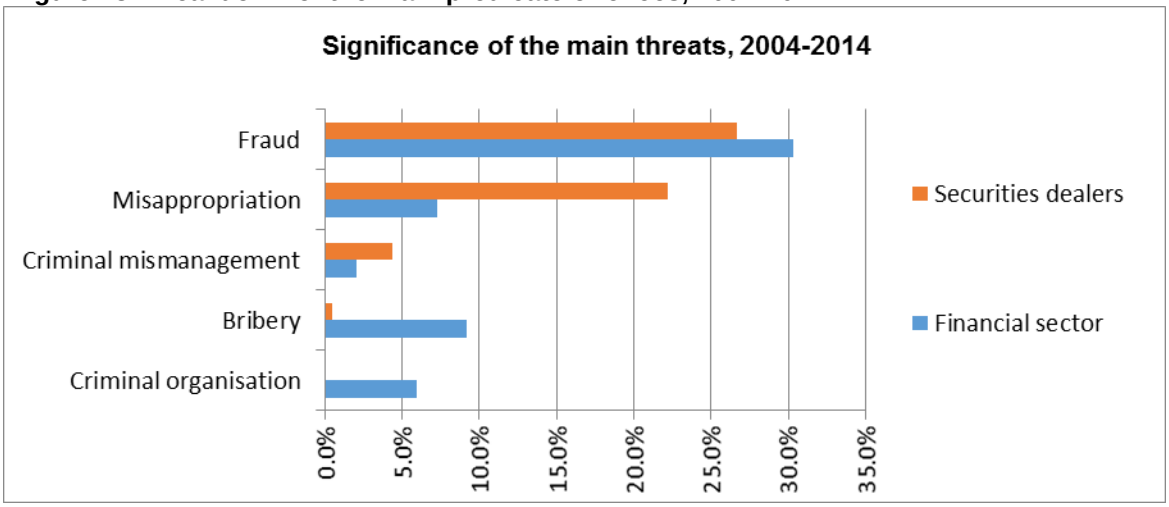
The number of suspicious activity reports filed with MROS by the sector between 2004 and 2014 is quite low. Two thirds of reports originated from the financial centres of Geneva and Zurich. The vast majority of BOs associated with suspicious activity reports are domiciled abroad, with a particularly high proportion outside of Europe (Figure 47). In 22.2% of cases, the contracting party was a domiciliary company.

Figure 47: Breakdown of the domicile of contracting parties, 2004-2014



Of the suspected predicate offences, the most frequently encountered are fraud, misappropriation and criminal mismanagement vis-à-vis third-party clients. Since the inclusion of insider trading and price manipulation as predicate offences as of 1 May 2013, around ten such cases have been reported to MROS. Reports of suspicions of bribery or participation in a criminal organisation are rare in this sector or even non-existent (Figure 48).

Figure 48: Breakdown of the main predicate offences, 2004-2014

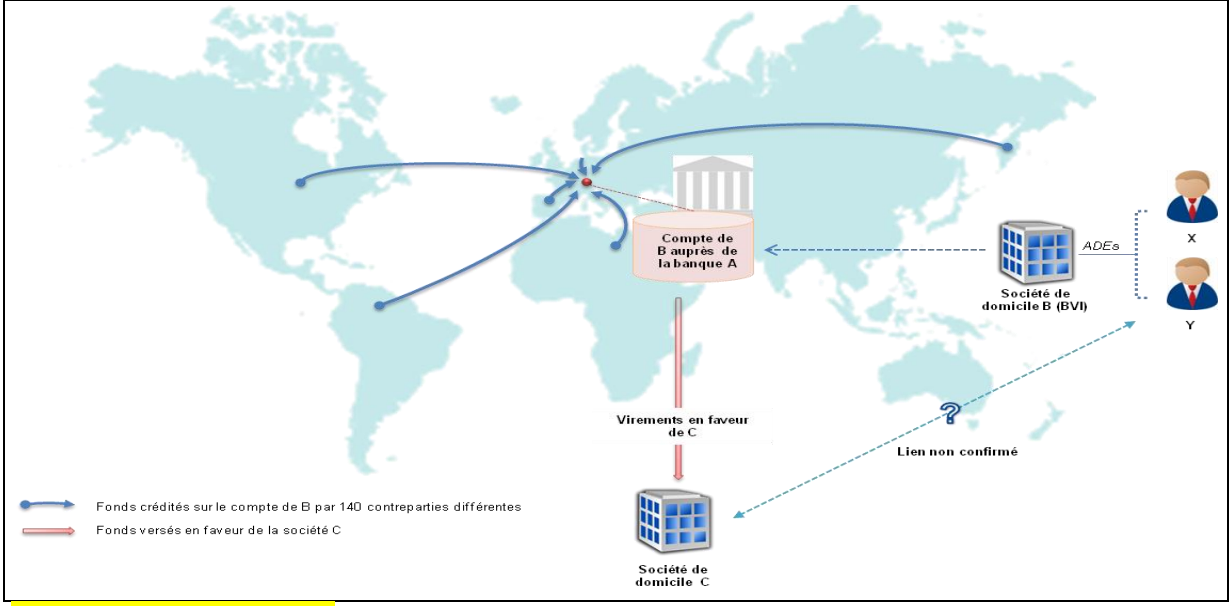


Typologies

A. A newspaper article in another country mentioned a domiciliary company involved in a money laundering affair with which the securities dealer has had a business relationship over a number of years by way of a fiduciary in Switzerland. The BO of the company in question is a PEP from another country. A study of the transactions carried out by the fiduciary revealed that a large sum of money had been paid in the name of the incriminated company to another domiciliary company, whose BO turned out to be the PEP's sister, with a view to buying real estate.

B. A financial intermediary realised that a third party had lost the funds he had paid into the account of a company managed by the financial intermediary. Said company had been created for the purpose of receiving dividends and making investments for the account of X and Y, the two BOs of the account. When analysing the relationship, the financial intermediary found the existence of numerous transactions, involving some 140 natural persons or legal entities domiciled in different jurisdictions. Most of the funds thus collected were then returned to the account of holding company C, whose BOs were unknown. The clients explained that they

managed several companies, which, although belonging to the same group, were located in different jurisdictions, offering a forex trading platform and brokerage services online, and that the payments made to the account in Switzerland originated from clients of companies wishing to invest via these platforms. It emerged, however, that these companies were not registered with any competent national authorities, and some were even on black lists. There were also complaints on various internet forums about reimbursement difficulties, suggesting possible fraud with a pyramid scheme (Ponzi scheme) or criminal mismanagement of funds with a forex scam.



Account of B with bank A
Domiciliary company B (BVI)
Beneficial owners
Transfers to C
Unconfirmed link
Domiciliary company C
Funds credited to B's account by 140 different counterparties
Funds paid to company C

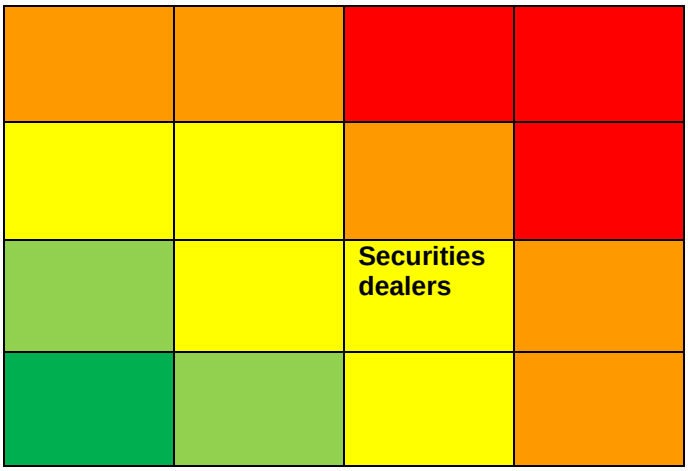
Assessment

The quantitative measurements suggest a moderately high risk for this sector, particularly on account of the size of the amounts involved and the complexity of the cases reported. However, an overall assessment of the risks facing the sector points to a limited risk, given that a large number of the transactions concern securities trading for the dealer's own account or for the account of a client who is himself a financial intermediary trading in proprietary institutional funds. Moreover, many dealers use custodian and payment services with a banking institution which, in turn, is subject to the provisions of the AMLA, thereby lessening the overall risk. The main vulnerability of this sector lies in the huge variability of its players, none of whom strictly limit their services to trading activities, while others combine custodian and management services.

In terms of the type of financial instruments available on the market, the Swiss securities market does not differ from other international trading centres.

The system for combating money laundering and terrorist financing in the area of securities dealers will be supplemented by implementation of new legislative provisions with the revised FATF recommendations, particularly measures to increase the transparency of legal entities. Furthermore, as part of the recent revision of stock exchange law, the system for combating money laundering has already been reinforced by including insider trading and price manipulation as predicate offences[130]. Therefore, given that the financial intermediaries in the sector are subject to the provisions of the AMLA, the vulnerabilities of this sector are appropriately addressed and do not require any additional regulatory measures.

[130] Article 40*a* a ticle 40 of the SESTA, enacted on 1 May 2013

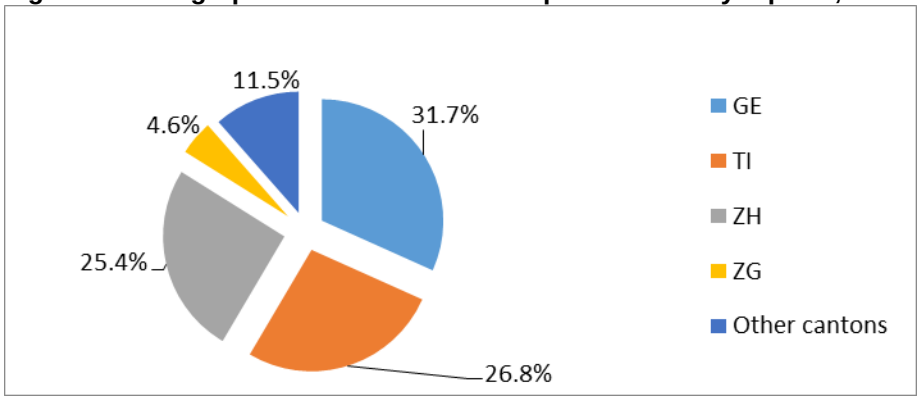


7.1.3 Asset managers

Asset managers select, buy and sell securities or other investment instruments on a professional basis for the account of a client, in keeping with a wealth preservation or growth strategy agreed in advance with the client. To this end, the client issues a power of attorney under which the asset manager opens an account with a financial institution and subsequently takes charge of the client's financial management. The asset manager thus represents the client's interests before the entities responsible for the technical aspects of asset management, whether banks, securities dealers or those involved in collective investment schemes. Independent asset managers sometimes also offer financial advice in areas other than investment *per se*, such as taxation, insurance or succession planning. When not affiliated with a bank or securities dealer and thereby acting autonomously, asset managers are subject to the provisions for combating money laundering and terrorist financing by virtue of Article 2 paragraph 3 letter e of the AMLA, provided they have obtained FINMA authorisation or are affiliated with a recognised self-regulatory organisation.

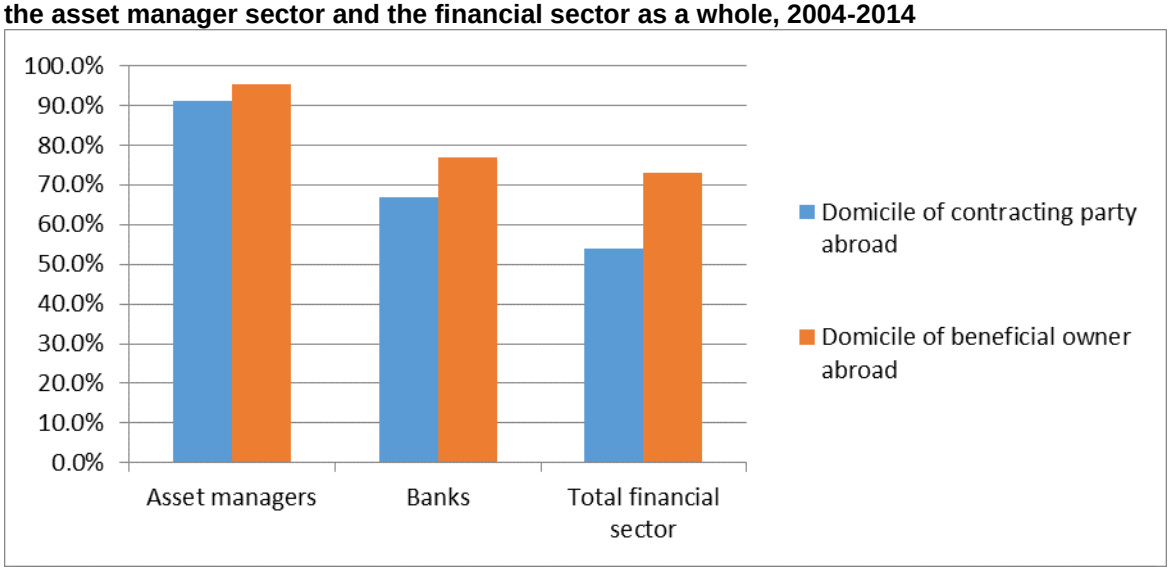
In Switzerland, some 3,000 asset managers share a highly diversified client base. Alongside the banks, these financial intermediaries manage some CHF 600 billion, representing around 11% of the entire asset management market. Most asset management firms are SMEs, with 75% of them employing no more than five people. Two thirds of asset managers have fewer than 100 clients. An analysis of suspicious activity reports from this sector reveals that, geographically speaking, asset managers operating in Switzerland's leading financial centres, i.e. Geneva, Ticino and Zurich, are the most exposed to risk and thereby carry out the most additional checks. Compared with the banking sector, the number of reports from the cantons of Geneva and Ticino is disproportionately high. The canton of Zug also has a higher level of exposure (Figure 49).

Figure 49: Geographical breakdown of suspicious activity reports, 2004-2014



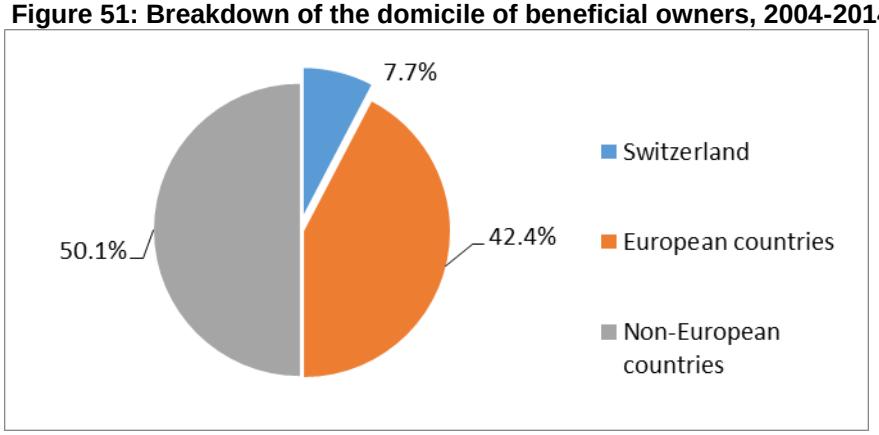
The most salient feature of the risks associated with asset management is the fact that the vast majority of clients are domiciled outside of Switzerland. This holds true for both the contracting party, e.g. a domiciliary company or a fiduciary, and the BO (Figure 50).

Figure 50: Comparison of the domicile of contracting parties and beneficial owners between the asset manager sector and the financial sector as a whole, 2004-2014



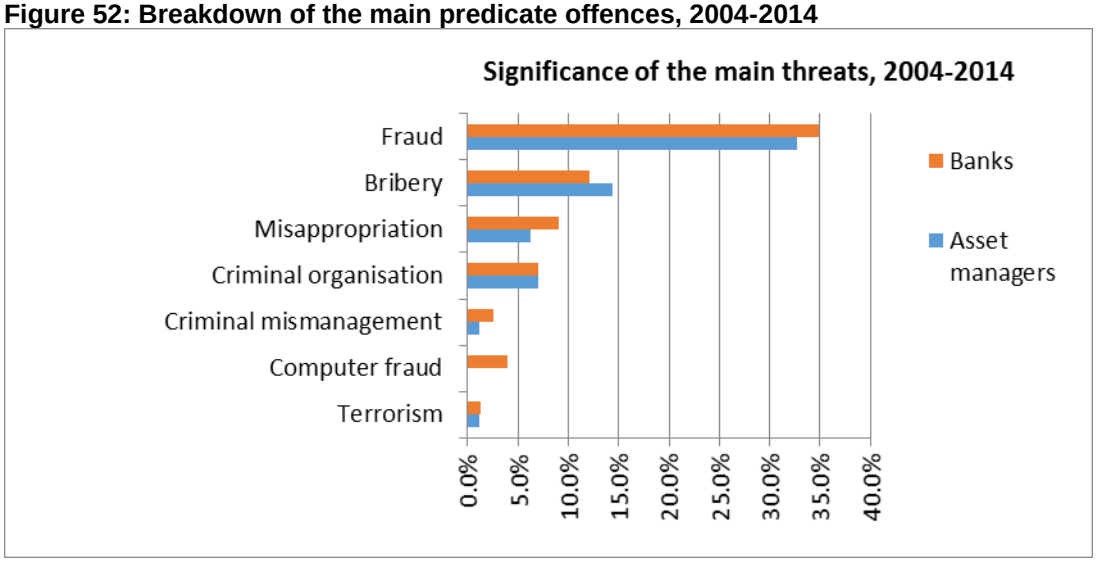
In most cases, the domicile of a BO implicated in a suspicious activity report is outside of Europe (Figure 51). On the other hand, 61.3% of BOs are citizens of a European country.

Figure 51: Breakdown of the domicile of beneficial owners, 2004-2014



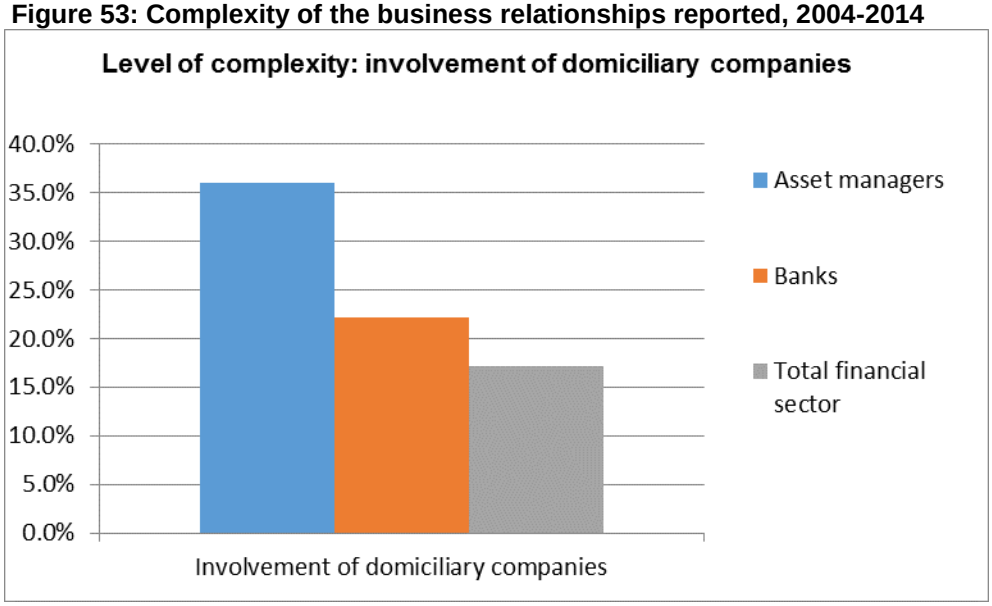
Compared with the banking sector, the analysis of the suspected predicate offences in this sector shows a higher proportion of assets obtained through bribery committed abroad, while the other predicate offences associated with financial crime are lower than the average for the banking sector. The proportion of predicate offences associated with a criminal organisation is the same as in the banking sector (Figure 52).

Figure 52: Breakdown of the main predicate offences, 2004-2014



Moreover, the suspicious cases reported by financial intermediaries in this sector are characterised by a high rate of involvement of domiciliary companies, which may reduce the likelihood of detecting any criminal origin of the assets involved and of identifying the BO (Figure 53).

Figure 53: Complexity of the business relationships reported, 2004-2014



Detection patterns in this sector indicate that suspicions are more likely to originate from an external source operating downstream than through internal checks made upstream. Suspicions based on falsified documents are slightly more prevalent than in the banking sector but may possibly be underestimated due to this sector's more limited resources for detecting any attempts to conceal the true BO behind a business relationship (Figure 54).

Figure 54: Grounds for and origin of suspicions, 2004-2014

Typologies

A. An asset manager contacted MROS to report the business relationships he had maintained over a number of years with two wealthy persons operating in precious metals. The relationships concerned assets of several million Swiss francs, which apparently originated from the business run for 40 years by the asset manager's two clients. The financial intermediary was not aware of any suspicious activities or transactions until being informed by a third party that one of these two people, who was domiciled abroad, had had some problems with the police. In an attempt to obtain further details and to verify the information received, the asset manager tried to contact these two clients, without success. Further enquiries by MROS confirmed the financial intermediary's misgivings: both individuals were suspected of money laundering associated with a criminal organisation. In particular, the company headed by one of them was suspected of failing to identify its clients and of making cash transactions so as to accept assets of criminal origin (prostitution, drugs.) The report was forwarded to the competent criminal prosecution authorities, which opened a criminal investigation.

B. An asset manager arrived at a client's office for a meeting and found the premises being searched by the police. According to newspaper reports published in the days that followed, the asset manager's client, along with seven other people, had been arrested for criminal mismanagement of several million in public subsidies from another country, which had been granted for the purpose of promoting employment. The funds were said to have been reinvested in the purchase of real estate by way of around 50 domiciliary companies. The report was forwarded to the competent prosecution authorities, which closed the case due to lack of proof that the funds were of criminal origin.

C. Following a police search of a client's premises, and after receiving a seizure order and a document production order, a branch of a foreign bank carried out a detailed examination of the relationships associated with that client. The bank found that the same business introducer had been behind several accounts held by different domiciliary companies. The opening of these accounts had been facilitated by an employee of the bank, in violation of his due diligence obligations, by accepting sub-standard photocopies of ID papers made by the asset manager in question. The investigation also revealed that this particular asset manager had assisted his clients in obtaining false papers, thereby enabling them to conceal their identity through various domiciliary companies set up and managed by him. The case is still under investigation.

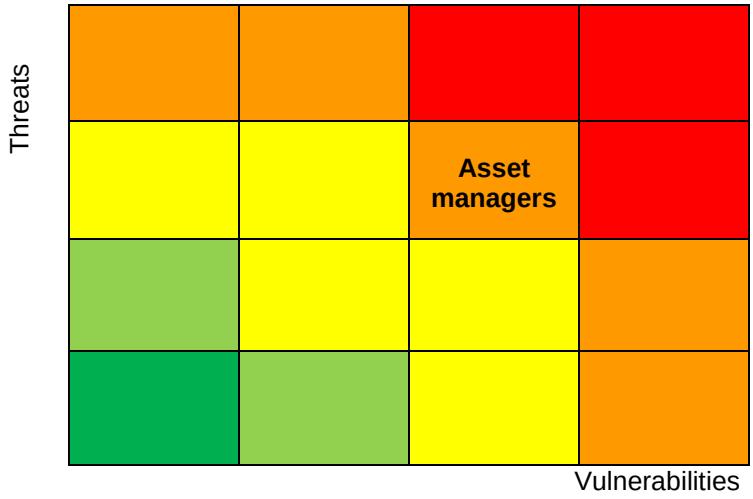
Assessment

The quantitative measurements indicate a particularly high level of complexity in the reports submitted by asset managers, making it all the more important to step up preventive efforts in this sector (verification of clients' economic background and documentation). Indeed, the real threat level in terms of predicate offences is high with respect to all the main threats facing the financial sector. The amounts of money involved are high for all threat factors and comparable to those for banks. Most of the predicate offences in relation to all the threats are committed abroad, making preventive efforts in this sector all the less effective. In particular, managing assets that originate from emerging markets raises the risk of the sector being used for money laundering, given the unconsolidated or even lax application of the law in the jurisdictions concerned. Moreover, the nature of the assets managed and issued in the sector in the form of securities makes the sector particularly prone to be used in the final

stage of the money laundering process, i.e. integration, at which point it is difficult to detect and establish a link between a predicate offence and the securities in circulation.

Therefore, given the vulnerabilities associated with using domiciliary companies and other such legal structures, financial intermediaries in the sector are required to perform additional due diligence in identifying the BO and the origin and destination of assets (Art. 44 *et seq.* and Art. 50 of the AMLO-FINMA). This risk is higher if the asset manager himself offers fiduciary-type services. In any case, the due diligence obligations must be observed by all financial intermediaries involved in the relationship, both asset managers and banks, separately, thereby helping to reduce the overall risk incurred.

The system for combating money laundering and terrorist financing is supplemented by the implementation of new legislative provisions introduced by the revised FATF recommendations, particularly measures to increase the transparency of legal entities (especially unlisted companies issuing bearer shares), an extension of the obligation to include family foundations and ecclesiastical foundations in the commercial register, tighter obligations to identify the physical BOs of legal entities, and the introduction of a new predicate offence in relation to direct taxation. Therefore, in light of the provisions and controls under the AMLA, which are applicable to all players in the sector, and given the intensity of the checks and controls carried out by the banks themselves, the vulnerabilities of this sector are appropriately addressed and do not require any additional regulatory measures. However, players in this sector should be made more aware of the money laundering risks associated with their sector by way of specific training sessions, enabling financial intermediaries in the sector to better adapt to the emerging risks.

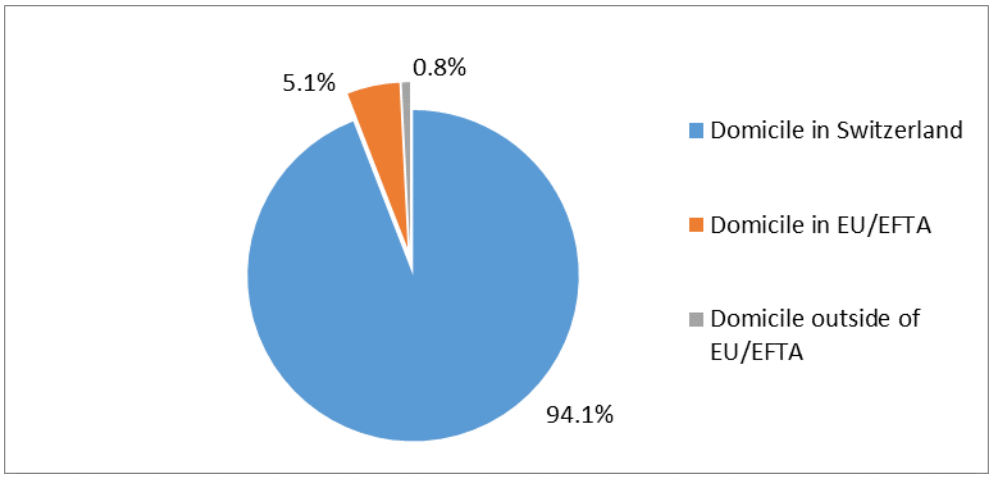


7.1.4 Insurers

Insurers in Switzerland are subject to the system for combating money laundering and terrorist financing by virtue of Article 2 paragraph 2 letter c of the AMLA. Around 30 large insurers share Switzerland's sizeable market. According to the industry's own information, more than 25,000 insurance contracts were signed by financial intermediaries in the sector in 2013, mainly in the form of life insurance policies, but also collective investment schemes and mortgages, which some insurers additionally offer.

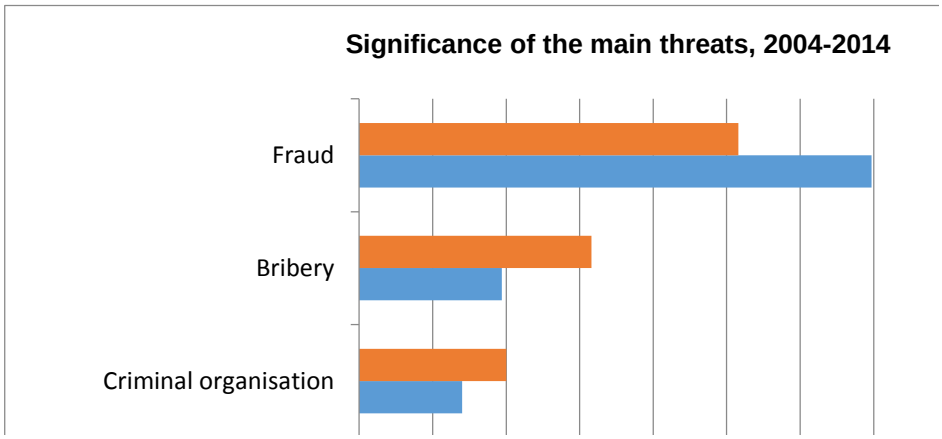
Compared with the banking sector or the financial sector overall, the insurance sector in Switzerland faces a lower real risk, given that most policyholders are domiciled in Switzerland (Figure 55) and also the fact that insurance products offer less potential for liquidity. This is largely confirmed by industry statistics concerning the domicile of policyholders in contracts signed by financial intermediaries in the sector in 2013.

Figure 55: Domicile of insurance policyholders, 2013



Regarding policyholders not domiciled in Switzerland, most of the financial flows under investigation originate in European countries, with very few cases from outside of Europe. Moreover, the cases under suspicion have a relatively low level of complexity, which would suggest a high probability of detection, resulting in this sector's low vulnerability. In terms of the extent of the threats, the insurance sector is more exposed to the main threats linked to the predicate offences of bribery and participation in a criminal organisation than cases of fraud (Figure 56). In both of these scenarios, insurance policies are often just one element of a broader criminal scheme, with the money launderers also using other instruments aside from insurance products. In cases of fraud and misappropriation, insurance products are generally the single means of laundering fraudulently obtained assets; this is done in a concentrated manner and thus entails higher sums of money.

