h e g

Haute école de gestion
Genève

In the fight against money laundering: How Swiss banks can counter the rise of money laundering networks

Bachelor Project submitted for the degree of
Bachelor of Science HES in International Business Management

by

Endrita BEHLULI

Bachelor Project Mentor:
Sylvain GODINET, Lawyer

Geneva, June 2nd, 2023
Haute école de gestion de Genève (HEG-GE)
International Business Management

Hes·so GENÈVE
Haute Ecole Spécialisée de Suisse occidentale

Disclaimer

This report is submitted as part of the final examination requirements of the Haute école de gestion de Genève, for the Bachelor of Science HES-SO in International Business Management. The use of any conclusions or recommendations made in or based upon this report, with no prejudice to their value, engages the responsibility neither of the author, nor the author's mentor, nor the jury members nor the HEG or any of its employees.

Acknowledgements

I would like to sincerely thank Mr. Sylvain Godinet, the supervisor for my Bachelor's thesis, for his valuable guidance and advice throughout the entire process.

Additionally, I would like to extend a special acknowledgment to Mr. Arnaud Beuret, the prosecution office of the canton of Aargau, as well as the interviewee 1 for generously dedicating their time to participate in the interviews. Also, I would like to thank the compliance officers who took part in the survey. The valuable contributions and insights of the interviewees and responders have greatly enriched this Bachelor's thesis, enabling a comprehensive analysis of the subject matter.

Furthermore, I am very thankful to my family, whose unwavering support has been instrumental during the months of my research.

Executive Summary

In recent years, there has been a notable increase in money laundering cases associated with various predicate offenses, both at the national and international levels. Notably, the annual reports from the Money Laundering Reporting Office Switzerland (MROS) and other Financial Intelligence Units (FIUs), highlight the significance of fraud as a predicate offense in the reported suspicious activities. As a consequence, this bachelor thesis focuses on money laundering with fraud as a predicate offense.

The advent of online banking has transformed the process of opening bank accounts, granting customers the convenience of bypassing traditional in-person visits to bank branches. However, this convenience has also attracted the attention of cybercriminals who exploit vulnerabilities in the system and use various methods coercing victims into transferring funds and even becoming unwitting money mules. Detecting and combating these illicit activities is crucial in countering money laundering, with banks playing a crucial role in this. Nevertheless, banks face significant challenges in identifying fraudulent patterns due to the massive volume of transactions processed within their systems, whereby traditional monitoring methods often struggle to keep up.

It is important to acknowledge that there are some inherent limitations within this study. Firstly, the scope of this project does not encompass all types of banks, and therefore, the recommendations provided may not be universally applicable to different banking activities and customer segments. Consequently, the focus is primarily on retail and neo banks, which are increasingly experiencing an increase in the number of fraud cases. Secondly, the perspectives of key stakeholders such as fraudsters themselves or the victims of fraudulent activities were not included in this study. While their viewpoints could offer valuable insights, incorporating them would deviate from the central focus of this thesis.

Through comprehensive analysis and insights garnered from interviews with relevant stakeholders, this study has identified effective strategies that banks can adopt to enhance their ability to detect and prevent money laundering more efficiently. However, an accurate assessment of risk costs relies on various factors such as a bank's size, employee count, risk exposure, and risk appetite. Yet it is worth noting that certain tasks, which traditionally required time-consuming manual work, can be swiftly accomplished by advanced systems. Although such systems require significant investments, in the long run, they offer a return on equity (ROE) that cannot be achieved with human labor.

Table of Contents

List of Abbreviations

AI	Artificial Intelligence
AML	Anti Money Laundering
AMLA	Anti Money Laundering Act
AMLD	Anti-Money Laundering Directive
AMLO	Anti-Money Laundering Ordinance
ANR	French National Agency for Fraud Prevention
BSA	Bank Secrecy Act
CDB	Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence
CFT	Countering the Financing of Terrorism
DGB	Bundesgesetz über die direkte Bundessteuer
EBA	European Banking Authority
ESFS	European System of Financial Supervision
EU	European Union
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FCC	Federal Criminal Court
FDF	Federal Department of Finance
FDFA	Federal Department of Foreign Affairs
FDJP	Federal Department of Justice and Police
FEDPOL	Federal Office of Police
FIU	Financial Intelligence Unit
FINMA	Swiss Financial Market Supervisory Authority
FTC	Federal Trade Commission
HRR	High Risk Relation
ICO	Initial Coin Offerings
KGGT	Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung
KYC	Know-your-customer
MROS	Money Laundering Reporting Office Switzerland
NCSC	National Cyber Security Center
NRA	National Risk Assessment
NZZ	Neue Zürcher Zeitung
OAG	Office of the Attorney General of Switzerland
PEP	Politically exposed persons
SAR	Suspicious activity reports
SBA	Swiss Bankers Association
SCC	Swiss Criminal Code
SKPPSC	Swiss Crime Prevention
SRT	Swiss Radio and Television
Tracfin	Traitement du renseignement et action contre les circuits financiers clandestins
US	United States
USA	United States of America