Figure 56: Breakdown of the main predicate offences, 2004-2014



The insurance sector could potentially be used in money laundering by concealing the origin of the assets. The main *modus operandi* in this respect would be to terminate an insurance contract prematurely and have the invested amount repaid to the policyholder. However, the risk facing the sector should be differentiated according to the different products offered by insurers.

The risk in mortgage lending is low. Here, the only means of laundering money is in repaying the loan and paying off the interest. However, as such mortgages are in relation to property located in Switzerland, which are listed in the land register, they offer lower capital mobility and, at the same time, more transparency in respect of the BO.

The risk entailed in life insurance policies is low or moderately high, depending on the contract terms and the amount paid in. For example, single-premium life insurance products offering a single payment increase the mobility of assets and, consequently, the risk of being used in money laundering. Conversely, insurance products with regular premiums or a benefit paid out over an extended period of time are exposed to a relatively low risk.

Products using an insurance wrapper pose a high risk. These are insurance products for which the insurer manages an account with a financial institution that is used to deposit assets paid in favour of a life insurance policy taken out by the client. Here, the client's assets are often used as a single

premium in a life insurance policy. In such operations, however, even though the client maintains a degree of influence in managing the assets, ownership of the assets invested is formally transferred to the insurer, and this reduces the level of transparency regarding the real BO of the assets. This is why, in 2010, FINMA tightened the regulations for life insurance policies with separately managed accounts and portfolios, requiring the custodian financial institutions holding the assets used for this type of insurance product to identify the BO of the assets involved; this has subsequently reduced the risk for this sector[131].

Insurers sometimes use insurance intermediaries or brokers to sell their products[132]. In such cases, some of the due diligence obligations, e.g. identification of the contracting party, are performed directly when the product is sold. However, the more detailed oversight that is required in order to perform the complete due diligence under the AMLA is carried out by the financial intermediary's centralised compliance centre, which performs a series of checks in relation to the risk posed in each case. In this respect, there are no indications that insurance products sold by brokers are exposed to a higher risk.

Typologies

A. In the course of its regular monitoring, the Compliance department of an insurer noted that a person with whom it had signed a life insurance contract was accused of bribery in another country. In exchange for payment of a single premium when taking out the policy, it was agreed that an annual pension would be paid into a bank account in Switzerland in favour of a predefined third party, and the obligations arising from the contract would end upon the policyholder's death. Payments were made for four years in succession. As MROS was unable to substantiate the suspicion that the funds were of criminal origin, the report was not forwarded to the criminal prosecution authorities.

B. An insurer informed MROS of a new business relationship with X, who had taken out a single-premium life insurance policy (already paid) with a death benefit. According to X, this insurance policy was contracted in relation to the purchase of land. Based on its enquiries, the insurer found that the value of the single premium was considerably higher than the price of the land stated on the deed of sale. The company also uncovered some bad press about X. As a result, the financial intermediary suspected that the life insurance policy was being used to commit fraud or as collateral to obtain credit financing. Following its enquiries, MROS discovered that X already had a criminal record for document forgery and fraud, among other things. The competent criminal prosecution authorities opened an investigation.

Assessment

The quantitative measurements suggest a low risk level for this sector, mainly because of the limited complexity of the cases reported; the main risk factor lies in the high amounts of money likely to be laundered with the financial products offered. Indeed, the average volume of assets that could be laundered by way of the insurance sector is very high at between CHF 300,000 and CHF 400,000. The predicate offences of bribery and participation in a criminal organisation, identified as the main threats in Switzerland alongside fraud and misappropriation, are the most prevalent predicate offences in this sector.

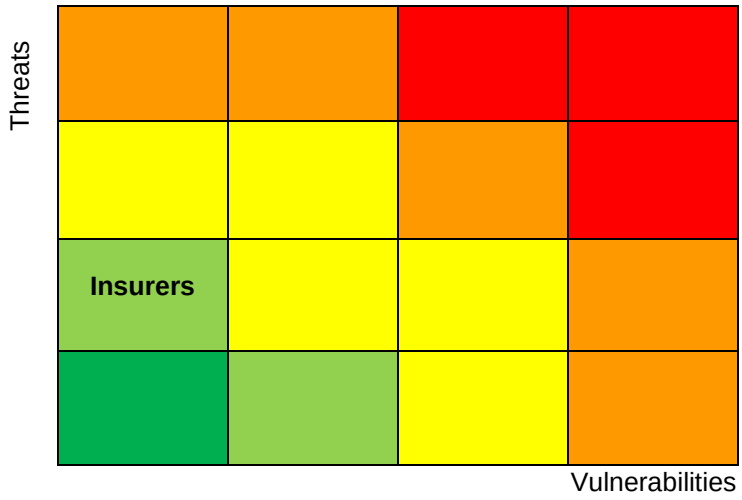
The detection patterns in the sector are quite sophisticated, encompassing numerous sources and grounds for suspicion, such as internal scrutiny of the economic background of clients. In general, the supervisory and regulatory mechanisms implemented by the self-regulatory and supervisory authorities and bodies show that insurance providers are sufficiently capable of adaptation and precise identification of the risks, particularly regarding the need to identify the true BOs, and that the financial intermediaries subject to the AMLA are receiving appropriate training.

Given that the financial intermediaries in the sector are subject to the provisions of the AMLA and also the fact that the sector-specific risks are low, the regulations in place for this sector may be deemed sufficient. Moreover, the system for combating money laundering and terrorist financing will be supplemented by the implementation of new legislative provisions introduced with the revised FATF recommendations, particularly measures to improve the transparency of legal entities and tighter obligations on financial intermediaries to identify the BOs of legal entities. The system therefore does not require any additional regulatory measures.

---

[131] FINMA Newsletter 18 (2010), Handling of Life Insurances with separately managed accounts/portfolios

[132] The insurance intermediary is defined in Article 40 of the IOA. Pursuant to Article 42 of the IOA, FINMA maintains a public register of insurance intermediaries.



7.1.5 Lawyers and notaries

Lawyers and notaries are subject to the provisions of the AMLA only insofar as they perform financial intermediation on behalf of a client (Art. 2 para. 3 of the AMLA). To determine whether an activity exceeds the classical framework of these legal professions, it is often necessary to examine the situation on a case-by-case basis[133].

Unlike in other countries, the Swiss system provides for direct reporting to MROS of suspicions of money laundering and terrorist financing by lawyers and notaries. There is no protective "filter"[134], i.e. an intermediary deciding on the appropriateness of the suspicious activity report, particularly with regard to the client-attorney privilege. The Federal Council has refused such a proposition, stating that "it is up to lawyers and notaries themselves to determine, within the context or their work and for each case individually, whether a matter is associated with their primary or secondary activity"[135]. This position is entirely in step with the Swiss approach to preventing money laundering and terrorist financing, i.e. making the financial intermediaries themselves directly responsible.

In quantitative terms, an analysis of the suspicious activity reports issued by the sector between 2004 and 2014 shows that the real threat is limited to only about 1% of all reports. In this regard, it should be noted that lawyers and notaries perform the role of financial intermediary as a secondary activity. Also, as legal professionals, their threshold of suspicion may be higher than for other players in the financial sector.

The vast majority of suspicious activity reports originate from Switzerland's main financial centres, i.e. the cantons of Geneva, Zurich and Ticino. The complexity of these reports is high, mainly due to the significant involvement of domiciliary companies in the relationships reported by this sector. Thus, among the low number of suspicious activity reports filed by lawyers and notaries, more than 40% of cases involved at least one domiciliary company. Likewise, the vast majority of the clients mentioned in the reports are domiciled abroad (Table 11).

Table 11: Inter-sectoral comparison of the complexity and domicile of the contracting party

	Involvement of domiciliary companies	Foreign domicile of client

[133] The PFIO specifies in further detail which activities are subject to the AMLA, based on the principle that such activities entail a power of disposal or of participation with respect to the assets in question, e.g. in the case of contractual consignments, to the extent that the specific legal competencies are not necessary for execution of the contract, or if the attorney makes the transactions himself with a view to founding a company. Cf. also FINMA Circular 2011/1 on the activity of the financial intermediary within the meaning of the AMLA, particularly Margin no. 114 to 123 with respect to attorneys and notaries.

[134] See in this regard the case of Michaud v. France – ECHR ruling of 6 December 2012

[135] Dispatch of 17 June 1996 concerning the Federal Act on Combating Money Laundering and the Financing of Terrorism in the Financial Sector, BBl 1996 1057, pp. 1008-1089

Lawyers and notaries	**40.1%**	**80.0%**
Fiduciaries	**26.8%**	**88.8%**
Asset managers	**36.0%**	**91.2%**
Banks	**22.1%**	**67.0%**
Total financial intermediaries	**17.1%**	**54.0%**

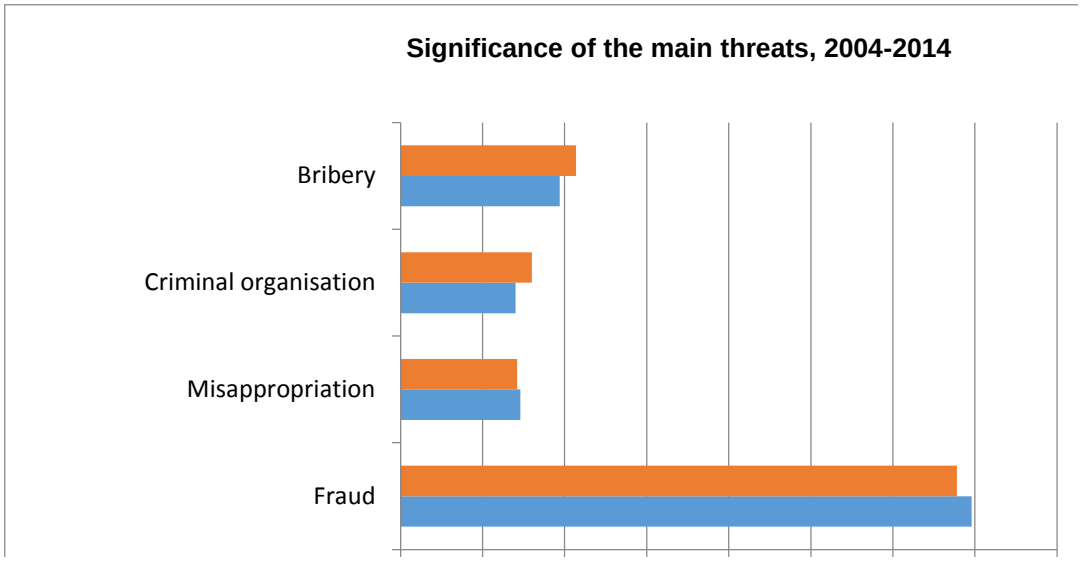
Moreover, an analysis of the number of suspicious activity reports shows that PEPs tend to favour lawyers and notaries for certain types of their financial activities in Switzerland, thereby adding to the sector's vulnerability (Table 12).

Table 12: Inter-sectoral comparison of PEP involvement

	PEPs
Lawyers and notaries	**24.6%**
Fiduciaries	**12.7%**
Asset managers	**8.9%**
Banks	**12.5%**
Total financial intermediaries	**10.4%**

Apart from fraud and misappropriation, the predicate offences of bribery and participation in a criminal organisation are higher for this sector than for the financial sector as a whole (Figure 57).

Figure 57: Breakdown of the main predicate offences, 2004-2014



The widespread use of domiciliary companies and the more prevalent involvement of PEPs in relationships with lawyers and notaries would appear to indicate a substantial threat of bribery involving PEPs: indeed, 43.9% of cases involving this type of client were in relation to suspected acts of bribery, as opposed to 10.3% of the cases reported for misappropriation, 6.5% for participation in a criminal organisation and only 5.1% for fraud.

Regarding clients classified as PEPs, lawyers and notaries are mainly used for managing the accounts of businesses or foundations held by the latter and for credit card management, particularly with Swiss banks offering private banking services or the branches of foreign banks with which their assets are deposited.

Only some cases originate from notaries also dealing with the buying and selling of property, thereby performing financial intermediary services under the AMLA that are not specific to exercising a notary function.

Typologies
A. A law firm is contacted by X, who says he is the manager of company Y registered in another country. X explains that he was doing business with a Swiss company Z and had sent it some goods and that company Z thus owed company Y a large sum of money. X wants the law firm to take charge of receiving the money owed to it, which Z will pay in several instalments, and to transfer it to him. The

law firm has received an initial cheque, which contains some suspicious details. According to the analysis by MROS, Z never had a business relationship with the company Y or with X. The latter apparently tried to defraud the law firm with a forged cheque. As no damage had been incurred and the perpetrator was abroad, MROS closed the case and notified its counterpart in the country in question.

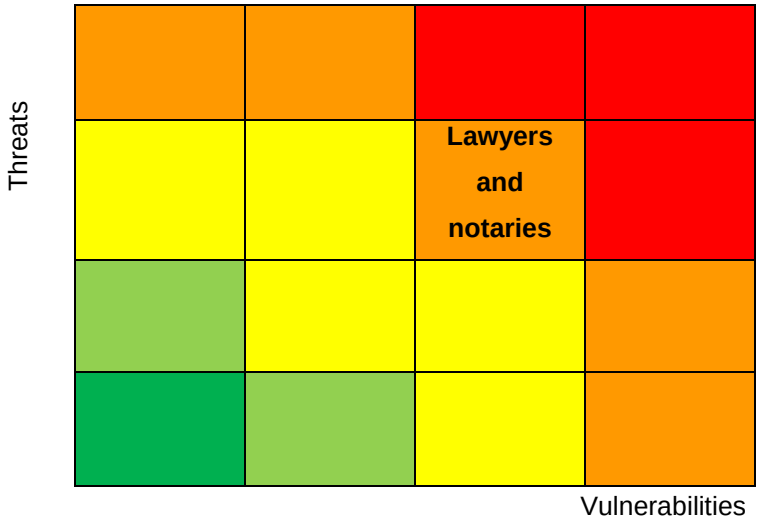
B. X, a former director of a foreign fund management institution with a semi-public status, established company Y, with the assistance of business manager Z, through the intermediary of a law firm. X stated that, on account of his former PEP function, he had always been required to declare all of his income. He declared therefore that the capitalisation funds of company Y, established in Switzerland, were tax-compliant. However, a scandal emerged in the country of residence of X, with allegations being made against several persons including X. It was alleged that X had abused his position in several ways and obtained undue pecuniary advantages. In light of this news, the law firm decided to report this business relationship. Enquiries by MROS found that Z was already listed in the anti-money laundering database. The case was forwarded to the competent public prosecutor, which opened criminal proceedings.

Regarding the detection of suspicious cases, lawyers and notaries rely almost exclusively on the information of third parties, particularly judicial injunctions or newspaper articles. However, as there is often a delay in detecting such articles, the predicate offence of bribery is very difficult to establish without a long-term change of policy in the regimes concerned. The simplicity of the detection pattern is thus in contrast with the complex nature of the suspicious cases that arise in this sector.

Assessment

The quantitative measurements indicate a high risk on account of the high complexity of business relationships in the sector, mainly through the involvement of legal structures that tend to use the services and specialised advice of the legal profession. Lawyers and notaries in Switzerland are primarily exposed to a risk of money laundering based on acts of bribery committed abroad, due to the presence of foreign PEPs among their clients. In such cases, the amounts of money involved are around three times higher than in the banking sector. In this context, the profession would appear to be particularly vulnerable in the case of clients likely to be involved in awarding public contracts, particularly in commodity trading. Compared with the banking sector, lawyers and notaries acting as financial intermediaries have more limited resources and means of detecting and investigating suspicious cases, particularly with regard to transaction monitoring, for which they rely on financial intermediaries in banking.

Implementation of new legislative provisions introduced with the revised FATF recommendations will supplement the system for combating money laundering and terrorist financing, particularly through measures to improve the transparency of legal entities, tighter obligations on all financial intermediaries involved in a business relationship to identify the BOs of legal entities, and an extension of the definition of PEPs to also include domestic PEPs and PEPs of intergovernmental organisations. Thus, given the provisions and controls under the AMLA that apply to all financial intermediaries involved in a business relationship, the mechanism does not require any additional regulatory measures.



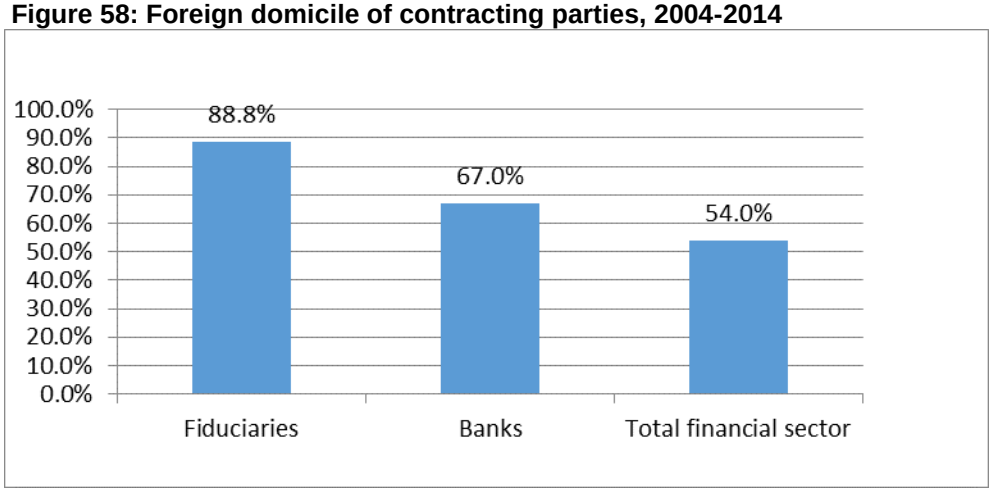
7.1.6 Fiduciaries

Fiduciaries perform a very diverse range of activities, some of which are subject to the provisions of the AMLA (Art. 2 para. 3 of the AMLA and FINMA Circular 2011/1 on the activities of financial intermediaries within the meaning of the AMLA, Margin no. 124 to 127). In 2013, there were around 1,900 fiduciaries subject to the AMLA on the basis of their financial intermediary activities. It should be noted that the size of the fiduciary firms subject to the AMLA may vary considerably.

Fiduciaries often intervene in the establishment and/or administration of domiciliary companies and/or trusts. While such structures are generally used in accordance with the prevailing legislation, it must be said that they also provide an opportunity for concealing assets or financial transactions, mainly for tax reasons. Such structures can also be used for concealing assets of criminal origin. In this context, the fiduciary sector is exposed primarily to stage II of the money laundering process – layering – which serves to conceal and transfer assets of criminal origin without being detected, before being integrated into the real economy (stage III).

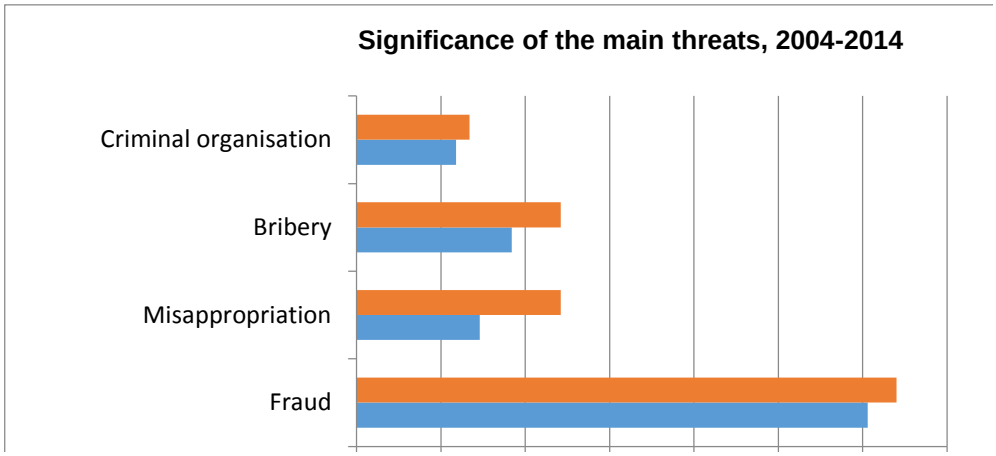
An analysis of the suspicious activity reports from fiduciaries with regard to the contracting parties' domicile (Figure 58) and BOs (Figure 60) shows that the predicate offences are mainly committed abroad (almost nine times out of ten). Based on this criterion, the sector is thus exposed to a high level of risk. The chart below shows the gap between the fiduciary sector and the banking sector with regard to the place where the predicate offences are committed.

Figure 58: Foreign domicile of contracting parties, 2004-2014



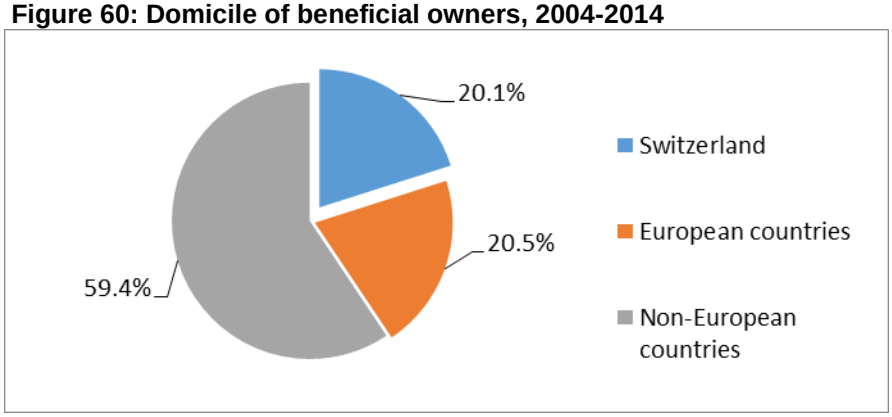
Moreover, with regard to predicate offences, an analysis of this sector reveals all the main threats, i.e. fraud, misappropriation, bribery and participation in a criminal organisation. These offences, which are already quite prevalent in the financial sector as a whole, are even more so among fiduciaries.

Figure 59: Breakdown of the main predicate offences, 2004-2014



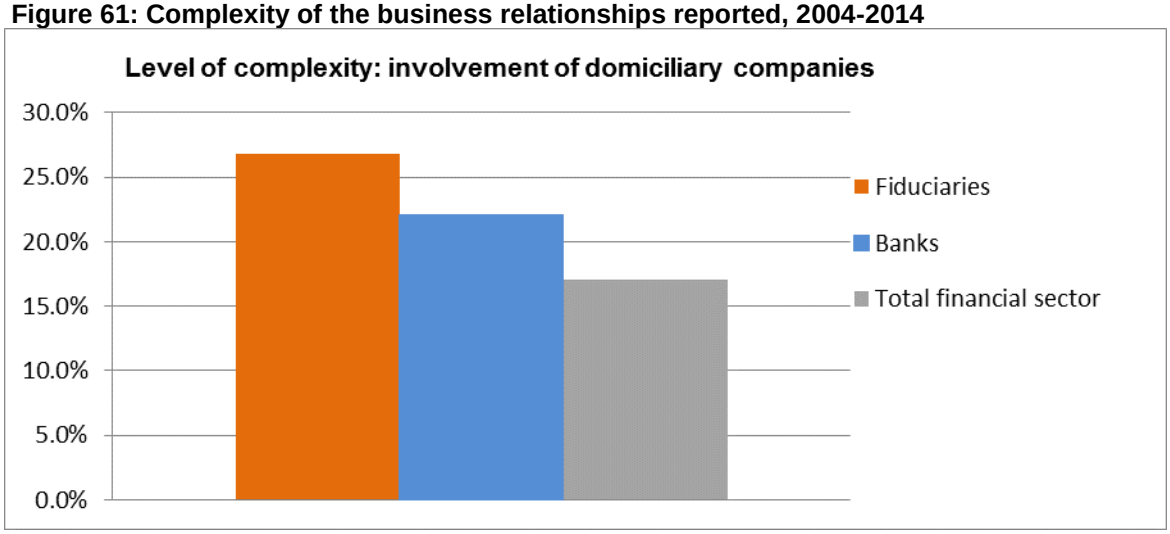
Most assets suspected of being of criminal origin in the fiduciary sector are from countries outside of Europe or certain specific countries in Europe, especially those bordering Switzerland (Figure 56).

Figure 60: Domicile of beneficial owners, 2004-2014



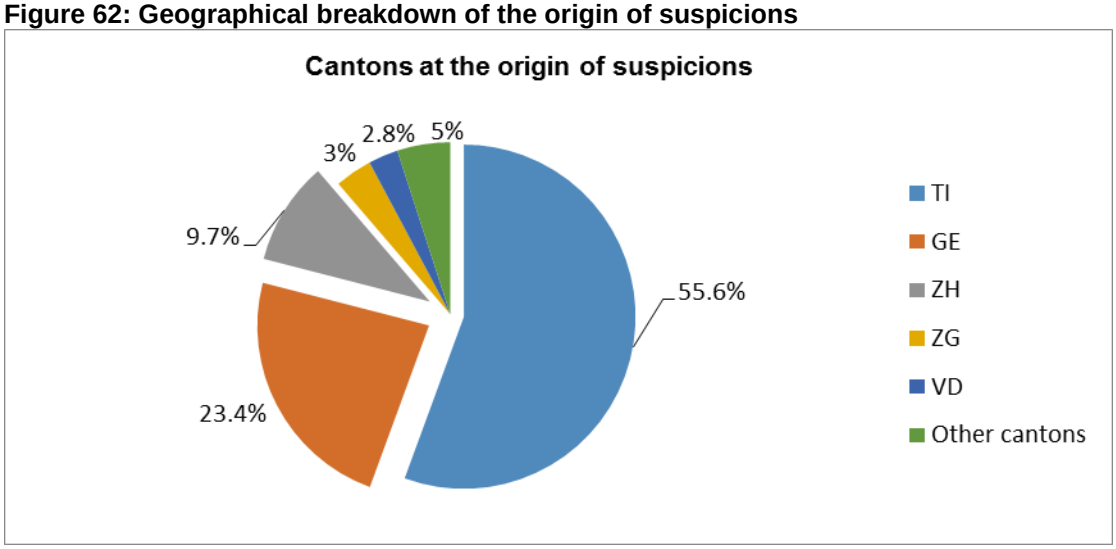
The suspicious cases reported by fiduciaries show a higher level of complexity than those from the banking sector or even the financial sector overall. Almost 27% of suspicious activity reports indicate the involvement of at least one domiciliary company (Figure 57). This is corroborated by information obtained from the sector. In fact, by some estimates, between 20% and 25% of the business relationships of fiduciaries in Switzerland comprise fiduciary activities associated with domiciliary companies or trusts.

Figure 61: Complexity of the business relationships reported, 2004-2014



In terms of geographical breakdown, fiduciaries in the canton of Ticino face the greatest threat level, followed by fiduciaries based in the cantons of Geneva and Zurich and, to a lesser extent, those in the cantons of Zug and Vaud (Figure 62).

Figure 62: Geographical breakdown of the origin of suspicions



Typologies

A. A fiduciary company contacted MROS to report that one of its contracting parties had, after three years, stated that it was not the BO of the assets entrusted to it. Further enquiries revealed that the true beneficiary of the funds was suspected of having committed an offence in another country that was not a felony under Swiss law. Given that this was not a predicate offence to money laundering under Swiss law, this suspicious activity report was closed by MROS.

B. Three individuals asked a fiduciary to provide its services in a transaction to buy and sell shares in a company. The seller had acquired the shares from the others, who then, six months later, asked to buy them back. Once the transaction was completed, the seller asked the fiduciary to deposit the money received, i.e. the proceeds from the sale of the shares, with the fiduciary company. The fiduciary thus opened an account with a bank. The bank carried out checks on the BO of the funds and decided to freeze them. According to enquiries made by MROS, the seller was under investigation abroad for participation in a criminal organisation. One of the buyers was known to the Swiss criminal prosecution authorities within the context of charges of theft, fraud and possession of stolen goods. The case was forwarded to the prosecution authorities so as to merge the different proceedings, if applicable.

C. A foreign PEP contacted a Swiss fiduciary to increase the level of confidentiality of a structure he had created to reduce his taxes on two of his properties. Thus, at the client's request, the Swiss fiduciary created a trust on top of this structure. One year later, several media outlets reported that an international arrest warrant had been issued against this PEP. According to enquiries by the Swiss fiduciary, the client was accused of having embezzled large sums of money in abuse of his position. The analysis by MROS revealed that the confidential structure set up by the PEP raised some serious doubts as to the reason for its creation. In particular, it could be used to hide funds of criminal origin. After analysing the case, MROS forwarded the report to the competent criminal prosecution authorities, which then brought charges for money laundering.

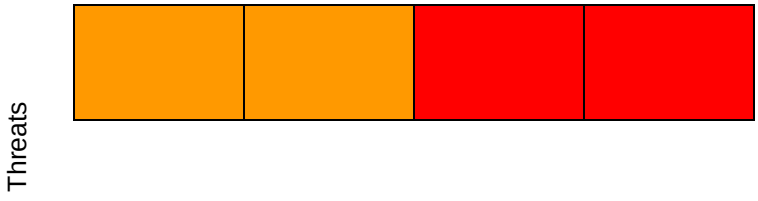
The high degree of complexity in the fiduciary sector contrasts with the detection pattern. Most suspicious activity reports are originally triggered by a media report. The grounds for suspicion are rarely based on the economic and transactional background. Fiduciaries often lack the technical resources to monitor transactions directly or to deploy automatic means of detection, mainly due to the high cost of such systems. In this context, the sector is even more vulnerable in the case of chain transactions involving several domiciliary companies or other complex legal structures and transactions on transitory accounts.

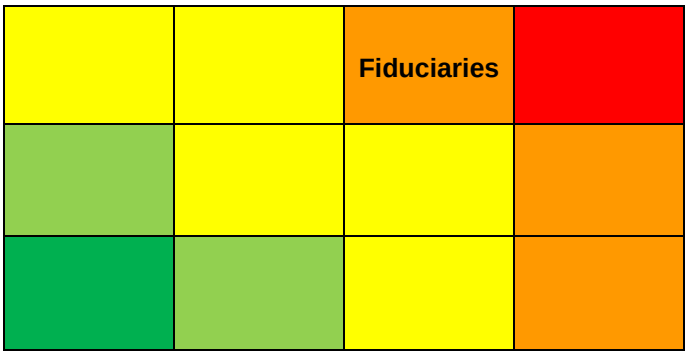
Assessment

The quantitative measurements indicate a high level of risk, mainly due to the complexity of the cases reported and the place where the predicate offences were committed (abroad in most cases).

Given the diverse nature of fiduciaries' activities, the analysis shows that the threat concerns certain specific services offered by a limited number of specialised fiduciaries, specifically those involving business relationships with BOs domiciled abroad. Most of the suspected predicate offences are committed abroad, making efforts to prevent and suppress money laundering all the less effective. In most cases, however, money laundering acts are committed in European countries, especially those bordering Switzerland, where international mutual assistance can be used effectively.

Implementation of new legislative provisions introduced with the revised FATF recommendations will supplement the system for combating money laundering and terrorist financing in this sector. In particular, this concerns measures to improve the transparency of legal entities, including extending the obligation to register family foundations and ecclesiastical foundations, tighter obligations on all financial intermediaries involved in a business relationship to identify the BOs of legal entities, extending the definition of PEPs to also include domestic PEPs and the PEPs of intergovernmental organisations, and introducing a predicate offence in relation to direct taxation. The system therefore does not require any additional regulatory measures.





7.1.7 Casinos

Swiss casinos are subject to the provisions of the AMLA by virtue of Article 2 paragraph 2 letter e of the AMLA. In parallel, they are also subject to the GamblA and the Ordinance of 24 September 2004 on Gambling and Gambling Casinos (GamblO)[136]. The FGB is responsible for overseeing casinos with regard to the AMLA.

Due to the nature of their activities, casinos face a potential threat of being used for money laundering on account of the opportunities to quickly inject huge sums of cash into the regular economic system. To this end, casinos mainly provide an opportunity for the first stage of money laundering, i.e. placement, for instance by transforming funds in the form of paper money (fiduciary money) into cheques (book money), the simplest method being to exchange the incriminating notes for neutral notes. Money launderers often use a straw man to perform this first transformation. To conceal the actual ownership of funds, money launderers are prepared to forfeit part of their gains in return for a more legitimate appearance. In comparison, in the second stage of the process, i.e. layering, money launderers will make more use of the financial services offered by casinos, while, in the third stage (integration), they tend to target total control of a casino. In correlation with these three stages of the money laundering process, the risk assessment for this sector is in three stages: the gambler is at the first level of risk, followed by use of the casino's financial services and, at the third level, use of a casino as a front company.

At the first level of risk, gambling is used as an excuse to justify a sudden increase in wealth which actually stems from criminal activities. Specifically, the prospective money launderer will use gambling winnings to justify their injection of an unusually high amount of money into the financial system, e.g. when depositing it with a banking institution. A second technique is to use the casino's currency exchange services to swap banknotes obtained through crime for neutral banknotes. To address this risk, casinos are subject to the AMLA and the Ordinance of the Federal Gaming Board of 12 June 2007 on the Diligence of Casinos in Combating Money Laundering (AMLO-FGB)[137], which specify a certain number of due diligence obligations regarding clients visiting a casino, such as: the obligation to verify the identity of the contracting party; the obligation to identify the BO; the obligation to repeat these two types of checks; the special obligation to obtain clarification; the obligation to draw up and retain documents; the obligation to take organisational measures and finally, if money laundering is suspected, the obligation to file a report with MROS.

An analysis of the suspicious activity reports suggests a real threat for the following:

- The client uses illicit money to buy chips, either all at once or in a series of transactions, then engages in minimal game play and redeems the chips before leaving the casino.
- Clients buy chips for large amounts of money but then play very little. They divide the remaining chips among accomplices, so that, when it comes to redeeming the chips, each one is below the threshold for registration and identification (e.g. smurfing), sometimes also with the use of forged documents.

At the second threat level, a casino may attract money launderers through the financial services it offers clients, in the form of client accounts or portfolios, or international payment transfers. This threat

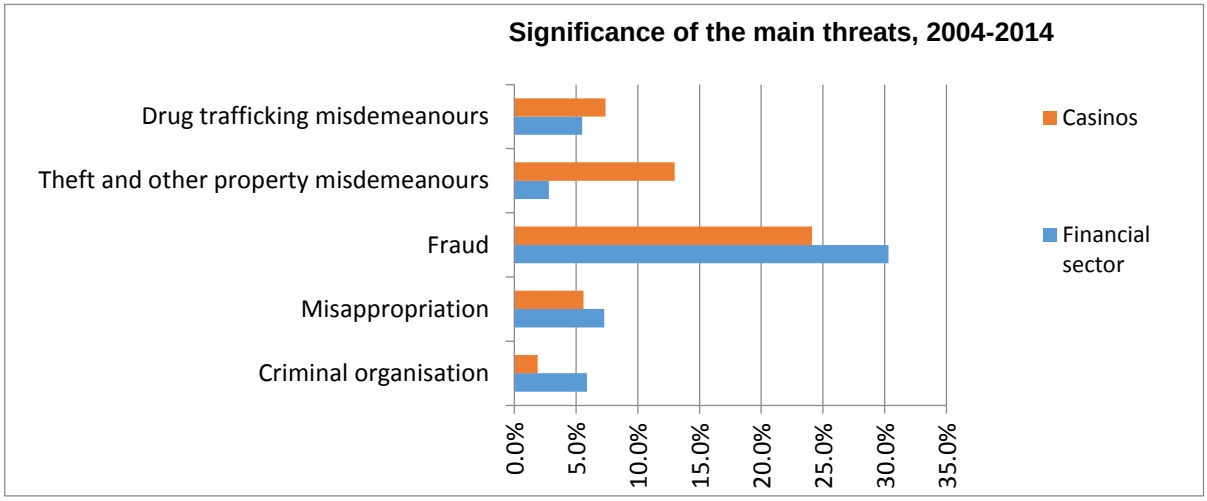
[136] SR 935.521
[137] SR 955.021

is very low for Swiss casinos: on the one hand, the regulations applicable to casinos require that, whenever an account is opened, the money is deposited on this account and may only be paid out by a bank in an FATF member state. It is therefore not possible to top up the account with cash or by a third party. Likewise, any balance that remains may only be reimbursed to the bank that made the initial payment. Moreover, only clients' winnings may be placed on chip accounts. Finally, only chips from the same casino may be played there. No chips of any other origin may be exchanged for cash. Moreover, a casino may not grant loans or advances and may not issue receipts for players' winnings. Neither may it issue or accept bearer cheques. When issuing a cheque in a gambler's name, it must also state the following: "This document does not attest to either a bet or winnings". In practice, only a handful of casinos offer chip accounts.

At the third threat level, the misuse of casinos involves using the management or certain employees in key positions for bribery purposes. To counteract such a possibility, Swiss casino legislation stipulates a series of strict cumulative mechanisms. Firstly, the conditions for granting a casino licence serve to identify the interests behind their operators and the BOs of casinos. In particular, the applicant and shareholders must have a good reputation and have established the lawful origin of the assets at their disposal[138]. Thus, given that the holders of a casino licence, the management and staff are subject to detailed scrutiny and are inspected throughout the duration of the licence, the risk of a casino serving as a front for money laundering is very low. Secondly, the terms of taxation under Swiss law make casinos unattractive to anyone tempted to use them for large-scale money laundering: apart from ordinary corporate taxes, casinos are also subject to tax on their gross income from gambling at a rate which may vary between 40% and 80%.

An analysis of the suspicious activity reports and suspected predicate offences shows that most money laundering in the casinos sector is in relation to the first stage and at the first level, mainly involving funds from drug trafficking and theft, as well as other property misdemeanours, concerning average amounts of less than CHF 10,000. The predicate offences of fraud and misappropriation, which tend to be more associated with the second stage of the money laundering process, are under-represented in this sector with respect to the financial sector as a whole, as is participation in a criminal organisation (Figure 63).

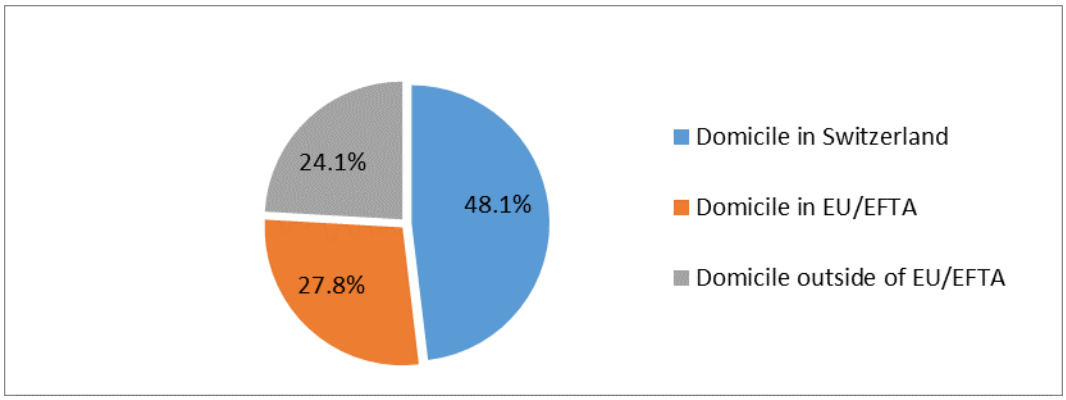
Figure 63: Breakdown of the main predicate offences, 2004-2014



Regarding the origin of the threat, most of the individuals under suspicion are domiciled in Switzerland or neighbouring European countries (Figure 64).

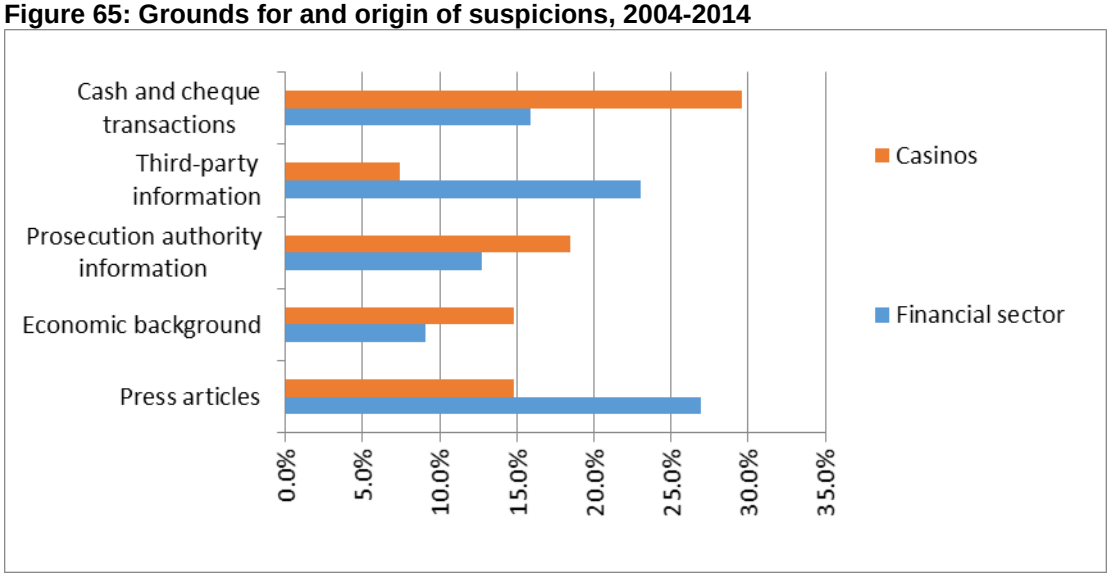
Figure 64: Breakdown of the domicile of contracting parties, 2004-2014

[138] Beneficial owners are classified as those holding a direct or indirect share of at least 5% in the capital, or persons or groups of persons affiliated by way of a voting agreement who hold at least 5% of all voting rights (Art. 4 para. 1 of the GamblO). The individuals holding such shareholdings must also provide the Board with a declaration stating whether they hold this share for their own account or on a fiduciary basis for the account of others and indicating whether they have granted options or other such rights on these (Art. 4 para. 2 of the GamblO).



Regarding drug trafficking misdemeanours, the proportion of suspects domiciled in Switzerland is even higher, while cases of fraud and misappropriation are more likely to be international. In most cases, the grounds for suspicion in the casinos sector are associated with cash and cheque transactions, information received from the prosecution authorities and doubts about clients' economic background (Figure 65).

Figure 65: Grounds for and origin of suspicions, 2004-2014



Typologies

A. The casino noticed that two clients, a man and a woman, were gambling very little after exchanging several wads of 100 franc notes for 1,000 franc notes, for a total of CHF 18,000. When the woman was questioned about the origin of the funds, the man accompanying her quickly left the casino. In the course of a subsequent visit, the woman told a member of the casino staff that her partner had been arrested by the police for theft and drug trafficking. Following this, the casino submitted a suspicious activity report to MROS, which forwarded it to the cantonal prosecution authorities. In a hearing before the latter, the man admitted to having exchanged cash on behalf of a drug dealer.

B. A client asked to redeem a large portion of the CHF 10,000 he had bought in chips after just one and a half hours of game play. After carrying out research online and with various databases, the casino found that this client, along with two other members of the same political party, had been accused of trading in influence within a European administrative body. The client is a businessman who owns a chain of restaurants. However, in the absence of concrete proof of the criminal origin of the money played in the casino, plus the fact that trading in influence does not constitute a predicate offence to money laundering in Switzerland, MROS did not forward the report to a criminal prosecution authority.

Assessment

The quantitative measurements point to a low risk, mainly on account of the low level of complexity of the reports filed. Indeed, thanks to the legislation on casinos, the risk of money laundering in this sector is almost exclusively concentrated on stage I of the money laundering process; the risks in stages II and III are very low, particularly because of the limited financial services that casinos are allowed to offer and the very strict licensing conditions. The FGB's oversight is efficient and

comprehensive; this body is responsible for application of the legislation on casinos, including continuous supervision of adherence to the licensing conditions and the provisions on combating money laundering.

In general, the level of training in the sector is appropriate. However, increased competition from online casinos and from rival casinos abroad with more flexible enforcement systems creates a vulnerability in terms of implementation of the mechanism: under growing economic pressure, casinos vary in terms of the resources made available, depending on their size and financial situation.

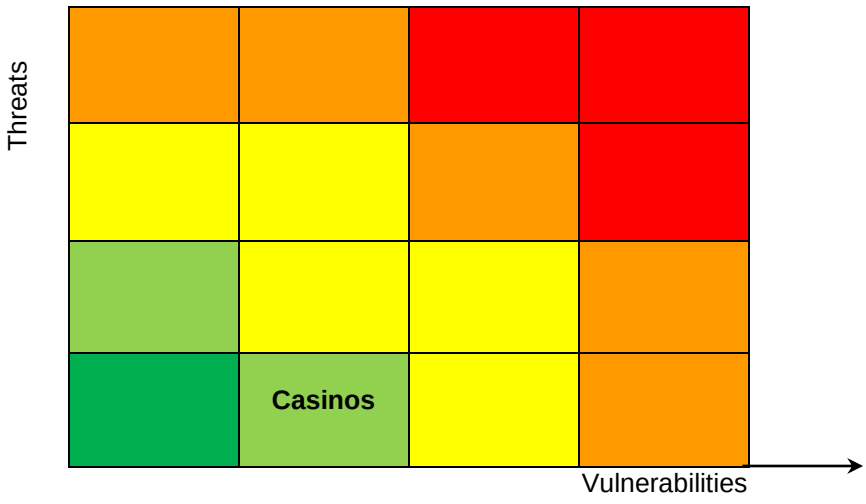
The emergence of new risks in the casinos sector mainly concerns the games of chance offered by online casinos, which are not currently authorised in Switzerland and therefore not subject to the provisions of the AMLA. However, the FGB is currently examining the measures applicable to online casinos, with a view to enactment of a new gambling law in 2018 applicable to all forms of gambling in Switzerland, including lotteries as well as casinos and online casinos.

The supervision and control concept envisaged by the legislator is based on the principle that it is preferable, for cost and efficiency reasons, to entrust the tasks of control and continuous supervision to casino operators themselves rather than having the Confederation perform continuous supervision of the running of games and the associated financial transactions. Nonetheless, it is up to the competent licensing and supervisory authorities to keep a rigorous check on the licensing conditions, to ensure that these are fulfilled throughout the duration of the licence and to assess on an ongoing basis the quality and efficiency of casinos' internal control systems in relation to operation of their games and the prevention of money laundering and terrorist financing. The authority carries out periodic onsite spot-checks, with the focus on verifying casinos' internal supervisory and control measures. In relation to the AMLA, casinos are inspected at least once a year. The findings are communicated to the casinos with a request for corrective measures within a specified deadline and may be subject to a follow-up audit.

Furthermore, casinos are required to have their annual accounts audited by an auditor. The auditor issues an explanatory report for the FGB in which it is required not only to present the casino's financial situation but also state its opinion regarding the casino's adherence to the financial licensing conditions and also its due diligence obligations under the AMLA.

In the event of any violations or irregularities, the FGB orders the corrective measures necessary to restore legal order to remove the irregularity. It may also issue administrative sanctions if the licence-holder has infringed the licence conditions to its advantage or contravened final judgments: such sanctions may be up to three times the profit realised or up to 20% of the gross income from games if the profit realised cannot be evaluated. In serious cases, if any failures or serious shortcomings are found, the conditions that prevailed for the granting of the licence are deemed to no longer exist and the licence must be restricted, suspended or even withdrawn.

Given the extent of the strict controls undertaken by casinos in combating money laundering and terrorist financing, the vulnerabilities in the sector are appropriately addressed and do not require any additional regulatory measures.

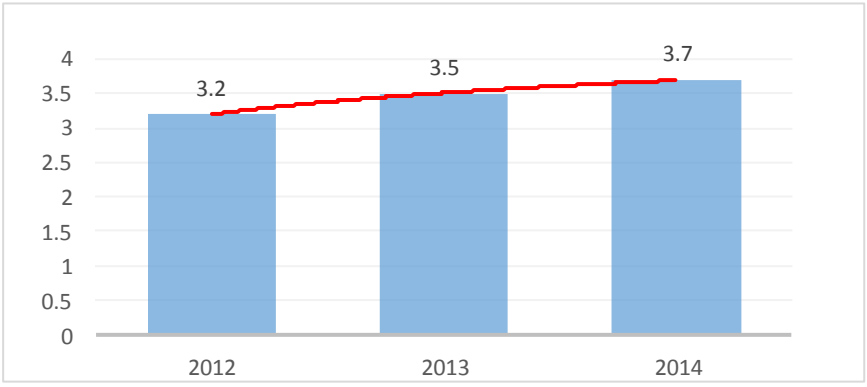


7.1.8 Money transmitters and foreign exchange transactions

Money transmitters are financial intermediaries within the meaning of Article 2 paragraph 3 of the AMLA. They are the main providers of money or value transfer services (MVTS). More than 85% of the financial flows in this sector concern transfers made from Switzerland to another country, in most cases to countries that do not have banking services for the fast and reliable transfer of funds. Apart from the general money transmitters operating worldwide, specialised MVTS providers also exist for certain countries. The majority of the clients of money transmitters have close family ties in another country. The money being sent is primarily in the form of remittances to help support family members in their country of origin. Money transmitters thus fulfil a social function, given that, in some countries, they are the only means of receiving money sent from abroad.

The total volume of transactions made by the sector is on the rise, confirming the sustained demand for this type of service in Switzerland (Figure 66). Since 2012, the total number of money transmitters has increased in line with the proliferation of points of sale available at newsagent kiosks. In 2013, there were more than 2,000 points of sale throughout Switzerland.

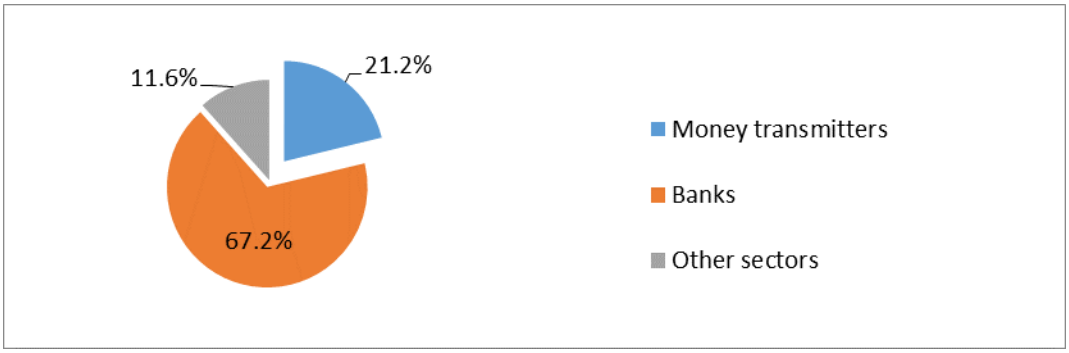
Figure 66: Estimated growth in CHF bn of the total volume of transactions made by money transmitters in Switzerland, 2012-2014



As the sector presents certain attractive features likely to increase the vulnerability of money transmitters, the inherent potential threat is high. The services offered by the sector are characterised by the ease and speed at which money can be transferred abroad. Moreover, the users of such services send cash, so it is more difficult to establish the origin of the money and the BO, especially in view of the differences in the level of verifications and checks between Switzerland and the destination country. While transfers abroad are subject to certain rules and regulations, the system for combating money laundering and terrorist financing could well be less stringent in the destination country than in Switzerland. There is also the fact that walk-in customers play an important role in this sector. This makes it more difficult to carry out checks on them, whether for the origin or destination of the funds.

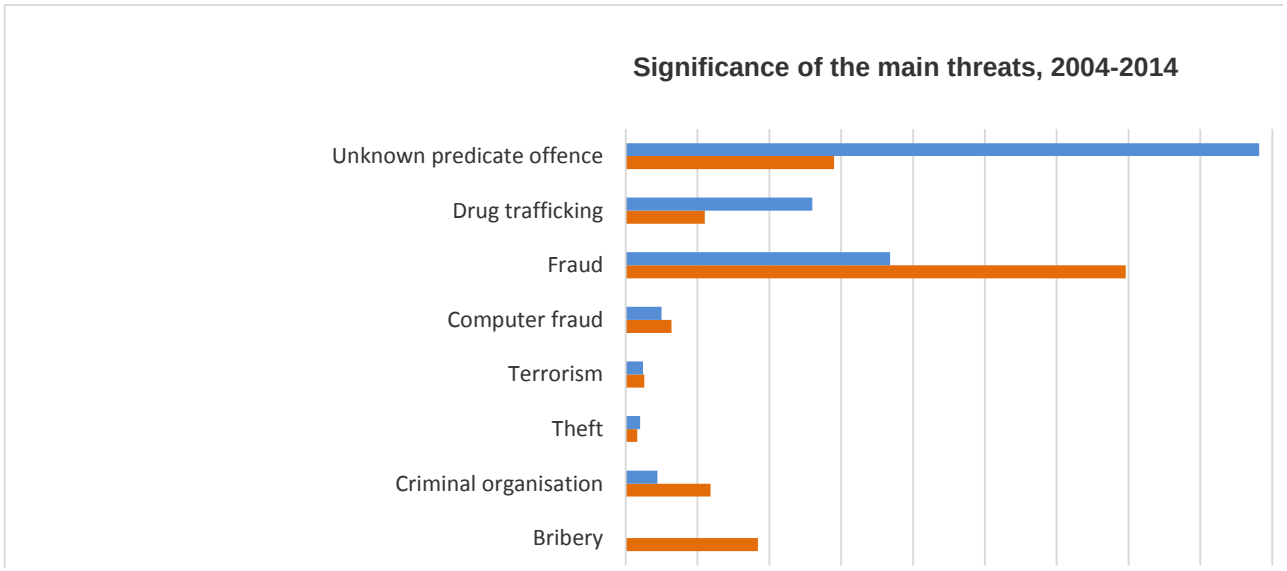
The high number of suspicious activity reports submitted to MROS gives an initial indication of the size of the real threat: in fact, with this sector representing almost a quarter of all reports, it is second only to the banking sector (Figure 67).

Figure 67: Proportion of suspicious activity reports submitted by money transmitters, 2004-2014



However, the sums of money involved are smaller than in other sectors. In general, the average transaction is for between CHF 400 and CHF 600, with a decline apparent since 2012. In the case of specialised money transmitters for certain destinations, of which there are fewer, the average amount sent is between CHF 5,000 and CHF 7,000. The threat associated with predicate offences related to offences against the NarcA is real and occasionally linked to the threat of participation in a criminal organisation. On the other hand, the predicate offences associated with fraud seem to be underrepresented, as these are generally detected only after more detailed verifications.

Figure 68: Breakdown of the main predicate offences, 2004-2014



In this sector, the threats of money laundering and terrorist financing may materialise as a result of different vulnerabilities at three levels, i.e. economic and structural (A), regulatory (B) and technical (C).

A. Economic and structural risks

Competition within the sector in recent years has led to market concentration, resulting in a smaller number of larger providers. Margins in this sector are determined by the price of the service billed to the client and the currency gains that money transmitters earn on the funds accumulated. This trend could potentially mitigate the risk in the sector, as the larger money transmitters, with their economies of scale, can devote more resources to performing due diligence. The filtering systems used by the larger providers are more sophisticated, comprising a transaction monitoring system that operates independently of the first filter used by the contact person. At the same time, market concentration produces greater disparities with respect to the smaller money transmitters, who try to maintain their margins against tighter competition by cutting costs.

Competition between the various players in the sector, whether the agents of financial intermediaries or auxiliary persons, may cause them to opt out of the regulated market, either leaving the business altogether or offering alternative modes of transfer that are less costly for them and, at the same time, cheaper for their clients. However, there is no indication of any such parallel market in Switzerland. Furthermore, neither the use nor the extent of alternative modes of transfer outside of market regulation, such as hawala, is known. With little demand in Switzerland for the destinations targeted by this mode of transfer[139], its use can be assumed to be relatively low.

The sector notes the continued and increasing difficulty in Switzerland of finding financial intermediaries, particularly banking institutions, offering transitory accounts. As banks consider relationships with money transmitters to be high-risk, they frequently refuse to conduct business with them or may decide to cease such relations, irrespective of the individual money transmitter's commitment and resources devoted to performing due diligence. This risk is even greater for small and medium-sized money transmitters, which banks assume will be less capable of fulfilling their due diligence obligations.

[139] FATF, The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing 2013

B. Regulatory risks

Money transmitters are subject to the provisions of the AMLA, by way of either FINMA supervision or an SRO. Most money transmitters submit to supervision by an SRO. However, financial intermediaries in the sector may delegate their specific collection activities to individuals, who often perform such activities in parallel with their primary business activity. These individuals, acting on behalf of and in the name of the financial intermediary, who performs the actual transfer to other points of sale, are affiliated with the financial intermediary by way of an exclusive service contract. They are included in the anti-money laundering mechanism of the financial intermediary, who is solely responsible for the performance of due diligence and is subject to supervision. In terms of regulation, these individuals are considered "auxiliary persons" as per Article 1 paragraph 2 letter f of the PFIO, as their business activity does not constitute independent financial intermediation. In 2013, 14 of the 71 financial intermediaries in this sector worked with a network of such auxiliary persons. In practice, it is the auxiliary persons who carry out the day-to-day money transmitting activities for the account of the financial intermediary.

The current regulation of auxiliary persons thus poses an element of uncertainty with regard to supervision, as the legal responsibility for their due diligence obligations under the AMLA, including the reporting obligation, remains with the financial intermediary itself. Specifically, it is up to the financial intermediary to ensure the exclusive affiliation of its auxiliary persons. The supervisory bodies depend to a large extent on the assurances given by the financial intermediary in this regard. It is therefore quite possible for a non-regulatory situation to exist for some time, where an auxiliary person is affiliated with more than one money transmitter, particularly as they will not be held liable for such a situation given that the AMLA is not directly applicable to them. Likewise, it is possible for an auxiliary person whose affiliation has been cancelled by a financial intermediary, e.g. due to lack of vigilance, to work with another financial intermediary without informing them of the previous situation.

C. Technical risks

Under the current regulation, all service providers in this sector who are in direct contact with clients are required to identify the client immediately, irrespective of the amount of money involved. In practice, the cashiers create a client profile at this point, photocopying or scanning the ID presented so that the agent and his auxiliaries do not have to check the same client's ID papers the next time, provided that they can be sure it is in fact the same person[140]. An analysis of the suspicious activity reports shows that the staff who come into direct contact with clients are not capable of carrying out detailed verifications beyond a cursory check of ID papers. Therefore, only the most obvious forgeries are detected. In this respect, walk-in clients with no regular contact with the service provider pose a higher risk. The low rate of reports from this sector that are forwarded to a criminal prosecution authority suggests a limited capacity to check the economic background of clients. In this respect, an analysis of the suspicious cases reveals that requests for clarification of the economic background are more dissuasive if they are made in real time. In comparison, transaction monitoring after the fact is less effective, with the notable exception of an authorised financial intermediary possibly detecting suspicious activity on the part of its auxiliary agents.