List of Figures

1. Introduction

There has been a notable rise in the number of reported suspicious activities associated with money laundering in recent years, occurring at both national and international levels. Fraud as a predicate offense to money laundering is an important component of this, which is also the main predicate offense analysed in this thesis.

Fraudsters have been capitalizing on the convenience of online bank account openings to engage in fraudulent activities and integrate illicit funds into the financial system. These perpetrators have devised various methods to exploit unsuspecting individuals, such as luring them with fake job offers that require unwittingly opening accounts for the fraudsters' illicit purposes. (Zurich Cantonal Police, 2020). Another type of job offer involves victims receiving funds in their personal accounts and being tasked with transferring the money to predetermined recipients. (Fribourg Cantonal Police, 2022). Interestingly, a significant portion of these funds often flows to countries like Russia or West African nations such as Benin. (Bernhard DROZ, 2021).

Of course, it is not only through fake job offers that perpetrators target their victims. Fraud can occur through various means, such as investment fraud or romance scams, which will be further explained in the following section.

The identification of suspicious transactions within banks and subsequent reporting to the MROS plays a crucial role in uncovering and dismantling money laundering networks. Collaborative efforts have led to notable successes, including the apprehension of over 200 individuals involved in such activities by Europol in 2019, including some within Switzerland. (NZZ, 2019). However, despite existing measures in transaction monitoring, banks still face challenges in identifying these suspicious transactions due to the high volume of transactions processed. Nonetheless, Swiss banks operate under the framework of the Anti-Money Laundering Act (AMLA), which mandates the utmost diligence in financial transactions. (Art.1 AMLA). Therefore, it is imperative for banks to strike a balance between complying with anti-money laundering regulations and fulfilling their obligation to provide financial services to their clients.

Overall, banks encounter various challenges resulting from the surge in money laundering activities and must find effective ways to mitigate these risks efficiently.

2. Literature review

2.1 The international rise of fraudulent activities

International cybercrime has increased significantly as a result of the COVID-19 pandemic. The sudden shift to remote work and increased online activity is one of the main drivers. Consequently, the use of digital technology and online communication platforms has increased with the growing number of people working from home. Cyber criminals took advantage of this situation by launching phishing attacks, malware attacks, and other cyber-attacks targeting remote workers and their devices. As a result, cyberattacks on businesses and individuals increased, and perpetrators gained access to victims' account information. (Deloitte[1]). According to statistics from the National Cyber Security Center (NCSC), 350 cases of cyberattacks were reported in Switzerland in April 2020, during the first months of the pandemic. Comparatively, between 100 and 200 cases were reported during the same period before the pandemic. One of the main causes was that the employees working from home lacked the same protective measures as at the workplace and may have received too little training on the phishing threats. (Deloitte). After all, according to a study, 47% of those working in the home office fell for a phishing scam. (Tessian, 2020). In private internet use as well, victims are often asked to provide their private details through fake websites, which are then used by the perpetrators for the purpose of carrying out fraudulent activities. (SKPPSC, 2022:2).

As described by the Interdepartmental Coordination Group for Combating Money Laundering and Terrorist Financing (KGGT[2]) in their National Risk Assessment (NRA) on fraud and phishing with the aim of identifying new money laundering and terrorist financing threats and proposing possible measures to mitigate them to the federal administration, phishing refers to the process of attempting to elicit confidential data from a user by misleading and in an unauthorized manner. (KGGT, 2020:27). Phishing attacks often aim to trick victims into providing sensitive information such as credit card details, bank account information, or login credentials. If successful, cybercriminals can use this information to steal money from victims, conduct fraudulent transactions or steal data to sell on the dark net. (KGGT, 2020:27). (Financial Conduct Authority (FCA), 2022). This

[1] N.B.: This article has no publication date, but talks among other information about data from May 2020 and must therefore necessarily have been published after this time.