The vulnerability posed by client identification, in particular, increases the risk of smurfing or the breaking-up of large amounts of money, a practice specifically associated with the sector. This entails breaking up assets of criminal origin into smaller amounts before transmission, thereby circumventing detection by remaining below a certain threshold. In Switzerland, the threshold above which a transmission is deemed to present a higher risk is CHF 5,000. Most of the suspicious activity reports are in relation to amounts below this threshold. Moreover, only 13 of the 2,487 suspicious activity reports examined in this study cited smurfing as the grounds for suspicion. This is an indication of the difficulties faced by money transmitters in detecting such methods. In such cases, an auxiliary's exclusive affiliation to a single financial intermediary restricts the risks to just that intermediary. However, the situation becomes more complicated if the cashier is actively involved in concealing the client's identity by creating a phantom client profile or making payments with pre-existing client profiles. Convictions for violation of due diligence obligations under Article 305ter of the SCC are frequently associated with the money transmitting sector, especially involving auxiliaries, thereby testifying to the reality of this threat.

Another means of money laundering in this sector concerns the use of "financial agents", i.e. money mules. This falls under the growing threat of money laundering in association with online fraud, often through the use of data obtained fraudulently online (phishing). In return for their services, the

[140] Provisions corresponding to Article 45 paragraph 2 of the AMLO-FINMA in the SRO's regulations

"financial agent" receives a percentage of the money transmitted. In some cases, therefore, the "financial agent" may not even be aware that they are working for a criminal enterprise.

In light of the growing trend towards online fraud and the difficulty in prosecuting such offences on account of technological and international ramifications, financial intermediaries involved in the transfer of funds play a crucial role in mitigating the money laundering risks of online fraud, in terms of both prevention and the protection of potential victims in Switzerland.

Typologies

A. An analysis of the transactions by an international service provider revealed that abnormally large amounts of money were transferred to a given country at a point of sale run by an auxiliary person. Some of the funds in question were transferred under the auxiliary's own name. Enquiries by MROS revealed that the recipients in the destination country in question were mentioned in other suspicious activity reports concerning assets suspected of originating in drug trafficking activities. It was therefore possible that the auxiliary person consciously helped to conceal his clients' identities and the suspected illicit origin of the funds transferred. The suspicious activity report was forwarded to a criminal prosecution authority but was subsequently closed due to lack of evidence.

B. During a routine check with a software program to detect forged ID papers at a point of sale, a financial intermediary found a scan of a forged document used by a client to make several transfers. As the person in question could not be identified or challenged, the charges brought after the report was forwarded by MROS were suspended by the prosecution authorities.

C. In relation to a transfer to a high-risk country, a client claimed that he wanted to help a person he met online purchase a plane ticket. The client explained that he had to pay an amount received by a third party to the person he met online, showing the bank statement as proof of the corresponding payment (around CHF 1,500). Checks carried out on the financial intermediary revealed that the client in question had already transferred a smaller amount to the same person. As the procedure had the characteristics of a phishing scam, the report was forwarded to the criminal prosecution authorities. The latter dismissed the case, as it was unable to prove that the person in question had acted intentionally with the objective of laundering money.

The service providers involved in foreign exchange transactions very often also act as money transmitters. As the same verification resources are used, the vulnerability of this activity is reduced. Moreover, given the growing use of other means of payment, particularly credit and debit cards, the amounts exchanged are quite small, and in most cases concern an exchange from foreign currencies into Swiss francs. Very few cases are thus reported to MROS, and these tend to be mainly in the border areas. The predicate offence to money laundering associated with this sector is almost exclusively drug trafficking.

Assessment

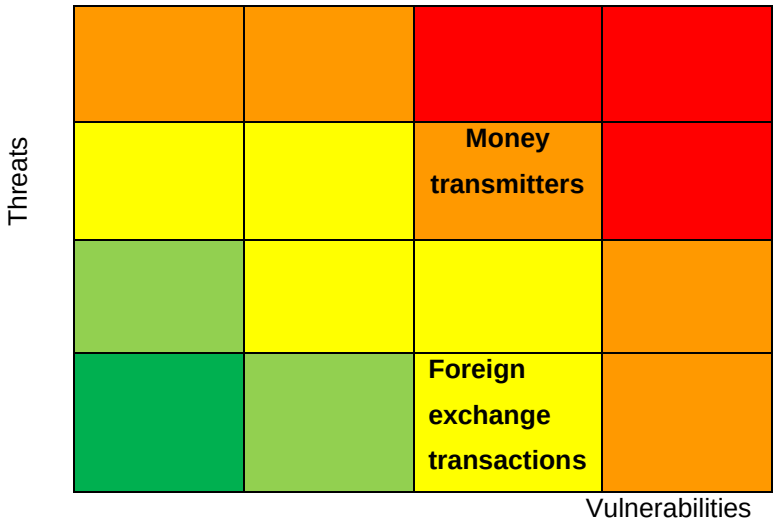
The quantitative measurements suggest a moderately low level of risk, given the small amounts of money involved and the absence of any serious risks such as the presence of PEPs or the use of complex legal structures. However, the risk is higher whenever a high-risk country is involved.

Nonetheless, the number of suspicious activity reports suggests a serious real threat. In terms of predicate offences, the main threat factor in this sector concerns offences against the NarcA, fraud and computer fraud (phishing) and, to a lesser extent, human trafficking with links to a criminal organisation and terrorist financing. The probability of detecting money laundering in connection with such offences is moderately high. The systematic use of forgery-detection software for ID papers can reduce the risk inherent to the use of forged documents for concealing the origin of funds.

The vulnerabilities in this sector are concentrated at the level of the auxiliary agents, whose ability to perform due diligence depends on the resources made available by the financial intermediary in terms of training, analysis and supplementary checks. The technical risks lie mainly in the risk of smurfing, which is amplified when the direct employees or auxiliary persons of financial intermediaries do not correctly identify the contracting party or are active accomplices in helping to conceal clients' identities.

The risk in the foreign exchange sector is lower, mainly because of the limited benefits of foreign exchange transactions in the money laundering process, given that, in principle, there is no transmission of financial flows to a high-risk country and the amounts involved are low.

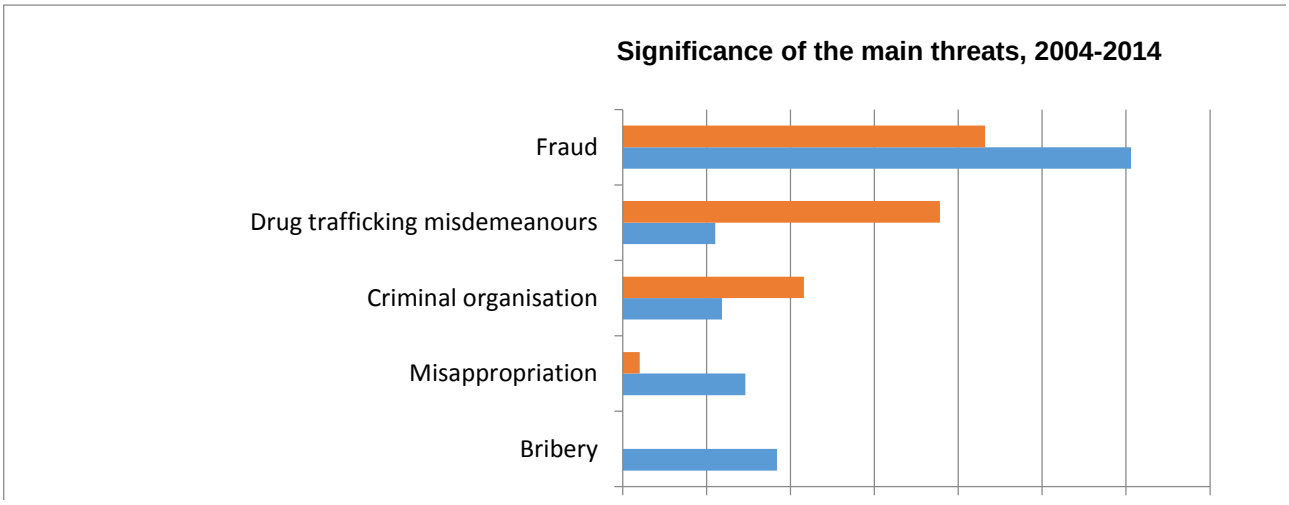
Overall, the sector's vulnerabilities are mitigated by the various controls provided for in the applicable regulations, which are among the strictest in the world and implement all international standards in this respect. Therefore, the system does not require any additional regulatory measures.



7.1.9 Credit services

Financial intermediaries that carry out credit transactions on a professional basis in Switzerland are subject to the anti-money laundering system by virtue of Article 2 paragraph 3 letter a of the AMLA. This mainly concerns financial intermediaries with transactions in financial leasing, consumer loans and commercial financing. The main potential threat lies in the placement stage, with a view to concealing the illicit origin of the funds concerned and making them available for consumer spending within a relatively short space of time. The threat of money laundering in this sector is particularly associated with predicate offences related to drug trafficking and, to a lesser extent, suspected participation in a criminal organisation. The other predicate offences are clearly under-represented, including fraud, which intermediaries in the sector frequently report as an offence committed against them, particularly in the non-payment of premiums (Figure 69).

Figure 69: Breakdown of the main predicate offences, 2004-2014



The number of suspicious activity reports is quite low for this sector. In more than 80% of the cases reported as suspicious, the business relationship had been established by way of a legal entity domiciled in Switzerland. Domiciliary companies were used in a small number of cases, particularly with regard to reports concerning a possible predicate offence linked to organised crime. An analysis of suspicious activity reports shows that the financial intermediaries in the sector are capable of correctly identifying the BOs behind such legal entities. Two-thirds of the BOs identified were domiciled in Switzerland, while the remaining third were often in a country bordering Switzerland. In this respect, it should be noted that in leasing transactions, as permitted by the SRO regulations,

identification of the contracting party and the BO is often delegated by the financial intermediaries to third parties, i.e. car dealers in most cases.

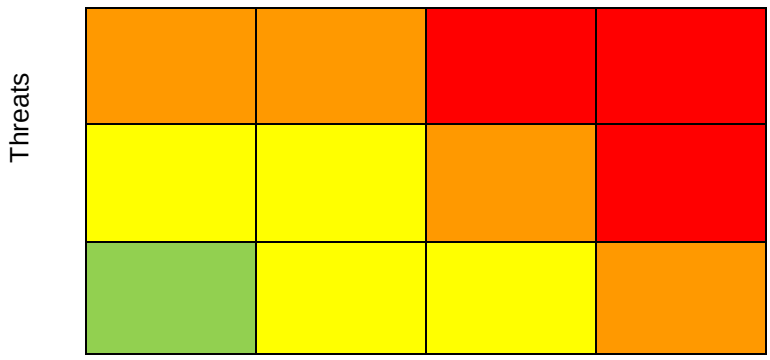
The grounds for detection in this sector are relatively straightforward, mainly in relation to cash payments or a subsequent suspicion regarding the contracting party's economic background, which often emerges in the case of late payment of premiums. For the predicate offences of fraud or participation in a criminal organisation, detection is primarily based on information received from a third party, particularly the prosecution authorities, e.g. if a vehicle is seized. Financial intermediaries in the sector do not use transaction monitoring tools.

Typologies
A. Following a request from a criminal prosecution authority in relation to an investigation concerning drug trafficking, a financial leasing company notified MROS that one of its clients had used its financing services to purchase three luxury vehicles within a six-month period, each of which exceeded CHF 100,000 in price. The official contracting party was a company managed by the person being investigated. For each vehicle, a cash deposit of between CHF 30,000 and CHF 40,000 had been paid. The suspicious activity report was forwarded to the competent prosecution authorities, and the person involved was convicted for offences against the NarcA but not money laundering.
B. Based on external information, a leasing firm learned that one of its clients, a company specialising in the sale and exportation of luxury cars, was actually operating at a loss. In fact, according to its own financial statements, the company had only survived the previous five years with funding from external sources. Additional enquiries revealed that the company's BO was closely associated with a leader of a notoriously corrupt regime currently involved in a civil war. The report was forwarded to the competent prosecution authorities, which dismissed the case due to insufficient evidence to initiate criminal proceedings.

Regarding consumer loans, the threat related to drug trafficking misdemeanours is greater than in financial leasing. Moreover, this field is exposed to a higher risk of terrorist financing. One pattern observed in the past involved a high number of small consumer loans taken out by persons resident in Switzerland under the influence of a movement considered by foreign authorities to be a terrorist organisation.

Assessment
The quantitative measurements suggest a fairly low risk level. Indeed, the cases reported have a very low degree of complexity and quite a high probability of detection, even if this takes some time to come to light. The amounts under investigation are generally between CHF 50,000 and CHF 100,000. In this sector, leasing transactions are less exposed to the risk of money laundering than consumer loans, mainly because of the increasingly limited possibilities of paying in cash, which could originate in drug trafficking, as opposed to the use of direct debit methods. Transactions are thus usually verified by a banking institution, which has additional transaction monitoring resources, and this helps to lower the risk. New business models emerging in this sector enable loans to be granted online, without any physical contact, making the task of identifying the BO more challenging.

Implementation of new legislative provisions introduced with the revised FATF recommendations will supplement the system for combating money laundering and terrorist financing in this sector, particularly with tighter obligations on all financial intermediaries to identify the BOs of legal entities. Therefore, the system does not require any additional regulatory measures for this sector.



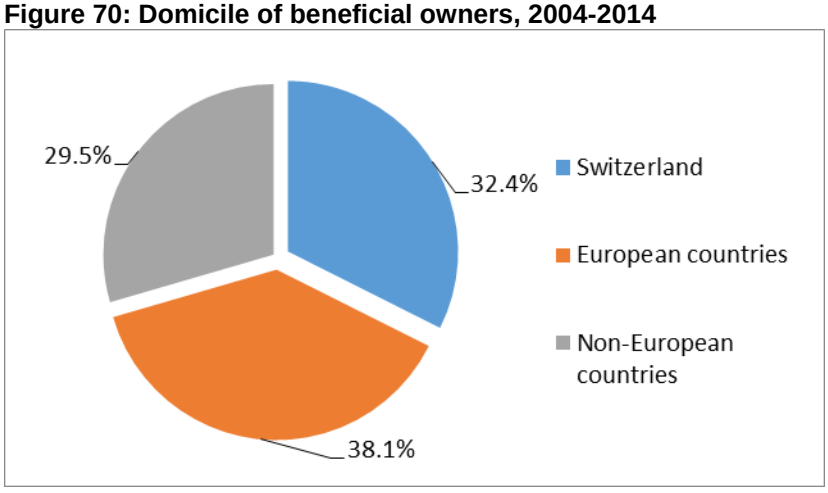
7.1.10 Payment transactions (credit cards, pre-paid cards, e-money)

In Switzerland, providers of services related to payment transactions on a professional basis are subject to the anti-money laundering system by virtue of Article 2 paragraph 3 letter b of the AMLA. This mainly concerns service providers in the field of credit cards and pre-paid cards and any providers in Switzerland offering to carry out electronic payments for the account of third parties.

A. Credit cards and pre-paid cards

An analysis of all credit card payments in Switzerland indicates a steady increase since 2004. The proportion of transactions made abroad is particularly high, accounting for 83.5% of all transactions in 2013[141]. Similarly, an analysis of the suspicious activity reports submitted to MROS between 2004 and 2013 shows that two thirds of the BOs involved in the reports filed by the sector are domiciled outside of Switzerland, with most of these in European countries (Figure 70).

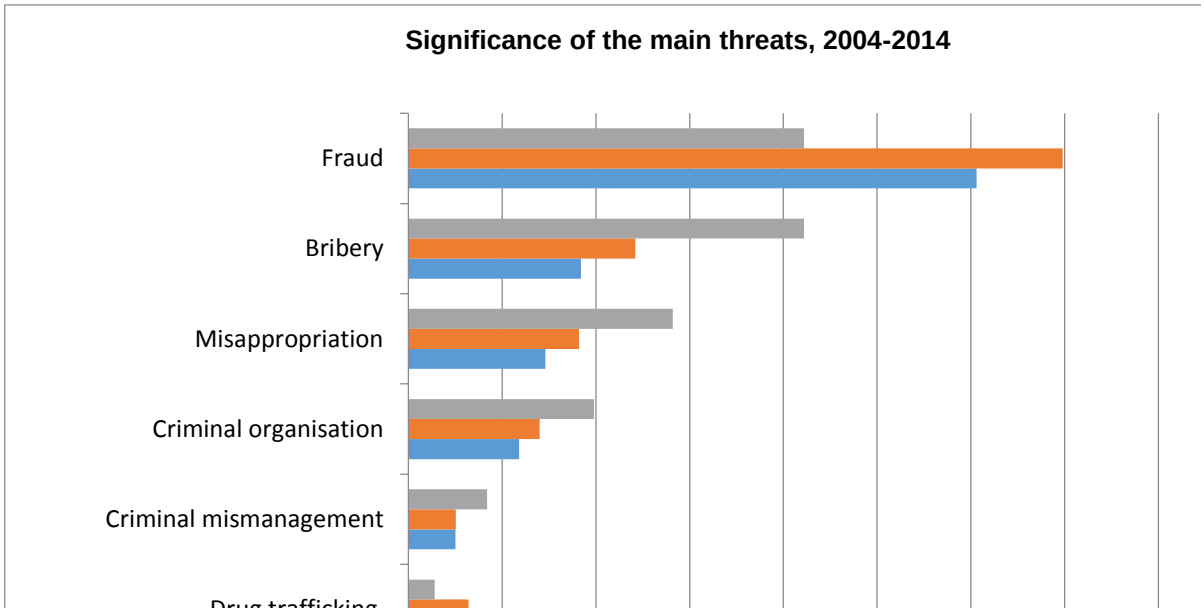
Figure 70: Domicile of beneficial owners, 2004-2014



The main suspected predicate offences reported by financial intermediaries in this sector are bribery, misappropriation, participation in a criminal organisation and weapons trafficking. The predicate offences of fraud and drug trafficking are less prevalent in this sector than in the financial sector as a whole (Figure 71).

Figure 71: Breakdown of the main predicate offences, 2004-2014

[141] SNB 2014



Suspicious cases in relation to credit cards are often detected at a late stage. In most cases, the suspicion arises through information from a third party, communicated to the financial intermediary by external sources or another financial intermediary, e.g. the bank that originally introduced the client.

Typologies

A. A credit card company was informed by a banking institution that one of its clients, a PEP and businessman operating in international trade, was wanted by Interpol on suspicions of fraud and criminal mismanagement in his country of origin. The bank's client had received two pre-paid cards from the credit card company, one in US dollars and the other in euros. The cards were regularly topped up using assets deposited at the bank in question.

B. A news report in another country stated that a client of a credit card company, domiciled in a European country, was involved in money laundering activities by way of precious stones on behalf of a criminal organisation operating in Asia. However, the correspondent bank, where the person under investigation had been a client for more than five years, had never noticed anything out of the ordinary. The criminal proceedings conducted by the Swiss authorities were ultimately closed due to lack of evidence.

C. A routine database search revealed that a recent client of a credit card company had been arrested in a Latin American country for participation in a criminal organisation. The business relationship was already known to MROS, which had received two other suspicious activity reports from two different banks several months beforehand.

B. Electronic payment services (e-money)

In general, as with credit card payments, the volume of transactions using electronic payment services is steadily increasing in Switzerland. These are generally used to pay small amounts. There is no clear, homogeneous definition of what constitutes electronic payments or e-money. The fundamental ambiguity lies in whether the emphasis is on the electronic nature of the transmission itself or the means of storing/depositing the money. For the present analysis, e-money may be defined as monetary assets with legal tender status stored in electronic form and accepted as a means of payment by other economic participants in a given transaction. In analysing the risks of money laundering and terrorist financing, a distinction should be made between e-money that uses electronic means primarily as a mode of transmission and e-money used for permanently storing assets in the form of electronic deposits. In the first case, assets having legal tender status are held on a bank account and gradually debited as electronic transmissions are made. In the second case, the assets are permanently stored on an electronic device, such as a microprocessor (i.e. chip), a network money system or a mobile phone (e-wallet). In performing the risk assessment, electronic payment services should be differentiated according to their primary purpose, i.e. payments between several individuals and payments made to acquire goods or services, depending on the significance of their current use and their potential use in the near future.

At present, the mode most commonly used by Swiss consumers is the electronic payment system without an electronic deposit (such as debit cards). The main risk with such electronic payment systems lies in their potential for laundering assets by way of non-existent commercial services, by

combining them with a business's standard products. The second most commonly used mode concerns electronic payment services with a permanent deposit, such as PayPal or WebMoney, enabling Swiss residents to make online payments. In parallel, the e-wallet is starting to be offered by service providers domiciled in Switzerland – a development that clearly lowers the risk, as such providers are subject to the AMLA. In any case, even when Swiss consumers use online or mobile electronic payment services of providers not domiciled in Switzerland, there is usually a link to a financial intermediary that is subject to the AMLA. The latter then makes the payment in ordinary currency to the electronic payment service for the client's account. Therefore, the main risk concerns the financial intermediaries themselves, insofar as they can act as relay agents for transnational fraudulent transactions or transactions serving no actual business purpose.

However, it is not possible to measure the real threat in Switzerland with respect to electronic money used in the form of network money, given that no specific cases have been reported by banking institutions in Switzerland. Currently, the levels of regulation and supervision of the electronic payment services available in Switzerland differ according to the geographical base of the electronic payment service provider in question. It is therefore possible for Swiss consumers to make online payments using foreign electronic payment services that are not subject to any anti-money laundering regulations or which are not subject to a system equivalent to that in Switzerland. On the other hand, economic players in Switzerland wishing to offer electronic payment services online to Swiss and foreign consumers are subject to a twofold verification process, as they are deemed financial intermediaries under the AMLA. In this respect, no distinction is made between financial intermediaries in Switzerland offering this type of online payment services and ordinary financial intermediaries regarding the nature of their due diligence and supervisory obligations.

Based on the present analysis, it can be concluded that the electronic payment services most exposed to the risk of money laundering in Switzerland are foreign-based service providers offering e-money in the form of network money. As these are not subject to the provisions of the AMLA or to FINMA supervision, it is difficult for the prosecution authorities to follow the paper trail of transactions made with such service providers. The risk is higher in the case of payments between private individuals and also where the means of payment allows for cross-border payments.

C. Virtual currencies

At present, the real threat in relation to virtual currencies, such as Bitcoin, is low in Switzerland. Very few financial intermediaries in Switzerland offer payment services and terms in virtual currencies[142]. Despite the virtual anonymity offered by virtual currencies, financial intermediaries – being subject to the anti-money laundering provisions under Article 2 paragraph 3 of the AMLA – are required to lower the risk for such payments by identifying their contracting party and carrying out further checks as part of their due diligence obligations.

Nonetheless, there could be a rapid rise in the number of economic players wishing to accept payments in virtual currencies. Therefore, the main potential threat in relation to virtual currencies lies in the growing number of financial intermediaries in Switzerland that will accept to exchange virtual currencies for non-virtual currencies on a large scale on behalf of their clients, whether in the form of book money or cash. The virtual mode means that the person depositing virtual currencies is not necessarily the same as the recipient. The second potential threat associated with the use of virtual currencies in Switzerland is in their use for transferring money abroad, instead of traditional money-transmitting services, thereby eliminating the need for a financial intermediary. For criminals, the main attraction in transferring money by way of virtual currencies lies in the possibility of concealing the identity of the persons depositing and receiving the funds. The fundamental principle underlying the functioning of virtual currencies is the fact that transactions using this currency do not need an intermediary to guarantee the terms of exchange, replacing them by cryptographic elements. The main potential threats associated with virtual currencies in terms of the predicate offences seen worldwide are in relation to drug trafficking, money laundering activities carried out by criminal organisations, online fraud, including the financing for setting up phishing websites, and terrorist financing. As yet, however, the real threat remains low in Switzerland.

Assessment

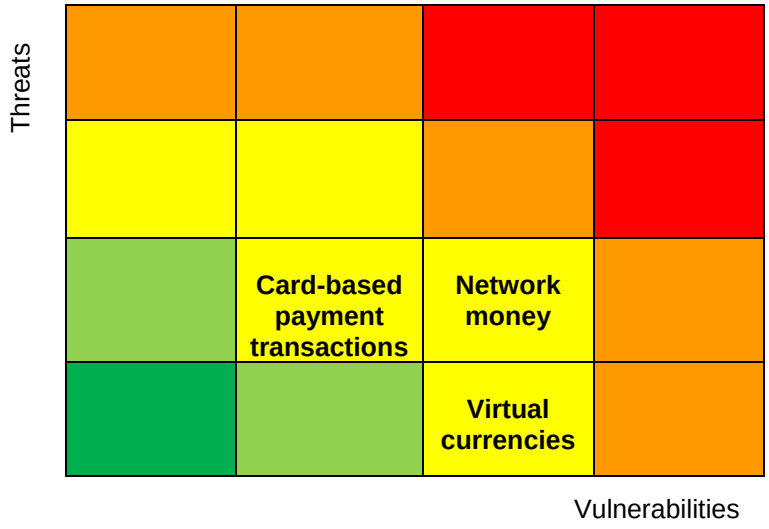
The quantitative measurements indicate a moderately high threat level for this sector, which is directly comparable with the banking sector. However, the risk in relation to the size of the amounts concerned

[142] Federal Council report on virtual currencies in response to the Schwaab (13.3867) and Weibel (13.4070) postulates

and the direct involvement of domiciliary companies is lower than for banking, as most of the transactions involved are for small amounts of money.

The main vulnerability in the sector as a whole lies in the proliferation of computerised payment service providers, which are not subject to the AMLA because they are domiciled in a foreign jurisdiction but are used by Swiss residents to make online payments (network money).

Despite the delay in detecting some cases, the traceability of credit card transactions is excellent when the assets are deposited with a bank. Also, although electronic payment services may be used in money laundering by using funds to pay for non-existent or overpriced business services, this risk is mitigated by the monitoring by banks holding the assets, which are subject to the AMLA. The vulnerabilities of the financial intermediaries in the sector thus appear to be under control. In this respect, implementation of new legislative provisions introduced with the revised FATF recommendations will strengthen the mechanism for the sector, particularly with tighter obligations for financial intermediaries to identify the BOs of legal entities. The mechanism therefore does not require any additional regulatory measures for financial intermediaries in the sector subject to the AMLA.



7.1.11 Trade in precious metals

Switzerland's precious metal trading sector is of global significance. This sector is subject to the AMLA by virtue of Article 2 paragraph 3 letter c of the AMLA. Moreover, under the Federal Act of 20 June 1933 on the Control of the Trade in Precious Metals and Precious Metal Articles (PMCA)[143], licences to operate in this sector are granted subject to the fundamental condition of a guarantee of proper business conduct (a condition that also applies to the banking sector by virtue of Art. 3 para. 2 letter c of the BankA). Furthermore, the Ordinance of 8 May 1934 on the Control of the Trade in Precious Metals and Precious Metal Articles (PMCO)[144] defines precious metals in terms of purity criteria and requires the holders of a melters licence to verify the lawful origin of the melt material, to adhere to the regulations of the AMLA and to keep records of their purchases (Art. 168 letters a to c of the PMCO).

[143] SR 941.31

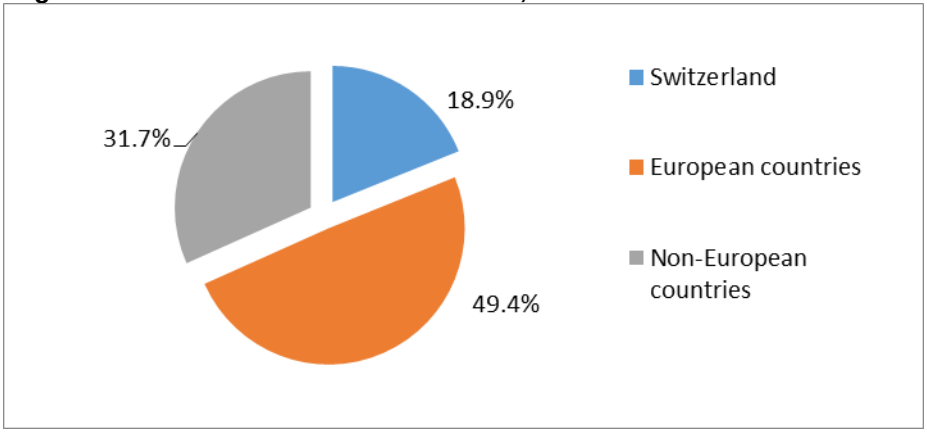
[144] SR 941.311 Pursuant to Article 178 paragraph 2 of the PMCO, banking precious metals are: (a) ingots and granules of gold with a minimum fineness of 995 parts per thousand; (b) ingots and granules of silver with a minimum fineness of 999 parts per thousand; and (c) ingots and sponges of platinum or palladium with a minimum fineness of 999.5 parts per thousand. Cf. also FINMA Circular 2011/1 on the activity of the financial intermediary within the meaning of the AMLA, Margin no. 75 to 79

Gold trading holds a dominant position in this sector, accounting for up to two thirds of the global trade in gold. Around 40% of global refining capacities are covered by Swiss gold refineries[145]. Four of the world's nine leaders in the sector concentrate their operations in Swiss refineries. Most of the gold imported into Switzerland is in the form of raw gold (gold ore or doré bars), non-monetary gold (gold dust) or waste. The refineries in Switzerland refine gold extracted from mines or melt down existing items made of gold. Thus, unlike Swiss trade in other precious metals, the gold traded and refined in Switzerland actually transits physically through the country.

The potential threat of money laundering in the sector comes in two forms: first with respect to the origin of precious materials, which may be unlawfully acquired, e.g. through bribery, theft or another offence, and secondly in the direct use of precious materials for laundering purposes or as financial vehicles to finance other felonies.

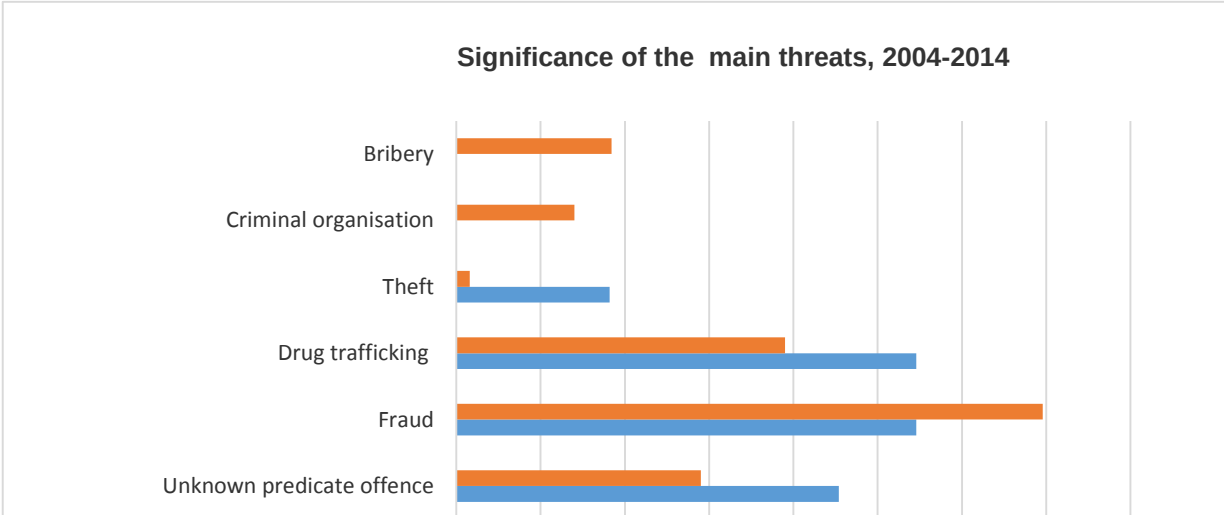
This sector has a low rate of reporting, with only one to three suspicious activity reports filed each year. In more than 80% of cases, the domicile of the BO of the reported business relationship is located outside of Switzerland, mainly in another European country (Figure 72).

Figure 72: Domicile of beneficial owners, 2004-2014



The suspected predicate offences primarily concern assets from suspected drug trafficking, theft or fraud in the acquisition of precious metals. Compared with the financial sector as a whole, the major threats in relation to bribery and participation in a criminal organisation are not a factor here. The absence of reports concerning these two threats would seem to contradict the sector's potential attractiveness to criminals, given the possibilities of reducing traceability, e.g. by melting down items, depositing them and moving assets around. The proportion of unidentified predicate offences is particularly high in this sector (Figure 73).

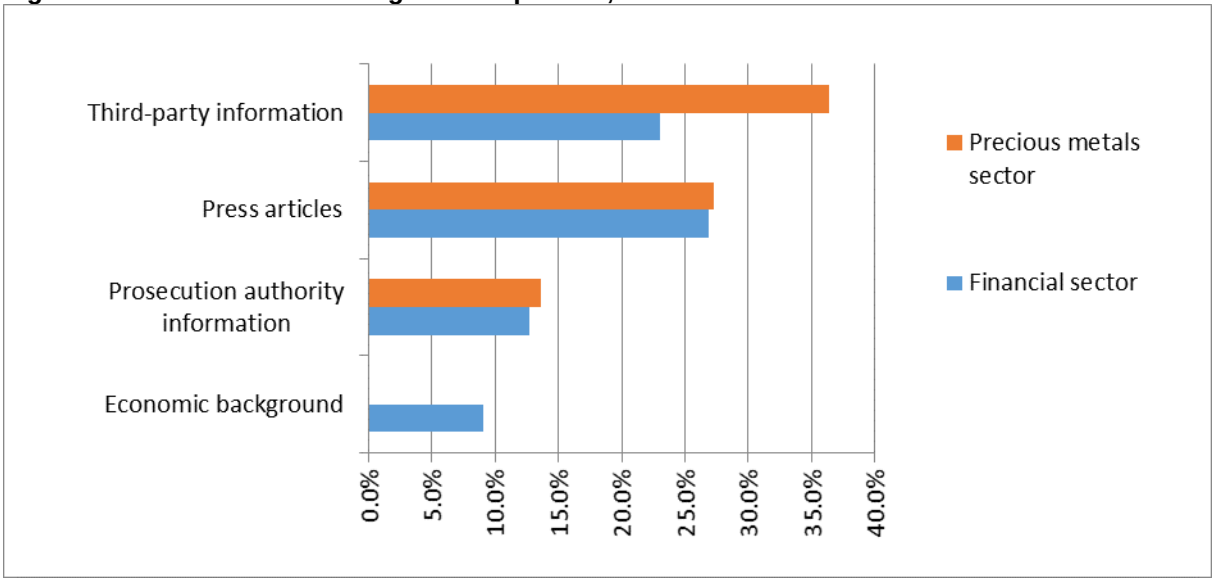
Figure 73: Breakdown of the main predicate offences, 2004-2014



[145] World Gold Council 2013

An analysis of the origin of suspicions reported to MROS indicates that the sector relies predominantly on information from third parties, such as news reports or local contacts. Generally speaking, few suspicions have their origin in the financial intermediaries' own research, such as detailed transaction monitoring or the economic background (beyond the obligation to disclose the BO) (Figure 74).

Figure 74: Grounds for and origin of suspicions, 2004-2014



The majority of sales in precious metal trading involve commercial enterprises buying gold ingots, in particular, for commercial and investment purposes (e.g. investment funds) or sales to the jewellery and watchmaking industry. The sale of precious metals to individuals thus seems to be limited. However, some traders in precious metals offer individuals the possibility of acquiring precious metals, even online, and/or storing them in safe-deposit boxes with a financial intermediary in Switzerland. In such cases, these financial intermediaries ask their clients to provide a declaration of the BO of the assets used to acquire the precious metals, using Form A.

Among commercial enterprise clients, the widespread use of complex corporate structures in the sector makes the task of identifying the real BOs considerably more challenging. In fact, to the extent that the business relationship actually involves intermediaries, as found by the sector, the retention and disclosure of data concerning their own providers is not guaranteed. This vulnerability primarily comes to the fore in the second part of the threat, when the financial intermediaries in the sector have to make payments for the account of their clients to legitimate structures or to third parties who are actually associated with their clients, e.g. to buy the precious metals to be refined. An analysis of the origin of suspicions shows that the sector has limited possibilities for researching its clients' economic backgrounds and for transaction monitoring.

With a view to reducing the first potential threat, most refineries subject to the AMLA as financial intermediaries also voluntarily submit to one or more international standards requiring them to perform checks throughout the entire supply chain. The leading international initiatives implemented by players in this sector are the Responsible Gold Guidance of the London Bullion Market Association and the Code of Practices and the Chain-of-Custody Standard issued by the Responsible Jewellery Council.

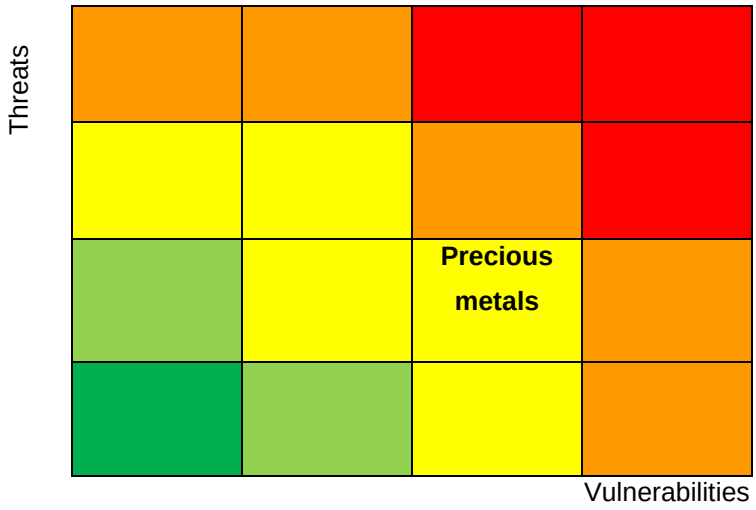
Assessment

Given the importance of precious metal trading in Switzerland, and the attractiveness of this sector for money laundering purposes as well as the complexity of the structures involved, the quantitative measurements suggest that the threat in the sector is underestimated, particularly with respect to the predicate offences of bribery and participation in a criminal organisation. This mainly concerns the second threat (see above), regarding the use of precious materials, frequently gold or precious stones, as vehicles for laundering assets of criminal origin. As these cases concern stages II and III of the money laundering process, often involving complex structures, the potential for detection is lower than for the second threat concerning precious materials acquired by criminal or unlawful means. In fact, in parallel with their obligations under the PMCO, most financial intermediaries in the sector have submitted themselves voluntarily to additional international due diligence standards, with verifications

that go beyond the requirements of the AMLA in terms of their familiarity with and monitoring of business relationships; this has a corresponding mitigating effect on the sector's vulnerability with respect to the first threat. Regarding the purchase of gold ore, the verifications made may take the form of onsite visits, an audit of the financial statements of the mines and their licences, an assessment of mining practices and requests for letters of recommendation. In specific cases, the presence of the first threat does not necessarily rule out the second. However, for refineries operating in Switzerland, the second treat is limited to a certain extent, given that most of their clients are institutional in nature.

Moreover, unlike the trade in gold ore or items such as ingots, which is subject to various forms of checks, the purchase and sale of old gold is completely unlicensed and not subject to the provisions of the AMLA. The volume of old gold being sold by individuals in Switzerland, mainly in exchange for cash, has risen sharply since 2009. It should be noted in this respect that Swiss refineries purchase only very low volumes of such materials directly from the buyers of old gold on account of their due diligence obligations. A large part of the old gold bought in Switzerland is probably sold abroad. This constitutes a vulnerability, as it means some of the trade in gold in Switzerland remains outside of the provisions of the AMLA. As a result, there is a greater probability of certain threats of money laundering and terrorist financing actually materialising. However, in light of the small amounts involved, such threats are mainly in relation to the predicate offences linked to street crime in Switzerland and abroad, such as theft, offences against the NarcA and fraud. Likewise, given the similarity with regard to the attractiveness and potential threats concerned, the risk of money laundering inherent to the overall sector of precious materials could shift to other trading activities not subject to the AMLA to the same extent as precious metals, such as the trade in precious stones.

In this respect, the new requirements of the AMLA, as of 1 January 2016, for traders to perform due diligence regarding commercial transactions of more than CHF 100,000 in cash (verification of the identity of the contracting party and identification of the BO and, if the transaction seems unusual, clarification of the origin of the assets), or for the transaction to be carried out via a financial intermediary subject to the AMLA, are likely to mitigate the risk in this sector and prevent any intensification of the shifting of assets. Furthermore, for financial intermediaries in the sector subject to the AMLA, the implementation of new legislative provisions will strengthen the system for combating money laundering and terrorist financing, particularly measures to improve the transparency of legal entities and tighter obligations on all financial intermediaries involved in a business relationship to identify the BOs of business relationships.



7.2 Analysis of the areas of activity not subject to the AMLA

7.2.1 Real estate sector

Money laundering in the real estate sector is a current topic that has been regularly making the front page in the media for some years, particularly in regard to spectacular purchases of real estate by citizens of the Commonwealth of Independent States (CIS). It was even assumed that organised crime

and some corrupt autocrats were using the Swiss real estate market to launder their funds. This question gave rise to several parliamentary initiatives being tabled.

Attraction of the real estate market for money laundering
Four factors have been identified which make the real estate market attractive for money laundering:

1. Real estate business allows above-average sums to be injected, including in cash. Furthermore, illegal transactions also benefit from the fact that the real value of residential property located in a privileged area, for example in the Lake Geneva or Lake Zurich regions, is difficult to determine.
2. In principle, residential property is an attractive capital asset because it is a sound investment, particularly in times of economic difficulty. It is not exposed to currency effects and can be rented profitably.
3. Real estate business provides numerous opportunities for money laundering because money of criminal origin can be used not just to purchase property but also for financing and operations and for refurbishment work, as the by no means exhaustive list of modi operandi below shows.
4. Contrary to what prevails in the EU, real estate business in Switzerland is not subject to anti-money laundering legislation for reasons inherent to the system adopted. The AMLA exclusively governs financial intermediation in general and not specific business activities. Real estate agents and notaries are thus not obliged to verify the origin of the funds used[146].

Possible modi operandi
There is a wide variety of possible modi operandi in the real estate sector and they may be used in any combination or modified.

- Cash injections: real estate presents many opportunities to invest cash, in particular:
  - purchase of real estate in cash;
  - rental payments (or rental deposits) in cash[147];
  - payment of refurbishment, renovation, conversion or extension work in cash;
  - investments in rental properties, restaurants or hotels (cash intensive businesses). These activities can then open up other possibilities for systematic money laundering because the funds of illegal origin can then be presented as rent revenues or operating revenues from restaurants or hotels.
- Mortgages: as investments that are considered safe, real estate allows funds to be obtained from financial institutions in the form of mortgages, which is particularly attractive for money launderers who need legal funds. Various possibilities can be considered:
  - cash payment for the property (by means of funds to be laundered), then taking out a mortgage;
  - taking out a mortgage, then amortisation or payment of the interest on the latter using the funds to be laundered;
  - to avoid using a banking institution as a credit provider, criminals can also grant each other loans intended for the purchase of property. The origin of the funds can subsequently be disguised by resorting to frontmen or bogus companies which usually have international links (loan back schemes).
- Inflated prices: the more expensive something is, the more money can be invested[148]. Criminals can in this way sell the same property several times in succession to the same BO as part of a group or by way of third-party companies, obtaining a higher selling price with every new transaction (domino effect).
- Purchase of real estate through complex international company or holdings structures: each

[146] The real estate agent is deemed to act in the capacity of a financial intermediary and must consequently meet the due diligence obligations resulting from this only when he transfers the amount of the sale price to the seller on the purchaser's instructions and if it is not related to services rendered subsequently. By contrast, debt collection by real estate agents at the seller's request is not subject to the AMLA (Section 129 of the FINMA Circular 2011/1, Financial Intermediation under the AMLA).

[147] Sales-based rents are particularly suitable because they vary and provide money launderers with a high degree of flexibility.

[148] However, money laundering is often not the only or main motive to acquire real estate at an exorbitant price. The discretion which must necessarily surround these transactions admittedly results in additional costs for the money launderer, but it can also be assumed that the purchase of property in the higher price category is primarily a matter of prestige.

interposed company makes it more difficult for the prosecution authorities to trace laundered funds because the ownership structure of each of the companies has to be clarified. Another obstacle for investigations is the international dimension of the networks of companies, which means that the information required can only be obtained by mutual assistance. However, this process is often very long and sometimes does not even produce any results. Moreover, real estate can also be used as a contribution in kind during the creation of a company limited by shares. They are thus transferred to the company and the BO must then be identified.

The money laundering situation in Switzerland in the real estate market

The analysis of some 40 preliminary investigative procedures and investigative procedures – both ongoing and closed cases – relating to cases of alleged money laundering in the Swiss real estate market shows that trade in real estate is very attractive for money launderers and suspicious cases are regularly observed in Switzerland. Much of this is the purchase of high-end residential property. The funds laundered on the real estate market originate mainly, and in roughly equal proportions, from the following three predicate offences: fraud/misappropriation, support for and participation in a criminal organisation, and violations of the Narcotics Act. The cases analysed often have an international dimension primarily because the predicate offence was committed abroad in the majority of these cases. The analysis also shows that the modi operandi are not as complex as described in specialist literature. Most of the properties are purchased through banking transactions and partial financing by the bank concerned is commonly used. If cash purchases of property have only been observed in a few isolated cases, partial cash financing and cash payment of rental costs and conversion work are not uncommon. Moreover, it would appear that in most cases, the prime objective of purchasing real estate is not to hide any traces documenting the origin of the assets involved, but to simply use these assets. Cantonal statistics show that only a small proportion of real estate purchases are made by companies, whereas in the money-laundering cases analysed, the purchaser is very often a company. This difference leads to the conclusion that companies are more often involved in purchases of real estate to launder money than ordinary real estate transactions. In a few cases, the company was even created solely with an eye to purchasing real estate and does not perform any operational activities, which strengthens the suspicion of money laundering. The purchase of real estate by a company does not in itself give any grounds for suspecting money laundering, but if there are other indications on top of this, the suspicion of money laundering may be well founded.

Other indicators of money laundering activities are, for example, an exorbitant price as well as excessive alteration or expansion plans, which are not economically feasible in the eyes of the experts or cannot be achieved for reasons concerning the protection of historic monuments. Finally, suspicions should also be aroused by properties that remain vacant for long periods of time for no apparent reason or by restaurants or hotels that operate for many years in spite of a blatant lack of customers.

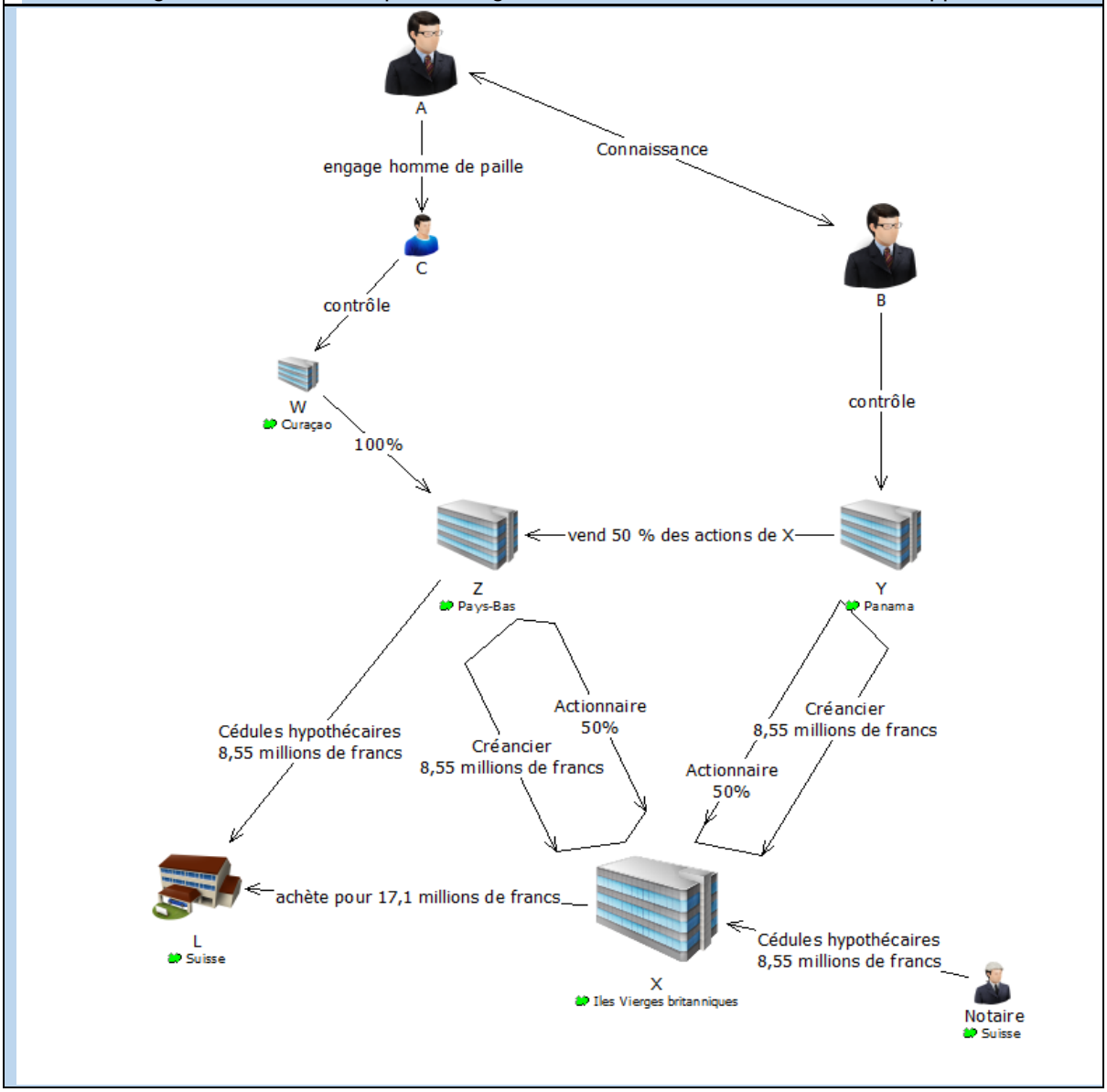
Although the real estate market is particularly attractive for money laundering, the analysis of the investigative procedures also leads to the conclusion that it is not more affected by this phenomenon than other sectors, such as trade in luxury goods. However, given that the figures on money laundering are, by definition, patchy, it cannot be stated with absolute certainty. Furthermore, the purchase of luxury goods does not have the same societal impact as that of purchasing residential real estate because housing is a basic need for the population and any increase in prices has negative consequences for a large part of this population. The availability of housing is already inadequate in a number of areas across the country and is going to become even scarcer. In this context, the feeling that this shortage is made even worse by money laundering may have an adverse effect on the social fabric, even if this sentiment is objectively unfounded. Moreover, investments in hotels and restaurants not only provide new opportunities for criminals to launder money, but increase still further the number of jobs that they control. Money laundering is thus an even more serious general threat in the real estate sector than is the case in other business sectors.

Money laundering cases based on the real estate business do not make specific demands on the prosecution authorities. Their analysis shows that providing proof of a real estate transaction only poses problems in very rare cases. It is often these suspicious real-estate transactions which spark initial suspicions of money laundering and lead to the opening of proceedings. As with most money-laundering cases, the biggest difficulty to overcome amongst those affecting the real estate sector is that of proving the criminal origin of the assets concerned, in particular when the predicate offence was committed abroad.

Typologies

Scenario 1: purchase of real estate using a complex company structure

Suspect *A* is accused of having benefited from his position as a manager in the national oil company of an oil-producing country to enrich himself illegally. Some of the criminal assets passed through different companies to finally be used by a frontman to acquire property in Switzerland. In a simplified form, the purchase consisted of the following steps: company *Z* (with its registered office in the Netherlands) purchases from company *Y* (in Panama) 50% of the shares in company *X* (British Virgin Islands). Behind company *Y* we find *B*, an acquaintance and presumed accomplice of *A*. Company *Z* is owned in full by company *W* (Curaçao), which in turn is owned by *C*, who has been a confidant and frontmen of *A* for many years. Company *X* existed up to now only on paper and has never conducted any operational business. As a result of the sale, 50% of it now belongs to company *Y* and the other 50% to company *Z*. The authorised signatory is a confidant of *B*. As the first and only transaction, company *X* purchases property *L* for CHF 17.1 million, which are loaned to it from company *Y*. Once the purchase has been completed, company *Z* loans CHF 8.55 million to company *X* and obtains in return a mortgage note on property *L* for the amount lent. Company *X* then transfers this amount to company *Y*. The situation of company *X* is thus as follows: company *Y* and company *Z* are shareholders holding 50% each and also have a claim of CHF 8.55 million each. *Z* holds a mortgage note on property *L* for CHF 8.55 million, the remainder has been deposited with an attorney at law in Switzerland. In the meantime, the property has been demolished and the media is reporting that *A* and *B* intend to replace it with a luxury hotel. The competent criminal prosecution authority has submitted a request for mutual assistance to the country in which the suspected predicate offence was allegedly committed. However, the investigations carried out on the spot conclude that the accusations made against *A* are groundless and that the money transferred to Switzerland is of legal origin. Due to lack of evidence as to the criminal origin of the assets, the proceedings initiated in Switzerland have to be dropped.



Engage homme de paille = employs frontman
Connaissance = acquaintance
Contrôle = control
Panama
Créancier, 8,55 millions de francs = lender, CHF 8.55 million
Actionnaire 50% = 50% shareholder
Cedules hypothécaires = mortgage note
Notaire Suisse = Swiss attorney at law
Iles Vierges britanniques = British Virgin Islands
Suisse = Switzerland
Acheté pour 17,1 millions de francs = purchases for CHF 17.1 million
Pays-Bas = Netherlands
Vend 50% des actions de X = sells 50% of X's shares

Scenario 2: purchase of a plot using funds from drug trafficking
In 2008, *A*, a Swiss fiduciary, and *B*, a high-ranking member of an international drug trafficking gang, meet through a mutual acquaintance. *A* is looking for funds to purchase a plot on which he would like to build several luxury villas. *B* is looking for a way to invest and launder his money from trafficking cocaine between Brazil and Switzerland. *A* creates several bogus companies and receives cash totalling CHF 1.2 million from B in two instalments. He then transfers almost CHF 400,000 in his name to the account of one of these companies and uses this to buy an apartment in São Paulo for *B*. In addition, *A* deposits the remaining CHF 800,000 with a Swiss attorney at law, and by contributing a further CHF 200,000 from his own funds, he obtains a mortgage of CHF 1.5 million from a Swiss bank. He then purchases the plot in the name of one of the bogus companies for the sum of approximately CHF 2.5 million. In 2009, *B* is convicted of drug trafficking by a Brazilian Court and is sentenced to 33 years in prison. In 2013, *A* is convicted in Switzerland under simplified proceedings of money laundering and the forgery of documents and is given a conditional monetary penalty and fine.

Assessment
This analysis shows that the real estate sector is exposed to a threat which can be considered moderate. There is a risk particularly of funds obtained from acts of bribery committed abroad or from organised crime being laundered in Switzerland. Even though the real estate sector as such is not subject to the AMLA, control is nonetheless provided in the majority of cases by the financial intermediaries involved in the transactions, primarily by banks and fiduciaries. Moreover, given that criminal assets are in general laundered not only on the real estate market but also via other channels, the result is a slightly increased probability of detection. From 1 January 2016, the revised AMLA also makes provision for any cash transaction exceeding the amount of CHF 100,000 to be carried out using a financial intermediary, failing which, the trader must verify the identity of the contracting party, identify the BO and, if the transaction seems unusual, clarify the origin of the assets. This system aims to reduce the risk of money of criminal origin being laundered for the purpose of buying and selling real estate in Switzerland.

Finally, real estate transactions performed using complex structures, based on domiciliary companies for example, or by taking advantage of business dealings with financial intermediaries abroad often allow the BO to be concealed. For this reason, a proposal to amend the CC makes provision for ensuring the uniform and unequivocal identification of people through the use of the AHV number, which will also allow searches to be carried out for property in Switzerland. This will result in greater transparency in the ownership structures of real estate property and a reduction in the risk of criminal money being discretely laundered on the Swiss property market[149].

7.2.2 Non-profit organisations (NPOs)

Basics
In Switzerland NPOs are generally referred to as public benefit organisations or non-profit making organisations or institutions in accordance with the FATF recommendations. Generally speaking, these organisations have the status of a foundation or an association. However, their character as a public utility does not depend on the legal form of the organisation but on the relevant criteria in tax law.

a. Association

[149] BBl 2014 3429 (Art. 949c [new] CC)

An association has a legal personality and is made up of a general meeting and a committee elected by the general meeting. Its statutes must be drawn up in writing and contain the necessary provisions on its goals, resources and organisation. Apart from these requirements, the creation and running of an association is rarely subject to any other requirement. An association does not require authorisation or share capital, does not have to be registered, and is not subject to supervision or audits[150]. As a result, if the association is not entered voluntarily in the commercial register or registered with a certification body, the authorities do not have any information on its members, its financing or its activities, unless it obtains them by coercive measures.

b. Foundation

A foundation is established by the allocation of assets for a particular purpose. Its most common form is that of the foundation in the traditional sense. Its supreme organ is generally the executive committee, which represents and manages it. Compared to the association, the creation and operation of a foundation must meet more requirements and as a result, the authorities have more publicly accessible information. Apart from family foundations, all foundations must be listed in the commercial register and must keep accounts and have them audited[151]. Depending on whether the foundation's purpose has a local, cantonal or (inter)national scope, it is the respective responsibility of the commune, the canton or the Confederation to monitor that this purpose is pursued in conformity with the wishes of the founder and the articles of association. When there are shortcomings in the organisation or in the committee of the foundation, the competent supervisory authority can take preventive and repressive administrative law measures. Preventive supervision instruments include most notably an audit of the annual financial statements, approval of regulations and amendments to them as well as amendments to the articles of association. As for repressive instruments, these range from warning of the dissolution of the foundation to freezing its accounts and revocation of the executive committee.

c. Public benefit

According to the definition of the FTA, there Is a purpose of public benefit when both of the following elements are fulfilled: firstly, the organisation must serve public interests, which means that the circle of participants must be open and must not be restricted, for example, to a family or members of a given profession; secondly, the activities of the organisation must be *selfless*. This means they must not serve the organisation's own interests as a legal entity nor those of its members.

d. Statistical data

Based on a major international study of the non-profit organisation sector conducted in 2008[152], it is estimated that Switzerland has approximately 90,000. They employ around 180,000 people (in FTEs) and generate around 4.7% of the country's GDP. Added to this is the work of volunteers, which corresponds to approximately 80,000 full-time employees.

Vulnerability of non-profit organisations to money laundering and terrorist financing

Specialist literature considers NPOs to be attractive vehicles for money laundering and terrorist financing for various reasons: firstly, NPOs benefit from overall confidence, particularly public trust, to the extent that financial intermediaries, the supervisory authorities, customs authorities and the prosecution authorities do not consider them to be a risk category a priori and do not submit their financial transactions or transportation of goods to any special inspections. Secondly, these organisations often have access to considerable financial resources, including cash, in various foreign currencies. Moreover, incoming payments carried out in a wide variety of ways and which may have varying orders of magnitude, a large number of donors (some of them foreign) and payments involving large sums in cash are part of the typical profile of NPOs as bank clients and do not as a result attract any attention. Thirdly, a large number of non-profit organisations operate internationally, including in countries where the rule of law is weak and bribery is common. Taking into account the diversity of the regions, the partners, the activities, the cultures and the legal systems concerned, as well as the sometimes con-

[150] Associations which operate a commercial business to achieve their purpose are the exception. They must be listed in the commercial register (Article 91 of the Commercial Register Ordinance of 17 October 2007, CRO; RS 221.411). All other associations are free to do so. However, if two of the three figures specified in Art. 69*b* of the CC (total assets of CHF 10 million; turnover of CHF 20 million; average annual total of 50 full-time staff) are exceeded in two successive business years, the association must submit its accounts to a full audit by external auditors and must also be entered in the commercial register.

[151] In addition to family foundations, ecclesiastical foundations are also exempt from the duty to appoint external auditors and to be entered in the commercial register.

[152] Cf. Bernd Helmig et al.: Der dritte Sektor in der Schweiz. Länderstudie zum John Hopkins Comparative Nonprofit Sector Project, 2010

siderable distances, it is therefore difficult to exercise appropriate control over the resources of non-profit organisations. Fourthly, as these resources are somewhat limited, non-profit organisations only spend a minimum amount of money on administrative tasks, primarily on managing their accounts and on internal controls. In a number of cases, this work is conducted somewhat informally by staff members with rudimentary technical knowledge. Very few non-profit organisations have compliance mechanisms, a code of conduct or other similar regulations in place. Finally, in particular in Switzerland, associations are not subject to any controls and only a few are required to have their accounts audited by an auditor. Without coercive measures ordered by a public prosecutor, it is often impossible to obtain information on the organisation, members of staff and financing of an association.

Situation in Switzerland relating to money laundering and terrorist financing through non-profit organisations

Although non-profit organisations are attractive for terrorist financing and in spite of the considerable evidence on this topic gathered in particular in the USA in the wake of the September 11 attacks, known cases of money laundering or terrorist financing by non-profit organisations are few and far between, and cases where such criminal acts were brought before the courts are even fewer. The risk of abuse should therefore not be confused with actual abuse. The difference between the risk of abuse and actual abuse can be explained by the fact that there are considerable gaps in the data available. As NPOs are not subject to practically any controls in Switzerland or to any supervisory mechanisms, evidence of criminal acts often goes undetected.

In practice, it appears that non-profit organisations typically do not finance specific terrorist acts but tend instead to support terrorist groups as a whole (logistics and infrastructure). In the majority of cases, these groups have a political or social arm, which is allegedly non-violent, and a paramilitary arm. Their operations in numerous sectors are accompanied by quasi-state activities to the extent that it is almost impossible to determine to which specific projects the money concerned has been allocated. This difficulty is only exacerbated by the fact that terrorist financing is often sustained by transfers of small amounts via alternative, informal remittance systems.

In Switzerland, the non-profit organisations which pose a risk of terrorist financing are to be found mainly in Islamic-nationalist or Jihadist circles and even ethnic-nationalist circles. Although the existence of contacts or links between NPOs operating in Switzerland and terrorist structures has been recognised in several suspicious cases, it has scarcely been possible up to now to confirm the suspicions of terrorist financing which have been sparked.

Typologies

Scenario 1: charitable financial agents

The example shown here is a big international case involving phishing and money laundering carried out using financial agents[153]. The people responsible for the phishing attacks, who were probably based in Russia or the Ukraine, claimed they were collecting money for *A*, an alleged charitable cause for children with its registered office in Poland, and supported their claims with a website which at first glance seemed authentic enough. However, closer examination quickly revealed that the texts had been copied directly from the websites of genuine charitable organisations. The financial agents had been recruited through job advertisements and instructed to make their own bank accounts available for incoming money. They then had to withdraw the donations received as quickly as possible, in cash, and send them to a recipient in Russia via a money transmitter. They were entitled to a commission of 10% of the amounts transferred. During 2007, several reports concerning this matter were received by MROS, which forwarded them to the competent cantons. The website of the alleged charity was subsequently closed down. The criminal investigation of the financial agents was closed for most of the cases because these people could not have known that the money was of illegal origin, which meant the constituent, subjective element of the offence had not been satisfied. The criminal investigation against the perpetrators of these phishing attacks also had to be closed.

Scenario 2: Islamic non-profit organisation with links to an Islamic-nationalist organisation in the Middle East

In 2003, the Swiss authorities established a link between *A*, a Swiss NPO, and terrorist financing. Established in 1994 as a branch office of the parent organisation in France, at that time *A* was the biggest, Swiss non-profit organisation operating in the area of aid for the Middle East. It had offices in Geneva and Basel and collected donations in the mosques and Islamic centres which would subse-

[153] People generally recruited through advertisements who, in exchange for payment, make their bank accounts available for incoming payments and then transfer the money abroad in line with the instructions received.

quently be sent to NPOs in the Middle East. According to one of the founders and secretary of the organisation, the sums in question represented annual amounts of between CHF 0.5 and CHF 1 million up to 2002. *A* claimed that these donations were used to support orphans, people with disabilities or those in need as well as agriculture and infrastructure projects.
Like other NPOs providing assistance to the Middle East, *A* was accused of indirectly supporting terrorist activities to the extent that it sent donations to organisations which reputedly carried out such activities. In 2003, the US Treasury identified five NPOs which had links to organisations in the Middle East as being Specially Designated Global Terrorists. These NPOs included not just the parent organisation of *A* in France but also *A* itself in Switzerland. Since then, *A* has been on the US Treasury's list of Designated Charities and Potential Fundraising Front Organizations for Foreign Terrorist Organizations because it is one of the primary fundraisers operating for a terrorist organisation in the Middle East. *A* then also appeared, under a number of aliases, on a list called the "Bush list" which was published by the former Anti-Money Laundering Control Authority (now FINMA).
From 2003 to 2004, *A* was at the centre of Federal Criminal Police investigations, which failed, however, to gather evidence of terrorist financing that could be used in court, as is often the case with NPOs. The NPO *B*, subsequently renamed *C*, was created in 2004 to replace *A*. In 2007, based on a report sent to MROS indicating suspicious money transfers from *A* and *B* to the Middle East, the Office of the Attorney General of Switzerland (OAG) opened a judicial police enquiry against persons unknown on suspected terrorist financing, in application of Article 260^{quinquies} of the CC. The investigation certainly established that the funds were from private donations and were allegedly used to finance humanitarian projects and child sponsorships, but it was not possible to gather sufficient evidence of terrorist financing from a legal standpoint. The proceedings were closed after six months.

Assessment
This analysis shows that the risk in Switzerland is focused on certain critical NPOs and non-profit areas of activity.

With regard to terrorist financing, NPOs which operate in regions where the rule of law is patchy or non-existent are particularly critical through their collaboration with partner organisations suspected of terrorist activities. As for the identification of critical organisations, this is done through regular sharing of information between the services concerned. In particular, the lack of transparency in terms of the allocation and use of donations, incomplete or contradictory information on the BOs, cash payments, big transfers to the accounts of managers of NPOs as well as frequent remittances to risk countries by money transmitters are clear indications of the NPO's possible criminal background or criminal intentions.

In relation to the risk of money laundering, NPOs operating in Switzerland have drawn attention to themselves primarily on account of their shenanigans which aimed at concealing the BOs of assets of criminal origin.

Finally, as for foundations, unlike the situation for associations, their supervision permits regular audits to ensure compliance with their purpose, which reduces the risk of money laundering. Moreover, the imminent integration of family and ecclesiastical foundations into the anti-money laundering system will reduce this risk even further. From 1 January 2016, these foundations will in effect be required to be entered in the commercial register.

7.2.3 Cross-border cash transfers

In Switzerland, control over the cross-border transportation of cash is based on the information system, which is deemed equivalent to the declaration system in the FATF international standards.

In accordance with Article 95 paragraph 1bis of the Customs Act of 18 March 2005 (CustA)[154], the FCA supports the fight against money laundering and terrorist financing as part of its tasks. However, it does not have investigative or prosecuting powers and its remit is limited to provisional sequestration. Under certain conditions, it can also enforce a right of customs lien on cash.

As part of its remit to monitor the movement of people and goods crossing the Swiss border (customs controls), the FCA carries out risk-based spot checks of cross-border cash transfers, checking in particular to see if the amount being carried reaches CHF 10,000. However, the import, export and transit of cash, whatever the amount, is not prohibited.

[154] SR 631.0

The information system makes provision for the person obliged to provide information being required to indicate the following information if expressly asked to do so during a customs control:

a. about him or herself;
b. about the import, export or transit of cash of at least CHF 10,000 or, if it is a foreign currency, the equivalent amount;
c. of the origin and the envisaged use of the cash;
d. about the BO.

In the event that it suspects money laundering or terrorist financing, the customs office can request this information even if the cash does not reach the threshold value of CHF 10,000 or, if it is a foreign currency, the equivalent amount.

The person obliged to provide information is required to provide information about him or herself and on the amount of cash. Refusal to provide information or the provision of false information is punishable for failure to comply with instructions. However, the person does not incur a penalty if he or she refuses to provide information on the origin and envisaged use of the cash or on the BO. This restriction takes account of the ban recognised by the Federal Supreme Court on compelling people to incriminate themselves[155].

Checks such as these can take place in all kinds of traffic, most notably in tourist traffic but also in commercial goods traffic. A difference must be made between the notification procedure for commercial goods traffic and those for tourist traffic. The checks are carried out by the Border Guard and Civil Customs. In practice, they occur mainly in incoming tourist traffic.

In performing their duties, Customs staff rely on the red flags/indicators in the FATF International Best Practices: Detecting and preventing the illicit cross-border transportation of cash and bearer negotiable instruments to identify suspicious cases of money laundering and terrorist financing.

In the event of suspected violations, the FCA can provisionally sequester cash which it then hands over to the police or to the OAG. However, it can happen that the sequestered cash cannot be handed over to the competent authority. Currently, if the BO cannot be found or if the cash is without doubt of criminal origin, then it is formally confiscated as a customs lien and is paid in to the Federal Treasury. This applies in particular to cash from drug trafficking. Measures were thus put in place which came into force on 1 March 2014.

The following facts may be indicators that cash stems from drug trafficking: amount made up of small notes, transport of cash carried out in a secretive way or persons linked to drug-related offences. The examination is carried out with the help of an ion trap mass spectrometer. An examination of cash as to whether it has been contaminated with drugs is not compulsory but is always possible. Cash which has obviously been contaminated by drugs must also be provisionally sequestered and handed over to the police or to the OAG. If cash which has been provisionally sequestered has not been handed over to the police or the OAG, it is formally sequestered as a customs lien and confiscated. Once the decision to sequester has entered into force, the cash must be handed over to the SNB to be destroyed because it can no longer be assimilated into the financial flow. On many occasions, the FCA has formally sequestered cash contaminated by drugs.

With the current amendment of the CustA[156], the FCA should acquire the authority to be able to definitively confiscate funds associated with criminal acts itself, without having to implement the customs lien for this.

All imports, exports and transits of cash amounts of at least CHF 10,000 as well as all cases of justified suspicions of money laundering and terrorist financing are recorded in the information system of the Border Guard (RUMACA), regardless of whether the money was left in the possession of the person obliged to provide information (no indication that an offence has been committed) or, on the contrary, provisionally sequestered for the purpose of being handed over to the police or the OAG in the event of suspicion of an offence. The RUMACA system contains information on the identity of the person whose duty it is to provide notification, the sum of cash sequestered, the origin and the envisaged use of this money and the BO.

[155] Cf. Decision of the Swiss Federal Supreme Court 131 IV 36 ff, findings 2 and 3
[156] Dispatch of 6 March 2015 on the amendment of the Customs Act, BBI 2015 2657

The 2013 and 2014 statistics on the cash amounts reported spontaneously or the transport of which was discovered following enquiries or during a customs checks and which was linked to the fight against money laundering are as follows:

Year	Incoming traffic	Outgoing traffic	Cases in Switzerland	Cases in road traffic	Cases in air traffic	Cases in rail traffic	Total	Total amount for all checks in CHF	Average amount per occurrence in CHF
2013	247	42	3	41	244	7	292	36,620,027	125,411
2014	263	23	28	70	217	27	314	30,882,373	98,351

Source: FCA

Here are some cases drawn from real-life as examples:

A. Upon arrival by plane in Switzerland, a Kuwaiti businessman declares EUR 27,000 in cash; this money is for his holiday.
B. In several cases, people arriving from Libya by plane declare the transport of cash intended for the purchase of a vehicle.
C. Upon departure from Switzerland by car, two people, who were said to be transporting money obtained by extortion, underwent a cash inspection at the request of the police. A body search was conducted on the two people and about EUR 20,000 was found on each of them. The two people and the money were handed over to the police.
D. Upon arrival in Switzerland, a vehicle from Italy was the subject of a Customs check. When questioned as to whether or not cash was being transported, the driver responded by saying that this was not the case. The ensuing verification found EUR 50,000 in a hideaway in the vehicle, which in addition had traces of cocaine in twelve different places.

Assessment
The information system can be considered to be working well because the transportation of cash with sums of at least CHF 10,000 (or foreign currency of equivalent value) is discovered and verified regularly in tourist traffic. On this point it is worth bearing in mind that the number of people that cross the Swiss border in one direction or the other amounts to more than 700,000 on a daily basis[157], including the some 270,000 to 287,000 cross-border commuters who work in Switzerland. The control ratios are between 2% and 5% for simple enquiries and between 0.5% and 1% for material checks.

In addition, it should be stressed that realistically, it is not possible to carry out systematic checks at the border because of the large number of roadside border posts which are permanently unmanned and also because of the principle of people checks based on suspicion enshrined in the Schengen Agreement. Thus, it has to be assumed that a good deal of cash transportation goes unnoticed and that it is thus not possible to quantify the amount of undeclared cash that crosses the border. Moreover, when checks of cross-border cash transportation occur, it is more difficult to determine if there is a link to money laundering or terrorist financing than for other crimes.

Often, instead of asking questions, border guards proceed directly to verifying, in line with customs law, the vehicle and luggage as well as carrying out a body search. Within the context of customs checks of this type, it is possible to corroborate relatively quickly and simply any suspicions of drug trafficking or other crimes (e.g. burglaries) thanks to the use of appliances which are able to detect drugs on people and on banknotes as well as being able to discover hideaways in vehicles.

Finally, to guarantee the execution of risk-based checks which are as effective as possible and to be able to swiftly determine if the people transporting cash have fulfilled their declaration duty under EU law, it is essential that the flow of information between the Federal Customs Administration and the customs administrations of EU member states functions smoothly. However, this flow of information still has room for improvement.

[157] We do not have precise figures.

7.2.4 Free ports[158]

A free port is a storage area, located on national territory, for goods from abroad for which the payment of customs duties and taxes is deferred for an unlimited period of time. The stored goods might be goods in transit (the lion's share) or imported goods which are destined for resale on national territory. Import duties and other taxes are levied on the latter. However, contrary to the initial vocation of free ports, i.e. to facilitate international trade by levying duties and other fees only when goods are placed on the market, free ports in Switzerland, as in a number of other countries, are being increasingly used for depositing assets over longer periods, which are often high-value goods. Indeed, free ports provide confidentiality and security for the assets in storage. High-value goods are considered to be more secure as long-term investments but frequently require adapted storage conditions[159]. Confidentiality primarily consists of the discretion offered to the owners of the assets deposited in relation to the authorities and private individuals, because the tenant of the space is not necessarily the owner of the assets deposited[160]. Confidentiality may also allow the origin or the routing of goods for example to be concealed[161].

In the face of increased use of free ports and their attractiveness in terms of confidentiality, they are at greater risk of being used to conceal and launder assets of criminal origin. However, the situation in Switzerland provides a more nuanced picture in this regard: faced with the new tools available (open customs warehouses), the importance of free ports in general has declined and the number of free ports has dropped from 18 in 2008 to 10 at present[162]. Their surface area varies greatly (from 200 to 46,000 square metres), as well as the number of tenants (from 3 to more than 500). However, the two free ports in Geneva, grouped together in the same company, are exceptions: they offer the biggest storage surface area in Switzerland and have seen their business expand by specialising primarily in the storage of high-value goods (fine wines, jewellery, art works and cultural property)[163]. With the fluctuating financial markets in recent years, these goods have become capital goods.

In Switzerland, operating a free port does not come under financial intermediation within the meaning of the AMLA. However, financial intermediaries within the meaning of the AMLA, whose clients use the services of a free port, are subject to due diligence obligations in that the financial transactions occurring in a free port must be checked the moment they go through a financial intermediary resident in Switzerland, including information relating to the origin of the assets involved and the BO. At the same time, despite the fact that customs services in the free ports do not have a mandate to verify the origin of assets, there is an extensive control system relating to the tax compliance of the goods in storage. Free ports are governed by the CustA (Art. 62 to 67) and by the Customs Ordinance of 1 November 2006 (CustO)[164] (Art. 175 to 185).

Previously, free ports were considered to be foreign territory and the law only made provision for goods inspections upon entry and exit. However, since the new law entered into force on 1 May 2007, free ports are an integral part of the Swiss customs territory and a customs office must be located in a free port. As a consequence, the customs services have the right to examine all goods in premises under customs control in free ports. Likewise, all operators of free ports in Switzerland must be in possession of an authorisation from the customs services and have a list of tenants and any sub-tenants of premises in the free port. This list must contain the name, address and lines of business as well as an address for service in Switzerland for foreign clients[165]. This information is required to the extent

---

[158] The analysis is based on non-confidential information, interviews with the Directorate General of Customs (DGC) and customs offices in free ports as well as the report of the SFAO "Free ports and open customs warehouses. An evaluation of licensing and inspection activities" from 2014.

[159] For example, a suitable temperature (e.g. for wine) and the possibility of storing bulky goods (e.g. a huge sculpture or antiques).

[160] SFAO report 2014, pp 41-42.

[161] For example, goods bought in country X are destined for sale in country Y. Between the two countries, the goods are stored in a free port in Switzerland. There they undergo changes in packaging and get new labels to be exported to country Y. The country of origin of the goods is thereby concealed because the export documents will mention export from Switzerland to country Y.

[162] SFAO report 2014, p. 34.

[163] SFAO report 2014, pp. 20-21 and 34. The report mentions a series of Swiss and international press articles about the free ports in Geneva which highlight the growth in the number of valuable items which are in storage there, the value of which allegedly exceeds CHF 100 billion.

[164] SR 631.01

[165] Art. 183 CustO.

that a tenant (storing party) can also sublet storage space[166]. The warehousekeeper must supply this list immediately at the request of the FCA[167]. Contrary to the open customs warehouses, which benefit from a high degree of flexibility in terms of access and the entry and exit of goods, the strict opening hours of the on-site customs office must be complied with in a free port. Outside the opening times, nobody has the right to access the free port[168]. During inspections, customs services will have access to all customs documents linked to the movements of goods (entry, exit and transit), irrespective of whether they belong to the owner or a company (declarant).

Free port operators are still obliged to make an inventory of goods categorised as sensitive, such as banknotes, coins, diamonds and precious stones, precious metals, jewellery, alcohol and spirits, tobacco, works of art and antiques[169]. The inventory of these goods must contain certain additional information such as the name and address of the person authorised to dispose of the goods in storage, the value of the goods in storage, proof of origin and the type of customs document preceding and following storage with the date of acceptance by the customs office[170]. However, the inventory currently does not (yet) need to contain the name of the effective owner, which is an aspect of confidentiality that could pose a risk. Furthermore, these obligations are essentially for tax purposes, as the operator is not responsible for the goods held in storage by his tenants (and possible sub-tenants). More specifically, apart from keeping an inventory, the operator is not obliged to check the contents of the storage cubicles[171].

Risk analysis is the core component of the customs strategy with regard to customs inspections. These inspections must be targeted based on information analysed and verified beforehand: the name of the person or company placing goods into storage, their area of business, the storage surface area, the movements of goods and frequency of these movements, etc. The section responsible for risk analysis at the FCA collaborates with the anti-fraud service. The analysis may also deal with the transactions conducted in one year by focusing on private tenants or large amounts, for example. In this regard, the customs services have identified the following risks: storage of unauthorised therapeutic products which are imported or stored in customs warehouses; storage and re-exportation of strategic goods (war material, dual-use goods) in or out of customs warehouses without the authorisation of SECO; evading payment of duties on works of art (VAT); not declaring or falsely declaring shipments of rough diamonds; forged certificates; unauthorised manipulation; goods which are badly inventoried or not at all; wrong number of packages when being deposited or removed from the warehouse; inventory not kept up to date or not available; changes in the markings on the certificates of origin (deception as to origin); non-compliance with provisions other than customs provisions, in particular those relating to the transfer of cultural property; sub-letting of cubicles not reported to the warehouse operator or the customs office. The risk of money laundering is not mentioned here[172].

The FCA believes that there are fewer risks (probability of a risk materialising and financial consequences) with goods in transit, which account for the majority of goods placed in storage in free ports, than there are with imports (risks to do with the collection of duties and charges) and exports (risks to do with declarations of origin). It also believes that it is more difficult to launder goods in a free port due to the inspections and the fact that it also involves yet another customs clearance[173].

Assessment

No known criminal proceedings have taken place in Switzerland for laundering money linked to assets deposited in a free port. However, criminal proceedings have taken place for offences relating to dual-use goods, counterfeits and illegal cultural property. Offences involving customs duties and fraud with regard to the origin or the entry and exit of goods are rarer[174]. Before the introduction of serious tax offences as predicate offences to money laundering, as provided for by the act of 12 December 2014, and in the absence of pertinent data, the threat of money laundering linked to aggravated tax fraud cannot be fully assessed at this stage.

---

166 Thus, in the biggest free port in Switzerland, the main storing party of the space available is a company which specialises in the conservation of works of art.
167 Art. 183 CustO.
168 SFAO report 2014, p.42.
169 Cf. Annex 2 of the CustO.
170 Art. 184 CustO.
171 SFAO report 2014, p. 61.
172 SFAO report 2014, pp 55-56.
173 The first clearance is upon entry to Switzerland and the second one is when entering the free port.
174 SFAO report 2014, p. 64.

On the recommendation of the SFAO, the Federal Council decided on the management and control of free ports and open customs warehouses on 6 March 2015 by setting out a strategy which can be summed up as follows: free ports and open customs warehouses are not legal vacuums in Switzerland. They are part of the Swiss customs territory and must comply with Swiss national law. The existence of a clearly defined legal framework contributes significantly to combating abuses. To this end, the following conditions should be met:

- Custom warehouses are under the control and supervision of the FCA. The FCA must be able to fully perform its role of supervision and control to ensure compliance with the legal system and to counter any possible abuses.
- The required transparency concerning goods in storage must be ensured in relation to Swiss and foreign authorities. For this purpose, the warehousekeeper and the storing party will be required, by law, to provide all the records and information required by the FCA so that it can carry out its tasks effectively and rationally based on a risk analysis tailored to the situation.
- In specific cases, the possibilities for national and international cooperation envisaged by the CustA must be exploited systematically. Administrative assistance and mutual assistance will be provided to foreign countries concerning foreign goods stored in customs warehouses.
- The Swiss Confederation's legislation not concerning customs matters (Art. 95 of the CustA) specifies the foreign goods for which storage in customs warehouses is subject to restrictions or even a ban (see the legislation on goods control, species conservation, war material, therapeutic products, narcotics and intangible assets).
- Goods placed under the export procedure must be exported by the deadline set.
- From now on, the inventory must contain the name of the owner of the goods in storage.

To put this strategy and the SFAO recommendations into practice, the FCA was given the mandate to present a report on the measures to be taken as well as a proposal for necessary legislative amendments.

7.2.5 Trade in works of art

The vast sums of money involved in art market transactions for many years now arouse suspicions not just as to the origin of the funds used for the purchases of the works of art, but also as to the mechanisms governing the exchanges and changes in ownership within this market. The question was raised several times recently, particularly in the European and US press.

This worrying situation is explained, on the one hand, by the particular features of the art market and, on the other, by the recent development of links between this market and the international financial sector.

Characteristics of the art market which favour money laundering
While the major areas of economic and financial activities have been the subject of tough regulations and restrictions with the aim of avoiding the laundering of dirty money, the art market sector has been oddly ignored by legislators, including in Switzerland. The dramatic rise in the prices of works of art has, however, drawn the attention of market observers, who see here the influence of dubious investments and concerted manipulation. The characteristics of the market which are favourable to fraudulent investments are as follows:

- trade in works of art is difficult to control, with its culture of discretion and lack of transparency
- the identification of the works of art is complicated
- subjectively, the value of the works of art is difficult to determine
- considerable sums of money are involved
- money laundering operations have an influence on the value of works of art, thus leading to market manipulation
- tax fraud is common in this area
- transactions can be done in secret
- transaction partners can be anonymous or virtual
- auctions can easily be manipulated

Money laundering techniques
The techniques are numerous and varied. Here are the most likely ones:

- false invoice issued for a fictitious purchase of a work of art
- a mock auction, the work of art is purchased by an accomplice of the owner with money provided by the owner
- bidding by telephone or by order, with the use of a cheque to cover the security deposit which will not be used and will be returned by and in the name of a recognised banking institution if the purchase of the work of art does not go ahead
- speculation allows considerable amounts of money to be achieved

Situation in Switzerland
International and national statistics on the art market are not accurate. The last assessment was that of the TEFAF 2014 report carried out at the request of The European Fine Art Foundation. The turnover of the global art and antiques markets is EUR 47.4 billion (USD 55 billion). The turnover in Switzerland in 2013 amounted to a sum of between CHF 1 to 1.5 billion.

Main markets by order of importance:
1) USA (38%)
2) China (24%)
3) UK (20%)
4) France (6%)
5) **Switzerland (2%)**
6) Other (9%)

As Switzerland is amongst the four or five top art markets in the world, it can be assumed that it is also affected by the phenomenon of money laundering through this market.

Switzerland has approximately 500 antique dealers, 1,200 art galleries, 15 auction houses, 1,073 museums and between 1,500 and 3,000 flea markets/second-hand shops. The auction houses are the institutions in the art market which are most exposed, and the two multinationals operating in Switzerland target wealthy customers. A branch of one of these two multinationals based in Zurich specialises in high-end Swiss art, the value of which has risen significantly in recent years (Amiet, Anker, Hodler, etc). Furthermore, this multinational is also very active in jewellery auctions in Geneva. Jewellery sales generate considerable sums of money, which will no doubt appeal to money launderers. The sale of watches, another specialty of Geneva, has undoubtedly the same effect. The other multinational, which also operates in Zurich and Geneva as well as in St. Moritz, has the same risk profile (jewellery, extremely valuable small works of art, Swiss art traded internationally).

Of the Swiss auction houses, only one competes with the leading international auctioneers, and operates in all market sectors (jewellery, paintings, drawings, graphic arts, furniture and sculptures, carpets and rugs, books and autographs, photographs, Asian arts, fashion, luxury and vintage, silverware, porcelain, wines, African art, watches, high-end Swiss art and international art). The auctions take place in Zurich and twice a year in Geneva. The risk profile is the same as for the big multinationals. The same is true for another auction house found in Bern that specialises in high-end graphic arts and visual arts.

In the mid-range segment, four auction houses dominate the market, two of which are found in Bern, one in Lucerne and the other in Geneva. The risk profile of these four auction houses is lower to the extent that the art works on sale do not reach the same high amounts as those of the auction houses mentioned above. However, niche markets attract individual investors and generate high prices: for example, Russian historical items sold at the Hôtel des Ventes in Geneva beat all records, and significant sums of money were paid for a number of antique weapons sold by another auction house.

The situation of the conventional art galleries and antique dealers presents the same risks insofar as the works of art can change hands relatively easily and in complete discretion (in the free ports, for example). One additional factor should be taken into consideration: on-line purchases. Each market player has set up an online sales operation. The amounts involved can also be significant.

Typologies
A. A bank informed MROS of a business relationship, which has since been terminated, with a Swiss salesman of valuable, classical string instruments. During an internal audit, it was found that the client had been accused of fraud and criminal mismanagement in a neighbouring country relating to international trade in string instruments. In Switzerland, an investigation had also been opened against the salesmen in the past relating to similar offences. Subsequent analysis of the transactions carried out revealed several suspicious deposits and withdrawals directly related to trade in violins and implicating

other suspicious people who had been mentioned several times in the media. Various pieces of information in databases as well as other research relating to the persons identified confirmed that investigations were in progress abroad. MROS thus forwarded the suspicious activity report to the competent cantonal prosecutor. An investigation has been opened.
B. A bank reported its business relationship with client X to MROS. Transactions linked to the purchase of contemporary works of art passed through X's account, before being credited to a third person, Y. In addition to some very unconvincing explanations, X supplied a certificate of authenticity to the bank relating to some of the works of art and also indicated that he owned them. MROS's analysis cast doubt on the authenticity of the signature on the certificate. Further investigations by MROS led to an estimate of the real value of the works of art in question, which was much less than the exorbitant value provided by X. In light of this information, the roles played by X and Y appeared to be sufficiently suspicious for MROS to justify forwarding the report to the competent criminal prosecution authorities. However, the latter have not instigated criminal proceedings.
C. As a result of newspaper articles naming X as a former leader of a Eurasian criminal organisation actively engaged in money laundering, a financial intermediary analysed his business relations with X. This analysis highlighted suspicious transfers of funds, amongst which were several deposits of large cash amounts. These factors led the bank to report the business relationship maintained with X over a number of years. The investigations undertaken by MROS revealed that X had been wanted for two years in a foreign country for illegal trade in cultural property, primarily in ancient coins. Other countries had shown interest in X, also for the smuggling of ancient coins. MROS forwarded the report to the competent criminal prosecution authorities.

Assessment
The art market in Switzerland is governed by the Federal Act of 20 June 2003 on the International Transfer of Cultural Property (CPTA)[175], which came into effect on 1 June 2005. This Act concerns the following areas in particular:

- protection of Swiss cultural heritage (exportation of cultural property out of Switzerland)
- Contribution to protecting the cultural heritage of other countries (importation of cultural property into Switzerland)
- Encouraging international exchanges between museums (return guarantees for museums)
- due diligence obligations for trade in works of art and auctions

The concept of "cultural property" is defined in Article 2 paragraph 1 of the CPTA as follows: "Cultural property is considered to be objects which are meaningful, from a religious or secular point of view, for archaeology, prehistory, literature, art or science and which belong to one of the categories provided for under Article 1 of the 1970 UNESCO Convention." Since the CPTA entered into force, the art market is subject to due diligence obligations (Art. 16). The provisions of the Act strive to uphold the compliance of cultural property transfers, i.e. that "they were not stolen or removed against the will of the owner, illegally excavated or illicitly imported". To ensure this, art dealers and persons active in the auctioning business are obligated:

a) to establish the identity of suppliers and sellers and require a written declaration from them of their right to dispose of cultural property;
b) to inform their customers about existing import and export regulations of the countries of the contracting parties;
c) to maintain written records on the acquisition of cultural property by specifically recording the origin of the cultural property, to the extent known, the name and address of the supplier or seller, and a description as well as the purchase price of the cultural property;
d) to provide the specialised body with all the necessary information on fulfilling this due diligence obligation.

The records and supporting documents must be stored for 30 years. Article 962 paragraph 2 of the CO applies by analogy.

Verification of fulfilment of the due diligence obligation is assigned to the specialised body of the Federal Office of Culture (FOC; Art. 17), according to the following legal terms:

a) The specialised body has access to the business premises and warehouses of art dealers and persons active in the auctioning business;
b) If the body has reasonable suspicion that criminal activity under the CPTA is present, the specialised body will file a complaint with the competent criminal prosecution authorities.

[175] SR 444.1

It should be noted that according to Article 20 of the Ordinance of 13 April 2005 on the International Transfer of Cultural Property (CPTO; ordinance implementing the CPTA)[176], the specialised body must give advance notice of the inspections to be carried out on site, except if the cultural property or related documentation risk being removed before the inspection.

If the principle of checking the origin of cultural property is enshrined in the CPTA, the Act does not make provision for the verification of the origin of the assets used to acquire the cultural property itself. However, origin checks will be supplemented by the new provisions introduced in the AMLA which, from 1 January 2016, provide for due diligence obligations for commercial cash transactions exceeding CHF 100,000 (verification of the identity of the contracting party and identification of the BO and, if the transaction appears unusual, clarification of the origin of the assets), or require that the transaction be carried out through a financial intermediary subject to the AMLA. In this regard, some auction houses in the mid-range sector already impose an upper limit of CHF 10,000 on cash transactions. This reduces the risk of trade in works of art in Switzerland being used for money laundering purposes.

7.2.6 Commodities trading

In Switzerland, commodities trading is subject to the provisions of the AMLA, where trading is done for the account of a third party (cf. Art. 2 para. 3 let. c of the AMLA in conj. with Art. 5 para. 2 let. b of the PFIO). Proprietary commodities trading is not, as such, subject to the AMLA. This is explained by the fact that such a scenario does not involve assets belonging to third parties being accepted or kept on deposit within the scope of trading activity. Indeed, those who engage in proprietary trading have no client relationships and do not deal with assets belonging to others. Subjecting proprietary trading activities to the AMLA would not make any sense because it would be the responsibility of the traders, as the counterparties and BOs of the goods, to impose the due diligence obligations established by the AMLA on themselves and to examine the background of their own transactions. The adoption of a rule like this is not very convincing at the conceptual level, particularly because the application of such a rule would risk causing too many conflicts of interest. Where an investor invests in commodities through his bank, on the other hand, that constitutes a financial transaction that is covered by the AMLA.

Even if proprietary commodities trading is not subject to the AMLA, the fact remains that the fundamental provision of the SCC, i.e. Article 305bis, prohibits money laundering regardless of whether the trading was done for the account of a third party or for one's own account[177].

At the global level, Switzerland is home to some of the world's largest commodities trading companies, as well as numerous medium-sized companies. Business in this sector is concentrated in the Lake Geneva region and in the cantons of Zug and Ticino.

In the crude oil and ore trading sectors, Switzerland is currently the largest global commodities trading centre, with a roughly 20% market share (figures 74 and 75). Furthermore, about one third of world trade in crude oil occurs in Switzerland. Some 75% of Russian crude oil is traded in Geneva[178]. Switzerland is also an important trading platform for sugar, cotton and coal. In 2013, the turnover of the commodities sector was estimated at more than CHF 800 billion, achieving an annual increase since 2011 of between 5 and 7%, stabilising at a high level by international standards[179].

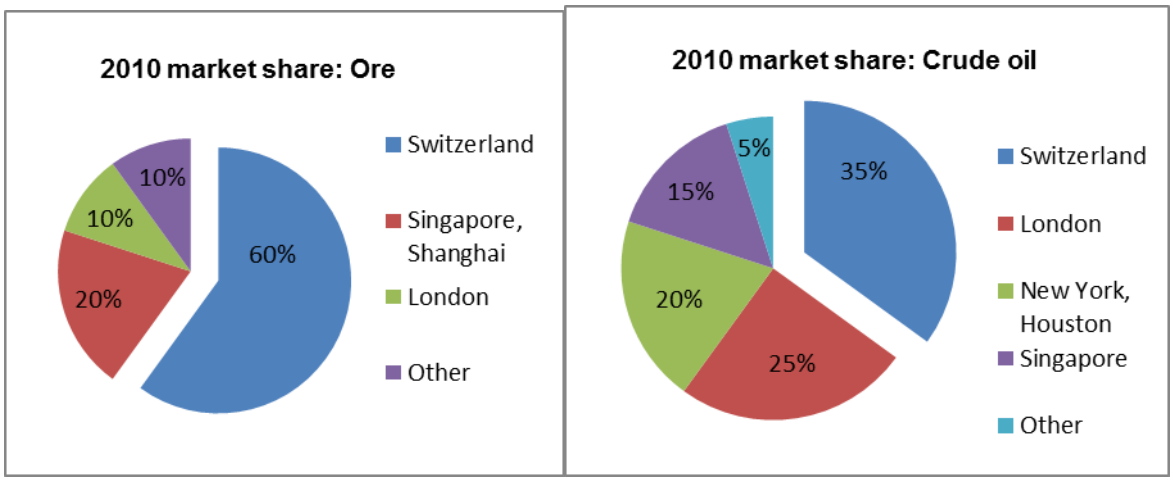
Figures 74 and 75: Market share at the international level of trading in main commodities, 2010

[176] SR 444.11

[177] Cf. the Federal Council's response to the Wyss motion (11.4161) "No money laundering in the proprietary trading of commodities"

[178] Background report: commodities, FDFA, FDF, EAER, 2013:
http://www.news.admin.ch/NSBSubscriber/message/attachments/30134.pdf

[179] SNB, Swiss Balance of Payments 2011, 2012



Source: "Background report: commodities", FDFA, FDF, EAER, 2013.

While most of the companies operating in the sector in Switzerland are active in both commodities trading and the extraction of resources, a smaller number of medium-sized companies operate only in commodities trading. Furthermore, the sector consists of a whole range of service suppliers. Thus, in Switzerland, "it is estimated that around 500 companies and some 10,000 employees are active in the commodities industry, shipping, transaction financing, inspections services and product testing"[180]. In Geneva alone, some 400 companies operate in this sector. Switzerland's sharp growth as a commodities trading centre, coinciding with a concentration in overall ancillary activities connected with commodities trading, goes hand-in-hand with the increased potential threat in this sector. Some 22% of the shipping of commodities worldwide is organised from Geneva[181].

One of the characteristics of commodities trading is the need for major financing which is readily available (commodity trade finance). This is why banks are the main financial intermediaries which this sector uses. Approximately 75% of Swiss commodities trading is financed by about fifteen banks which specialise in this field. These banks include in particular the big banks, some cantonal banks as well as branches of foreign banks domiciled in Switzerland. The latter may also provide financing from abroad. Some commodities traders finance or secure part of their business through publicly traded financial transactions in commodities derivatives. The financial instruments concerned are for the most part negotiated with foreign counterparties outside the Swiss Stock Exchange[182]. This mode of financing used by the commodities trading companies has a weakness, which is due to the lack of transparency relating to the identification of the BO of the counterparty and to the possible implication of politically exposed persons.

In this sector, the threat is linked to acts of bribery involving foreign officials and commodities trading companies. It is well known that the extraction industries figure prominently amongst the activities exposed to foreign bribery[183]. From the point of view of money laundering, this threat materialises when a corrupt individual seeks to place or invest funds obtained directly through bribery. The Swiss anti-money laundering system addresses this threat in that the investment of assets generally has to be carried out through a financial intermediary subject to the AMLA. From this point on, the legal mechanisms for detecting the suspicious origin and for communicating with the FIU are triggered.

From the point of view of criminal prosecution, it is difficult to establish a causal link between the act of bribery (for example, to obtain an operating contract) and all the proceeds and commodities trading resulting from this. To be considered as proceeds of the predicate offence, the Federal Supreme Court specifies that the assets obtained as a result of the awarding of a contract through act of bribery (the briber's income) must have a natural and adequate causal link to the predicate offence in question, without them necessarily being the direct result[184]. However, this causal link is difficult to establish for commodities, which are fungibles, generally traded in significant amounts, often mixed with commodi-

[180] Background report: commodities, FDFA, FDF, EAER, 2013:
[181] Geneva Trading and Shipping Organisation (GTSA), 2012.
[182] Background report: commodities, FDFA, FDF, EAER, 2013, pp. 14-15
[183] OECD Foreign Bribery Report, OECD, 2014
[184] In this regard, please see Decision of the Federal Supreme Court 137 IV 79

ties obtained legally and are rapidly consumed. Criminal justice in Switzerland, as well as abroad, encounters systemic limits here in the performance of its tasks.

Another difficulty is the qualification of the predicate offence to money laundering activity. In the commodities trading sector, this is not necessarily an act of bribery committed by a third party, but is perhaps the result of criminal mismanagement of public or private interests by natural persons, often PEPs effectively controlling the supply of commodities in the resource-producing country. Under this arrangement, the purchasing terms of commodities on the international market are truncated, for example by granting concessionary terms to trading companies that serve as a front, operating in Switzerland and abroad but in reality controlled by PEPs. Benefiting from more favourable conditions, the PEPs can, for example, purchase commodities without carrying out a proper tender procedure in the resource-producing country or have access to easy financing. In such circumstances, it is difficult to fully identify assets of criminal origin which are likely to constitute direct kickbacks to other entities, because the profits from the purchases and sales of these trading companies are already part of the assets under the control of the PEPs. Moreover this method can dispense with a financial intermediary in Switzerland, in particular for financing, which means the trading occurs outside the AMLA mechanism.

However, MROS does have suspicious activity reports from banks which directly concern commodities traders. The analysis of these reports enables a number of indicators of the real threat to be outlined. It should be mentioned that two thirds of the information analysed by MROS in the reports linked to this sector come from foreign counterparts. This international element underlines the significance of the transnational dimension of the threat in this sector, which renders money laundering activities especially hard to detect. Furthermore, the pattern which emerges from the analysis of the real threat shows a particularly high level of complexity, involving for the most part a combination of actors (consultants acting as intermediaries/business introducers, commercial enterprises or domiciliary companies). On the trading company side, the different entities are for the most part contained in a holding structure, which facilitates the fragmentation and multiplication of the points of contact with the different entities put forward by the intermediaries/business introducers. Very often, several financial intermediaries, banks, lawyers or fiduciaries active in Switzerland or abroad are involved at different levels of the suspicious relationships reported, thereby increasing the complexity of the arrangement. The payments are carried out using a cascading system through various channels and often with a time delay. The complexity that is characteristic of this sector is due to its quintessentially international nature. These legal and/or commercial structures do not necessarily aim to prevent confiscation of the proceeds from crime. However, they do make it more difficult for the prosecution authorities to establish a causal link.

The basis of trading is provided by confidential service agreements which link the party in a position to secure an advantage for the trader from the purchase of commodities. In a number of cases reported, this party is close to a PEP. In this arrangement, the corrupt foreign public officials sometimes request the intermediaries/business introducers in the trading company to make payments to third parties for services rendered or to finance the purchase of goods and services, for example real estate.

Assessment

The commodities trading sector poses the risk of Switzerland being used as a platform to launder assets derived from bribery committed abroad in resource-producing countries for the purpose of obtaining contracts. A significant part of commodities trading and its financing at the global level occurs in Switzerland. For the last decade, the trend has been an upward one. The trading carried out in Switzerland mainly concerns commodities which do not enter or leave Switzerland physically, such as trade in bauxite between Guinea and the USA. The physical trade flow therefore does not occur in Switzerland. Switzerland is the location for a trading centre. Trading data is gathered and presented in accordance with the new international standard of the International Monetary Fund, the Balance of Payments and International Investment Position Manual (BPM6). In Switzerland, the SNB gathers the trading data. This data has a certain degree of granularity for each country and also for the trading category. It provides a picture of the flows linked to trading, their origin and their destination. However, the degree of granularity does not cover each country individually[185]. As for the trading categories, they comprise agricultural products, stones and metals, energy commodities and other marginal categories. Greater detail in these categories is not available. In addition, there is no individual breakdown of the trading categories for each country. These statistics thus do not permit specific risk analysis.

However, analysis of the real threat clearly shows very complex crime patterns in this sector very often involving several intermediaries scattered over a large number of jurisdictions. The systematic use of

[185] Sub-Saharan Africa is thus made up of three groups: South Africa, Nigeria and other countries.

cascading legal structures, such as domiciliary companies and service agreements, facilitates the concealment of the BOs, the assets of criminal origin as well as of the various payments made during the act of bribery, thus rendering detection unlikely. As the reports processed by MROS indicate, the amounts involved in the money laundering activities linked to this sector are significant, and PEPs are often involved. Criminal prosecution is thus difficult in this sector due to the complexity of the cases and the requests for international mutual assistance, which turn out more often than not to be inconclusive or remain unfulfilled.

In general, in terms of potential risk mitigation, a distinction should be made between the due diligence requirements in accordance with the AMLA applicable to financial intermediation activities and the other measures, outside the AMLA, applicable directly to trading companies themselves. Within the framework of commodities trading for the account of third parties, the due diligence obligations provided for in the AMLA are sufficient as they are. The problems stem above all from detection due to the complexity of the cases and the difficulties regarding criminal prosecution. These problems cannot be resolved by strengthening the due diligence obligations applicable to financial intermediaries. As for proprietary commodities trading, subjection to the AMLA is not the answer either. It would scarcely make any sense because as mentioned earlier, it would amount to obliging the trading company to apply the due diligence obligations to itself, such as clarifying its own transactions or the origin of its own funds. On the contrary, risk mitigation linked to commodities trading must involve measures other than the rules on combating money laundering which would apply directly to trading companies. This relates in particular to ethical rules, codes of conduct or increasing transparency on the origin of commodities themselves or on the transactions connected to them. In this context, the following two projects should be mentioned which, if they are concluded, will by their nature ensure greater transparency in the future:

- The planned bill on the Financial Market Infrastructure Act (FMIA) makes provisions for commodities traders to be subject to the obligation to declare the purchase and sale of all derivative financial instruments in Switzerland, including those based on commodities, on the same basis as other financial market participants. By increasing the transparency of these products in Switzerland, this obligation will contribute to reducing the vulnerability of the sector.
- Likewise, the revision of the law on companies limited by shares aims to make the Swiss commodities sector more transparent and will thus help to reduce the risk in the sector. The proposed provisions in the preliminary draft will oblige raw materials extraction companies to disclose payments made in favour of governments. The rules concern big companies which produce ore, oil, natural gas and wood. These companies must mention in a report the payments made as soon as these reach CHF 120,000 per financial year. The aim is also to authorise the Federal Council to extend these obligations to companies operating in commodities trading within the scope of an internationally harmonised procedure.

8 Conclusions and recommendations

Switzerland has been actively involved in the fight against money laundering and terrorist financing for many years. Although the competent authorities have been regularly performing risk analyses in their respective areas of responsibility, this report collects and presents the threat and vulnerability analyses in Switzerland in a single document for the first time, thus providing an overall but also differentiated assessment of the current risk of money laundering and terrorist financing in our country. The CGMF's analytical work, which also benefited from contributions from a certain number of private-sector specialists, has enabled those involved in the process to develop a shared understanding of the main threats and, at the same time, to better understand the risks associated with their respective fields of activity.

The analyses in this report focus essentially on the risks in the financial sector and, consequently, on the activities covered by the AMLA's scope of application. They were also extended to certain other areas of the economy that have received particular attention from the authorities and the public sector. It must be noted, however, that unlike the financial sector, for which there is a substantial database of quantitative data, the analyses on the other areas are based to a large extent on qualitative elements. Moreover, despite the fact that the financial intermediation activities in these areas are already subject to the due diligence obligations established by the AMLA, it is not possible to reduce the risks of criminal activities in these commercial transactions by way of conventional instruments applicable to the financial sector. Therefore, the conclusions to be drawn from this report need to be modified slightly depending on whether they relate to either financial intermediaries or other economic activities. Never-

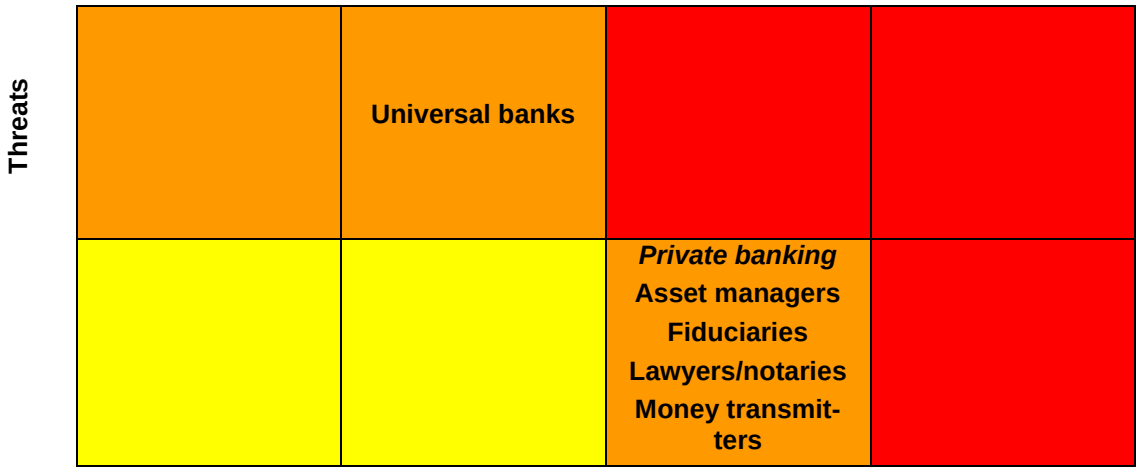
theless, to the extent that the financial flows associated with the commercial transactions in these areas involve financial intermediaries subject to the AMLA, the due diligence obligations can be viewed as having an indirect risk-reducing effect in the areas not subject to the AMLA.

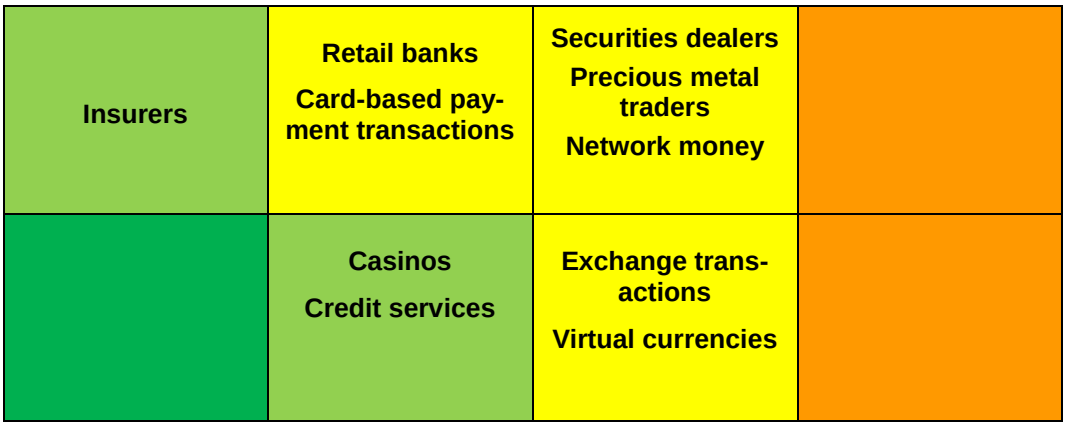
It is clear from the report that Switzerland is not immune to financial crime. This report highlights the very fact that Switzerland is still an appealing location for the laundering of assets derived from offences that are mostly committed abroad. In terms of predicate offences, the main threats for the Swiss financial sector are fraud and misappropriation, bribery and participation in a criminal organisation. An analysis of predicate offences also suggests that some money laundering activity at the international level is performed by specialists. The threats associated with bribery performed abroad and participation in a criminal organisation show increased vulnerability because they are more complex, which makes them more difficult to detect and suppress. As a result, there is a growing need for international cooperation to effectively combat the laundering of money linked to predicate offences. For instance, the number of requests for mutual assistance both sent and received from abroad has increased in the past decade, which indicates that the competent authorities are making extensive use of this means. Criminal prosecution authorities are also spontaneously sending information abroad to support criminal proceedings in the countries concerned or to initiate such proceedings. By contrast, information from abroad is rarely forwarded spontaneously to Switzerland.

Financial intermediaries

In general, the increase in suspicious activity reports in recent years and the high proportion of these forwarded to the criminal prosecution authorities as well as the growing number of convictions show that financial intermediaries are becoming more aware, vigilant and committed with regard to the fight against money laundering and terrorist financing. This is also due to a particular feature of Switzerland's system, i.e. financial intermediaries are fully included in its anti-money laundering and terrorist financing mechanism. In addition to their duty to report suspicious activity to MROS, financial intermediaries have a legal responsibility to detect cases of suspected money laundering and terrorist financing and thus play a vital role in the Swiss anti-money laundering mechanism.

The overall evaluation of the risks of money laundering showed a medium risk for all of the areas covered by the AMLA. Nevertheless, the level of risk differs for each of the areas analysed. So even if the biggest threat has been identified in the area of universal banks, the vulnerabilities in this area are significantly reduced by the existing anti-money laundering measures in such a way that appropriate risk management can be expected despite the higher risk. The same is true for the areas of private banking, asset managers, lawyers and notaries, fiduciaries and money transmitters. The analyses showed that the areas of insurers, casinos and credit services are exposed to a low risk in Switzerland. The other areas analysed (retail banking, securities trading, trade in precious metals, foreign exchange transactions and payment services [including virtual currencies and online payment systems]) are exposed to a medium-to-high risk. However, the existing measures to prevent and reduce the risk of money laundering and terrorist financing are commensurate with the risks identified. As a result, these areas are exposed to limited risk.





The analysis also revealed a limited risk for terrorist financing, which could have a significant impact, however, if it occurred. Furthermore, the risk could increase if terrorist financing networks were to exploit alternative money remittance systems in Switzerland more systematically. This would increase both the threat to Switzerland and its vulnerability. At present, the financial intermediaries most exposed to the threat of terrorist financing are banks, money transmitters and credit services. The sums of money in question are generally low. The authorities are working together closely in this area at both the national and international levels. The continuation and strengthening of this cooperation, particularly between intelligence services, and awareness-raising among social partners potentially affected by the issue of terrorist financing as well as the application of other available legal remedies to combat terrorist financing are essential for controlling the risk. Furthermore, in the context of current terrorist threats, the management of fedpol, FIS and of the FDFA State Secretariat have set up a task force (TETRA – Terrorist TRAvellers) with the aim of exchanging information effectively and coordinating all national efforts to combat the terrorist threat from Jihadist travellers.

The CGMF is of the opinion that the existing legislation, which was supplemented with the Federal Act of 12 December 2014 for Implementing the Revised Financial Action Task Force (FATF) Recommendations of 2012, and the other risk-reducing measures outlined in the report adequately respond to the current risks of money laundering and terrorist financing. Nevertheless, it believes that the application of the instruments established by the legislation should be improved further at the operational level. For this reason, the CGMF recommends the following measures:

1. Dialogue with the private sector about risks will be intensified. This means that MROS and FINMA are to further increase awareness among financial intermediaries subject to risks as part of their respective tasks. Furthermore, as part of the CGMF's work and in coordination with the authorities concerned, regular dialogue will be established with the financial sector and, as needed, with other sectors regarding the outcome and forthcoming risk evaluation work and the ways in which to deal with the situation. This dialogue will also look at emerging risks from the perspective of a mutual early warning system between the public and private sectors.
2. The Office of the Attorney General of Switzerland is to continue gathering and analysing information from the cantonal and federal criminal prosecution authorities in the field of money laundering and terrorist financing, particularly for establishing consolidated statistics on the processing of cases in these areas.
3. The public and private players involved in combating money laundering and terrorist financing are to develop and systematise statistics taking the quantitative measurements used in this report into consideration, particularly when entering information on suspected predicate offences and the place they were committed. This information will be made available to MROS once a year so it can be included in its annual report, where relevant.
4. The CGMF will continue to perform risk analyses. It will update existing analyses based on the development of money laundering and terrorist financing threats and extend its analyses to include new predicate offences for which there are currently no risk analyses, particularly tax-related predicate offences.

<u>Other issues and areas</u>

The CGMF also included analyses of six areas not subject to the AMLA in the report, which were selected as a result of their economic significance and the interest triggered in Switzerland by certain activities in these areas in recent years. The areas are the real estate sector, non-profit organisations, cross-border money remittance, free ports, trade in works of art and commodities trading. In response to a parliamentary initiative[186], a separate analysis will be conducted on safe-deposit boxes provided by companies not subject to the AMLA.

What is common to all of these areas is that they are for the most part outside of financial intermediation, which is the criterion for subjection to the AMLA. The risk of these areas being used by criminals is therefore countered firstly by the fundamental provisions of the Swiss Criminal Code that target all acts of money laundering (Art. 305bis of the SCC). Secondly, to the extent that the financial flows from these activities involve financial intermediaries subject to the AMLA, the strengthening of the due diligence obligations introduced by the AMLA on 12 December 2014 indirectly helps to reduce risks in these areas. Finally, as noted in the report, other measures to this effect are now in place in the aforementioned areas, which include in particular provisions on cross-border cash transfers, anti-bribery legislation and legislation on the sale of cultural property. In addition to these measures, new provisions have been introduced in the AMLA which establish the obligation of either involving a financial intermediary or performing due diligence regarding commercial cash transactions exceeding CHF 100,000 (verification of the contracting party's identity and identification of the BO and, if the transaction seems unusual, clarification of the origin of the assets), which will be applied from 1 January 2016. This measure aims to reduce the risk of money laundering and terrorist financing for all commercial transactions, particularly in sectors such as real estate, trade in works of art and commodities trading.
The CGMF has nevertheless drawn up additional measures to respond to the shortcomings identified in this report:

5. In order to reduce the vulnerabilities identified in the real estate sector, the national real estate register envisaged in the Federal Council dispatch of 16 April 2014[187], and which is accessible to the federal authorities, must be implemented swiftly. However, the national register will be limited to registering only the AHV numbers of building owners. In order to enable the federal authorities to carry out effective searches on foreign owners of property in Switzerland too, it should be possible to perform searches based on full names, or on company names for legal entities that own property.
6. To enhance supervision and thus reduce the risks of foundations being used for money laundering and terrorist financing purposes, the Federal Supervisory Board for Foundations should be strengthened and allocated additional resources. The CGMF will also work with the authorities responsible for supervising foundations and with the authorities involved in the area of non-profit organisations to draw up proposals for specific measures where necessary.
7. The Federal Council's strategy on customs warehouses[188] must be put into practice primarily by implementing the recommendations of the Swiss Federal Audit Office and by establishing a legal framework through an implementing ordinance. In particular, the warehousing of goods for export should only be permitted for a defined period of time, and inventory contents should be expanded together with the disclosure obligation of the warehousekeeper and storing party. When implementing the recommendations of the Swiss Federal Audit Office, it is essential that the inspections conducted in free ports are made more consistent.
8. The proposals contained in the preliminary draft of the amendment to the Swiss Code of Obligations (law on companies limited by shares)[189] concerning accounting rules for raw materials extraction companies in order to ensure greater transparency in this area, and the extension of these rules to the commodities trading sector as part of an internationally coordinated approach, should be included in the future bill and the corresponding dispatch which will be submitted to Parliament.

Due to the fact that criminals are constantly adapting their methods, the national risk assessment is an ongoing process. The report will therefore be updated and supplemented with other reports and anal-

[186] Postulate 14.4049 Fabio Abate: "Safe-deposit boxes outside of banks"
[187] Dispatch of 16 April 2014 concerning the amendment of the Swiss Civil Code (Recording of marital status and real estate register), BBI 2014 3395, 3420
[188] Cf. Dispatch of 6 March 2015 on the amendment to the Customs Act, BBI 2015 2657, p. 2665
[189] Preliminary draft of the amendment to the Swiss Code of Obligations (law on companies limited by shares), in consultation from 28 November 2014 to 15 March 2015

yses to ensure that the effectiveness of the Swiss system is evaluated and new threats are addressed. The Federal Council established the CGMF as a permanent coordinating body that brings together the federal authorities concerned precisely to meet the need for an ongoing risk analysis and, where necessary, adapting the Swiss system to new threats.

9 Appendices

9.1 Risk calculation

1. Procedure for calculating risks using a quantitative matrix

Initially, the 10,491 suspicious activity reports received by MROS between 2004 and 2013 (N^{tot}) were evaluated according to the five risk criteria selected on the basis of the AMLO-FINMA, i.e. the risks associated with the countries involved (A), the amount of assets involved (B), the number of players involved (complexity factor I, C), the involvement of domiciliary companies (complexity factor II, D) and the presence of PEPs (heightened risk, E). The result of each evaluation was expressed as a number. In a second step, the results obtained for each risk factor were weighted using a coefficient considered appropriate:

Factor A: Country risk (**coeff. 3**)=A*3=a^r

Factor B: Financial risk (**coeff. 1**)=B=b^r

Factor C: Complexity risk I: number of players involved (**coeff. 2**)=C*2=c^r

Factor D: Complexity risk II: involvement of domiciliary companies (**coeff. 4**)=D*4=d^r

Factor E: Political risk associated with PEPs (**coeff. 4**)=E*4=e^r

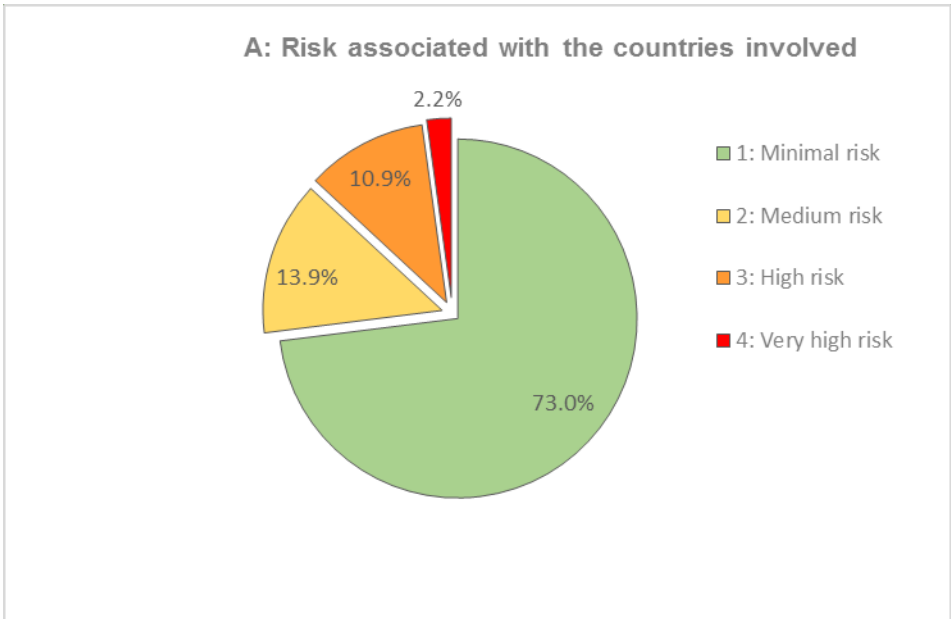
Finally, in a third step, the reports from each sector were selected (N^{sec}) and compared to the maximum risk that all of the reports could have obtained for the sector, expressing this difference on a scale of 0 to 5.

$$\Delta \frac{\sum_{N^{sec}} (a^r \times b^r \times c^r \times d^r \times e^r)}{\sum_{N^{sec}} (a^{max} \times b^{max} \times c^{max} \times d^{max} \times e^{max})} \times 0.05 =$$

A. Risk associated with the countries involved

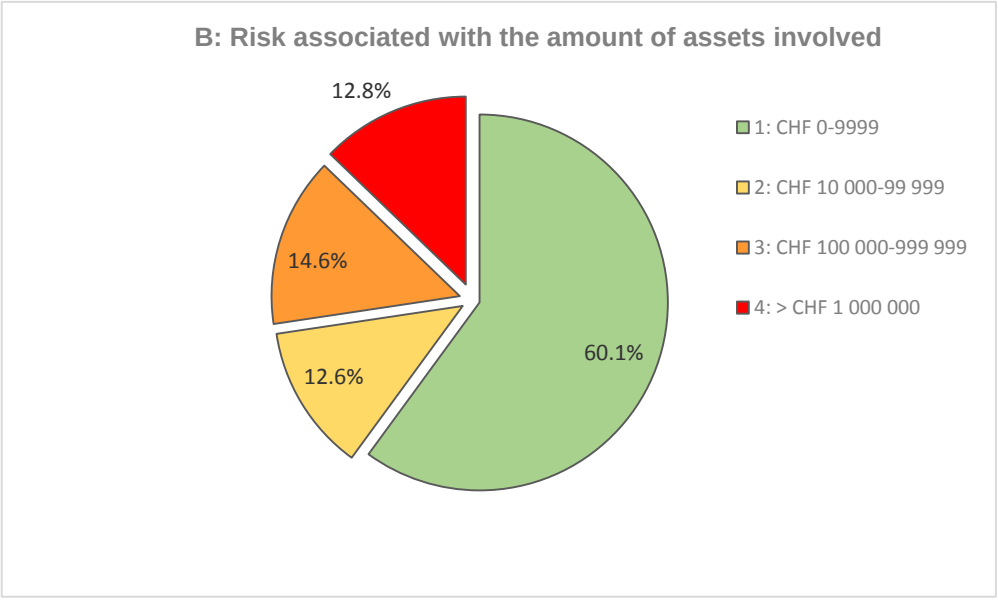
In order to evaluate the risk of the country involved, four levels of risk were defined taking into account a whole series of indicators such as the crime rate, compliance with FATF regulations, the level of corruption and compliance with the principle of the rule of law.

	N	Percentage applicable	Cumulative percentage
1: Minimal risk	7645	73.0%	73.0%
2: Medium risk	1458	13.9%	86.9%
3: High risk	1143	10.9%	97.8%
4: Very high risk	231	2.2%	100.0%
N applicable	10477	100.0%	
Total (∑)	10491		



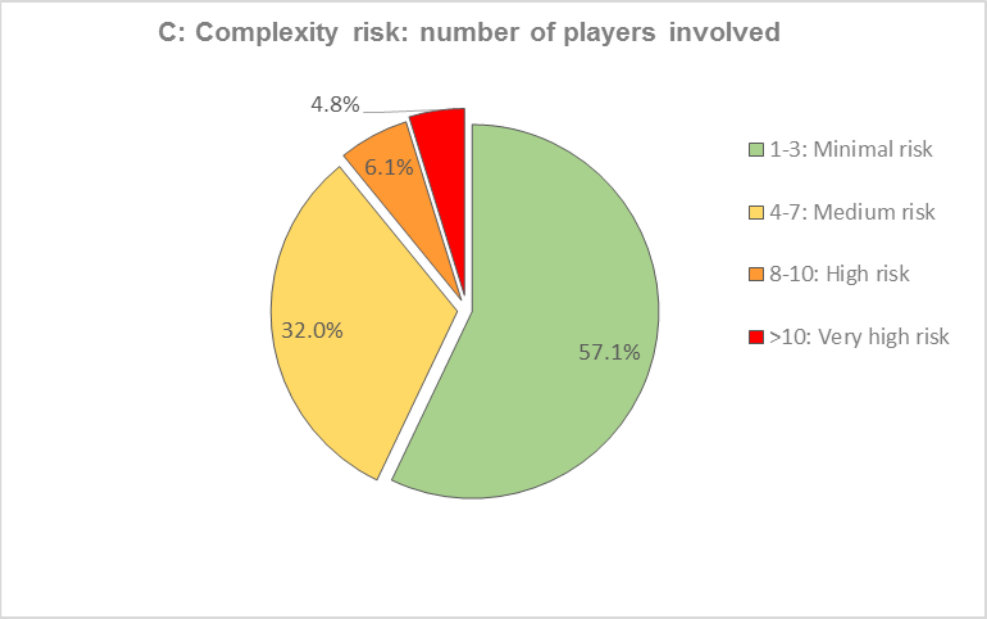
B. Risk associated with the amount of assets involved

in CHF	N	Percentage applicable	Cumulative percentage
1: CHF 0-9999	6300	60.1%	60.1%
2: CHF 10 000-99 999	1319	12.6%	72.6%
3: CHF 100 000-999 999	1532	14.6%	87.2%
5: > CHF 1 000 000	1340	12.8%	100.0%
N applicable	10491	100.0%	



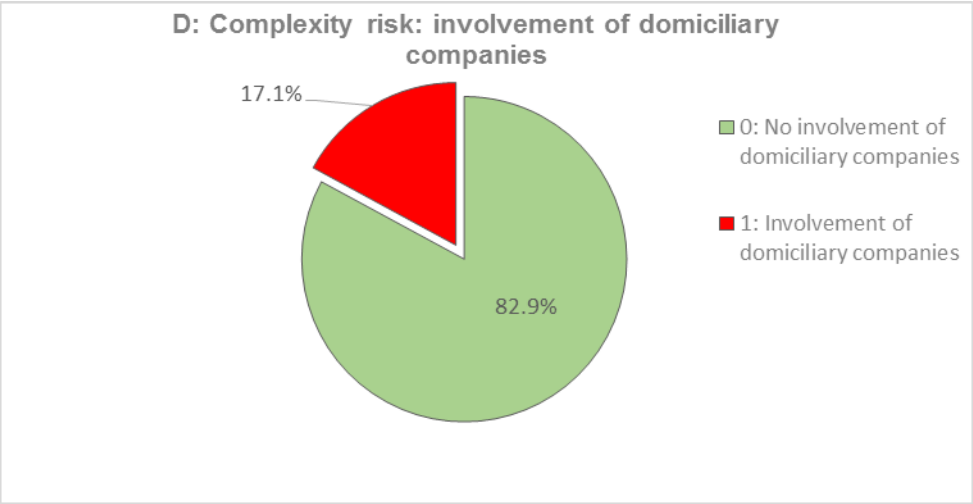
C. Complexity risk I: number of players involved

Number of players	N	Percentage applicable	Cumulative percentage
1: 1-3: Minimal risk	5756	57.1%	57.1%
2: 4-7: Medium risk	3223	32.0%	89.1%
3: 8-10: High risk	620	6.1%	95.2%
4: >10: Very high risk	479	4.8%	100.0%
N applicable	10 078	100.0%	
Total (∑)	10 491		



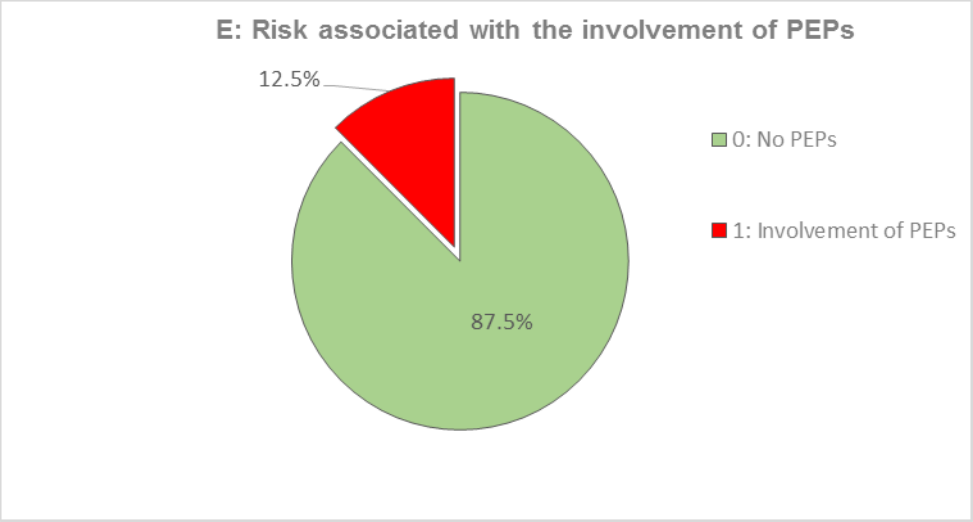
D. Complexity risk II: involvement of domiciliary companies

	N	Percentage applicable	Cumulative percentage
0: No involvement of domiciliary companies	8697	82.9%	82.9%
1: Involvement of domiciliary companies	1794	17.1%	100.0%
N applicable	10 491	100.0%	



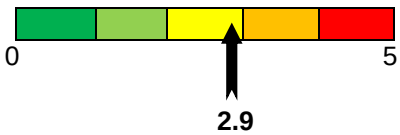
E. Heightened risk associated with the involvement of politically exposed persons

	N	Percentage applicable	Cumulative percentage
0: No PEPs	3565	87.5%	87.5%
1: Involvement of PEPs	509	12.5%	100.0%
N applicable	4074	100.0%	
Total (∑)	6738		

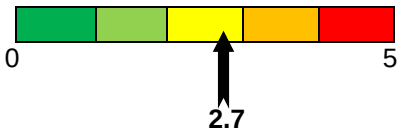


2. Results of the risk calculation using a quantitative matrix per sector

Banks

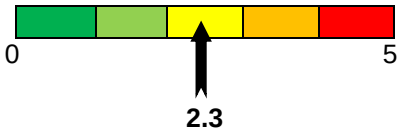


Category 1 banks

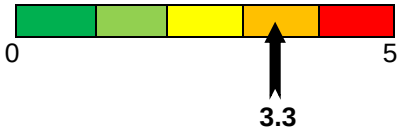


Category 2 banks

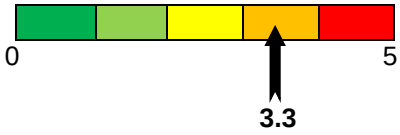
Category 3 banks



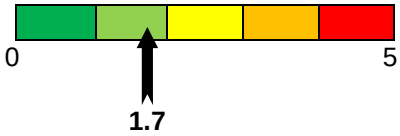
Securities dealers



Asset managers

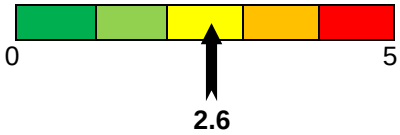


Insurers

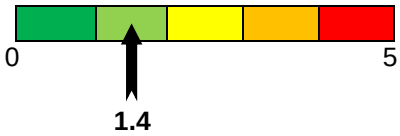


Lawyers and notaries

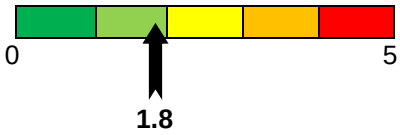
Fiduciaries



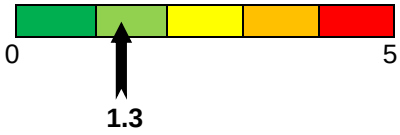
Casinos



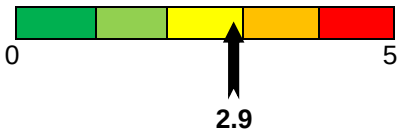
Money transmitters



Lending businesses



Payment service providers



(The number of suspicious activity reports from the precious metal traders sector was insufficient to be statistically significant.)

9.2 Sources

Official statistical sources consulted

- Federal Statistical Office (FSO), Police Crime Statistics (PCS), 2009-2013
- Federal Statistical Office (FSO), Conviction Statistics (COS), 2009-2014
- Swiss National Bank (SNB), Monthly Statistical Bulletins, 2011-2014

Statistics and databases made available to the CGMF

- Money Laundering Reporting Office Switzerland (MROS), database of suspicious activity reports and other information (GEWA), 2004-2014

National documentation and reports consulted

- Dispatch of 17 June 1996 regarding the Federal Act on Combating Money Laundering in the Financial Sector, BBl 1996 III 1057
- Dispatch of 13 December 2013 regarding the implementation of the revised Financial Action Task Force (FATF) recommendations of 2012, BBl 2014 585

- Annual reports of the Federal Office of Police (fedpol), 2004-2014
- Annual reports of the Money Laundering Reporting Office Switzerland (MROS), 2004-2014
- Annual report of the Cybercrime Coordination Unit Switzerland (CYCO), 2013
- Analytical report on money laundering in the real estate market, Federal Office of Police (fedpol), 2013
- Analytical report on money laundering rulings handed down in Switzerland, Federal Office of Police (fedpol), 2008
- Analytical report on money laundering rulings handed down in Switzerland, Federal Office of Police (fedpol), 2014
- Analytical report on the organised smuggling of migrants and Switzerland, Federal Office of Police (fedpol), 2014
- Situation reports of the Federal Intelligence Service (FIS), 2010-2014
- Evaluation report entitled "Free ports and open customs warehouses. An evaluation of licensing and inspection activities", Swiss Federal Audit Office (SFAO), 2014
- Background report on commodities prepared by the interdepartmental commodity platform for the attention of the Federal Council, Federal Department of Foreign Affairs (FDFA), Federal Department of Finance (FDF), Federal Department of Economic Affairs, Education and Research (EAER), 2013
- Switzerland's strategy in relation to the freezing, confiscation and restitution of illicitly acquired assets of politically exposed persons, Federal Department of Foreign Affairs (FDFA), 2014
- Federal Council report on virtual currencies in response to the Schwaab (13.3867) and Weibel (13.4070) postulates, 2014
- Federal Council's response to the Wyss motion (11.4161) "No money laundering in the proprietary trading of commodities", 2012
- Response to postulate 13.3365 of the National Council Foreign Affairs Committee entitled "Greater transparency in the commodities sector", 2013
- Federal Council's response to the Abate postulate (14.4049) entitled "Safe-deposit boxes outside of banks", 2015

- National Risk Assessment, Anti-Money Laundering/Countering Financing of Terrorism, New Zealand Police, 2010
- Singapore National Money Laundering and Terrorist Financing Risk Assessment Report, 2013
- National Risk Assessment of Money Laundering in the Republic of Serbia, 2013

- Internal/confidential reports

- Responses to mandates given by MROS to authorities and the private sector

FINMA documents consulted

- FINMA Newsletter 18 (2010), Handling of life insurances with separately managed accounts/portfolios
- FINMA position paper on legal and reputational risks in cross-border financial services (2010)
- FINMA circular 2008/4 "Securities journals"
- FINMA circular 2011/1 "Financial Intermediation under the AMLA"
- FINMA circular 2011/2 "Capital buffer and capital planning – banks"
- FINMA circular 2013/3 "Auditing"

- FINMA circular 2013/8 "Market conduct rules"
- Due diligence obligations of Swiss banks when handling assets of "politically exposed persons" – An investigation by FINMA, 2011

Reports of the FATF and other international bodies involved in combating money laundering and terrorist financing
- Third mutual evaluation report on anti-money laundering and counter-terrorist financing in Switzerland, 2005
- Follow-up report to the mutual evaluation of Switzerland, 2009

- Money Laundering and Terrorist Financing in the Securities Sector, 2009
- Detecting and preventing the illicit cross-border transportation of cash and bearer negotiable instruments, 2010
- Global Money Laundering and Terrorist Financing Threat Assessment, 2010
- Money Laundering Using New Payment Methods, 2010
- Combating Proliferation Financing: A Status Report on Policy Development and Consultation, 2010
- Laundering the Proceeds of Corruption, 2011
- Report on Money Laundering Vulnerabilities of Free Trade Zones, 2011
- Money laundering risks arising from trafficking in human beings and smuggling of migrants, 2011
- Money laundering and terrorism financing vulnerabilities of legal professionals, 2013
- National Money Laundering and Terrorist Financing Risk Assessment, 2013
- Politically Exposed Persons (Recommendations 12 and 22), 2013
- The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing, 2013
- Risk of Terrorist Abuse in Non-profit Organizations, 2014

- International Monetary Fund (IMF), "Macroeconomic Implications of Money Laundering", Peter J. Quirk, International Monetary Fund, Monetary and Exchange Affairs Department, 1996
- International Monetary Fund (IMF), "Financial System Abuse, Financial Crime and Money Laundering – Background paper", 2001
- United Nations, United Nations Office on Drugs and Crime (UNODC), World Drug Reports, 2001-2011
- United Nations, United Nations Office on Drugs and Crime (UNODC), "Estimating Illicit Financial Flows Resulting From Drug Trafficking and Other Transnational Organized Crime, Research Report", 2011
- United Nations, Counter-terrorism Implementation Task Force (CTITF), "Tackling the Financing of Terrorism", Working Group Report, New York, 2009
- House of Lords, Money Laundering and the Financing of Terrorism, London, 2009
- Asia/Pacific Group on Money Laundering (APG), Typology report – Trade-based money laundering, 2012
- Bank for International Settlements (BIS), Derivative Statistics, 2014
- OECD, OECD Foreign Bribery Report, An Analysis of the Crime of Bribery of Foreign Public Officials, Paris, 2014
- European Union Terrorism Situation and Trend Report, EUROPOL 2014

Reports of non-governmental organisations and associations
- Swiss Bankers Association (SBA), "The economic importance of the Swiss financial centre", 2012
- Swiss Bankers Association (SBA), "Wealth management – at a global level and in Switzerland", 2013
- Swiss Bankers Association (SBA), "Switzerland as a commodity trading centre", 2013
- The Boston Consulting Group, "Global Wealth", 2013
- Ticino Banking Association, "Ticino's financial centre", 2014
- World Gold Council, Quarterly Statistics, 2012-2013
- World Gold Council, PricewaterhouseCoopers, The Direct Economic Impact of Gold, 2013
- Geneva Trading and Shipping Organization (GTSA), Annual Activity Report 2013-2014
- Global Financial Integrity, "Illicit Financial Flows from Developing Countries 2001-2010", 2012
- Global Financial Integrity, "Illicit Financial Flows from Developing Countries 2003-2012", 2014
- Qatar Financial Centre, "The Global Financial Centres Index 15-16", London, 2014
- Transparency International, Corruption Perceptions Index, 2015

Academic sources

- Anthony Amicelle, "Les professionnels de la surveillance financière. Le malentendu comme condition de possibilité", Criminologie, vol. 46, n° 2, 2013, pp. 195-219.
- Isabelle Augsburger-Bucheli (dir.), Blanchiment d'argent: actualité et perspectives suisses et internationales, Paris, 2014
- A. Bergmann et al., Regulierungskostenanalyse zum Finanzinstitutsgesetz, ZHAW School of Management and Law, Zurich, 2014
- Paolo Bernasconi, Finanzunterwelt. Gegen Wirtschaftskriminalität und organisiertes Verbrechen, Zurich, 1988
- Claudio Besozzi, Organisierte Kriminalität – Synthese der Forschungsprojekte", in: Mark Pieth (dir.), Gewalt im Alltag und organisierte Kriminalität – Die Ergebnisse eines nationalen Forschungsprogramms, Bern, Stuttgart, Vienna, 2002, pp. 71-150
- Marie Boillat, Trafic illicite de biens culturels et coopération judiciaire internationale en matière pénale, Schulthess éditions romandes, Geneva, 2012
- Fausto Martin, De Sanctis, Money Laundering Through Art. A Criminal Justice Perspective, Cham 2013
- Stefan D. Heigner, Friedrich Schneider, Florian Wakolbinger, "Combating Money Laundering and the Financing of Terrorism: A Survey", Economics of Security Paper 65, Berlin, 2012
- Bernd Helmig, Hans Lichtsteiner, Markus Gmür (dir.), Der dritte Sektor in der Schweiz. Länderstudie zum Johns Hopkins Comparative Nonprofit Sector Projekt (CNP), Bern, Stuttgart, Vienna, 2010
- Martin Killias et al., Sondage au sujet des expériences et opinions sur la criminalité en Suisse, Analyse dans le cadre du sondage national de victimisation, University of Zurich, Criminology Institute, Zurich, 2011
- Mark Pieth and Dieter Freiburghaus, Die Bedeutung des organisierten Verbrechens in der Schweiz. Report on behalf of the Federal Office of Justice, Bern, 1993
- Mark Pieth (dir.), A Comparative Guide to Anti-Money Laundering. A Critical Analysis of Systems in Singapore, Switzerland, the UK and the USA, Cheltenham, 2004
- Friedrich Schneider, "Shadow Economies around the world: What do we really know?" in: European Journal of Political Economy, vol. 21, n° 3, 2001, pp. 598-42
- Friedrich Schneider, "Turnover of organized crime and money laundering: some preliminary empirical findings", in: Public Choice, vol. 144, n° 3, 2010, pp. 473-86
- Friedrich Schneider, "The Financial Flows of the Transnational Crime: Some Preliminary Empirical Results", Economics of Security Paper 53, Berlin, 2011
- Jeffrey Simser, "Money Laundering: Emerging Threats and Trends", in: Journal of Money Laundering Control vol. 16 n° 1, 2013, pp. 41-54
- Tamara Taube, Entstehung, Bedeutung und Umfang der Sorgfaltspflichten der Schweizer Banken bei der Geldwäschereiprävention im Bankenalltag, Zurich, St. Gallen, 2013
- Brigitte Unger, The Scale and Impacts of Money Laundering, Cheltenham, 2007
- Brigitte Unger and Daan van der Linde, Research Handbook on Money Laundering, Cheltenham, 2013
- John Walker, "How Big is Global Money Laundering?", in: Journal of Money Laundering Control, vol. 3, n° 1, 1999, pp. 25-37

European case law

- Michaud v. France, Judgment of 6 December 2012 of the European Court of Human Rights (ECHR)

List of abbreviations

AMLCA	Anti-Money Laundering Control Authority
BO	Beneficial owner
FTA	Federal Tax Administration
FCA	Federal Customs Administration
SBA	Swiss Bankers Association
SNB	Swiss National Bank
CC	Swiss Civil Code
CDB 08	Agreement of 2008 on the Swiss Banks' Code of Conduct with regard to the Exercise of Due Diligence
SFAO	Swiss Federal Audit Office
SFBC	Swiss Federal Banking Commission
FGB	Federal Gaming Board
CPM	Central Office for Precious Metal Control
CO	Swiss Code of Obligations
SCC	Swiss Criminal Code
CrimPC	Criminal Procedure Code
FIU	Financial Intelligence Unit
DIL	Directorate of Public International Law (FDFA)
DDPS	Federal Department of Defence, Civil Protection and Sport
EAER	Federal Department of Economic Affairs, Education and Research
FDFA	Federal Department of Foreign Affairs
FDF	Federal Department of Finance
FDHA	Federal Department of Home Affairs
FDJP	Federal Department of Justice and Police
DGC	Directorate General of Customs
ACLA	Federal Act on Administrative Criminal Law
SFPD	Sectoral Foreign Policies Division (FDFA)
AEOI	Automatic exchange of information
IMAC	Federal Act on International Mutual Assistance in Criminal Matters
Fedpol	Federal Office of Police (FDJP)
FINMA	Swiss Financial Market Supervisory Authority
IMF	International Monetary Fund
FATF	Financial Action Task Force
CGMF	Interdepartmental coordinating group on combating money laundering and the financing of terrorism
GRECO	Group of States against Corruption (Council of Europe)
BankA	Federal Act on Banks and Savings Banks
AMLA	Federal Act on Combating Money Laundering and the Financing of Terrorism in the Financial Sector
SESTA	Federal Act on Stock Exchanges and Securities Trading
UCA	Federal Act on Unfair Competition
PMCA	Federal Act on the Control of the Trade in Precious Metals and Precious Metal Articles
CustA	Federal Customs Act
FINMASA	Federal Act on Federal Financial Market Supervision
CivISA	Federal Act on Responsibilities in the Area of the Civilian Intelligence Service
GamblA	Federal Act on Gambling and Gambling Casinos
ISA	Federal Act on Measures to Safeguard Internal Security
DEBA	Federal Act on Debt Enforcement and Bankruptcy
CISA	Federal Act on Collective Capital Investment Schemes
RIAA	Federal Act on the Restitution of Assets Obtained Unlawfully by Politically Exposed Persons

IOA	Federal Act on the Oversight of Insurance Companies
SPTA	Federal Act on the Surveillance of Postal and Telecommunications Traffic
NarcA	Federal Act on Narcotics and Psychotropic Substances
CPTA	Federal Act on the International Transfer of Cultural Property
FISA	Federal Act on Intermediated Securities
OAG	Office of the Attorney General of Switzerland
MROS	Money Laundering Reporting Office Switzerland (FDJP)
NPO	Non-profit organisation
SRO	Self-regulatory organisation
AMLO-FGB	Ordinance of the Federal Gaming Board on the Diligence of Casinos in Combating Money Laundering
AMLO-FINMA	Ordinance of the Swiss Financial Market Supervisory Authority on the Prevention of Money Laundering and the Financing of Terrorism
OECD	Organisation for Economic Co-operation and Development
PMCO	Ordinance on the Control of the Trade in Precious Metals and Precious Metal Articles
CustO	Customs Ordinance
FOPI	Federal Office of Private Insurance
FOC	Federal Office of Culture (FDHA)
FOJ	Federal Office of Justice (FDJP)
FCRO	Federal Commercial Registry Office (FDJP)
FSO	Federal Statistical Office (FDHA)
PFIO	Ordinance on the Professional Practice of Financial Intermediation
GamblO	Ordinance on Gambling and Gambling Casinos
GDP	Gross domestic product
FCP	Federal Criminal Police (FDJP)
SMEs	Small and medium-sized enterprises
PEP	Politically exposed person
CYCO	Cybercrime Coordination Unit Switzerland (FDJP)
SECO	State Secretariat for Economic Affairs (EAER)
FSBF	Federal Supervisory Board for Foundations
SIF	State Secretariat for International Financial Matters (FDF)
GS-FDF	FDF General Secretariat
FIS	Federal Intelligence Service (DDPS)
EU	European Union
UNODC	United Nations Office on Drugs and Crime