[2] N.B.: In this paper, KGGT is used as an abbreviation for “Interdepartmental Coordination Group for Combating Money Laundering and the Financing of Terrorism”, which is the German abbreviation for "Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung", given that there is no official English translation.

makes it difficult for banks to detect that fraud is taking place, despite having the proper systems in place. Often it is a sudden increase in the number of outgoing transactions or the information from the victim itself that allows the bank to detect it.

Similar patterns can be seen internationally. In PwC's Global Economic Crime and Fraud Survey 2022, among 1296 companies in 53 countries, 46% reported experiencing some type of fraud or other financial crime in the past 24 months. (PwC Global Economic Crime and Fraud Survey 2022, 2022:4). The most common type of fraud in the financial sector was customer fraud with 44%, followed by cybercrime with 38% and Know-your-customer (KYC) failure accounting to 29%. (PwC Global Economic Crime and Fraud Survey 2022, 2022:6)

As a result of the lockdown, many people switched to online shopping, and online commerce grew strongly during the pandemic. Criminal groups have also taken advantage of this trend and are increasingly using online channels for criminal activities such as fraud and trading in counterfeit goods. (The Economist, 2021:2). In the 2021 semi-annual report, the NCSC reported that the number of cases increased to 21’714, twice as many as in the previous year. The most frequently reported cases, which accounted for about half of all reports, were related to fraud. The identifiable phenomena were fake sextortion, which accounted for the largest share of reports, as well as other categories such as advance fee fraud, investment fraud, and classified ad scams. (NSCS Semi-Annual Report 2021/2, 2022:10).

Similarly, the MROS reported in its 2021 annual report that 54.9% of the suspicious cases received indicated fraud as the predicate offence. (MROS, Annual Report 2021, 2022:19).

The KGGT describes in the NRA of 2020, among other things, the fraudulent phenomena at the expense of private individuals, which include the following:

2.1.1 Investment fraud

In investment fraud, fraudsters try to convince their potential victims to invest their money by offering high profits. However, these funds or other assets are not or only partially invested, but are used to enrich the perpetrator. (KGGT, 2020:34).

According to a research of the Swiss Radio and Television (SRT), a high increase in investment fraud has been observed in Switzerland in recent years. The victims are usually contacted by very professional acting fraudsters and are promised high returns. Often after a first deposit, the victims see 100% profits, which drives them to invest more

and more. It is difficult for the victims to detect the fraud, because the websites are also professionally designed with security measures similar to those of e-banking. (SRT, 2022).

In 2021, the Swiss Financial Market Supervisory Authority (FINMA) published a report on “How investors can protect themselves against unauthorised financial market providers". In it, it also provided information on the various tactics used by investment fraudsters, such as using sustainable investments as bait. (FINMA, 2021:10). According to an undated publication of the city of Zurich, the amount of loss in such dubious sustainable investments is up to CHF 500'000. Investment fraud often involves the operation of international networks. Not least in 2020, a European network of investment fraudsters was identified in Germany, who obtained more than 100 million euros through investment fraud. (Spiegel, 2020).

In order to commit investment fraud, the fraudsters make use of various schemes of allocation, such as the following:

- Ponzi scheme: It's an investment fraud where new investors' money is used to pay returns to previous investors, creating the illusion of success. The scam relies on recruiting new investors and doesn't actually invest the money as promised. If there aren't enough new investors or the fraud is exposed, the scheme collapses. (KGGT, 2020:35).

- Snowball or pyramid scheme: It's an investment system where new investors are recruited to generate money. Participants pay an upfront fee and receive rewards for recruiting more members. Each level of the pyramid gets rewards from the levels below. The scheme relies on continuous recruitment to pay rewards. (KGGT, 2020:35).

The main difference is that in a pyramid scheme, participants recruit new members, while in a Ponzi scheme, they don't. Pyramid schemes often sell products/services to appear legitimate, while Ponzi schemes lack real business activity.

Both schemes are illegal and can cause significant financial losses.

Another form of investment fraud is the fraudulent Initial Coin Offerings (ICO) which involves cryptocurrencies. Through an ICO, developers typically raise the necessary capital to bring their new cryptocurrency or business idea to market, similar to fundraising. Investors provide funds to ICO organizers and in return receive so-called tokens of the new currency. One form of ICO fraud is the so-called ICO exit scam. The

perpetrators pretended to start a new company and raise money through an ICO. Ultimately, they leave with the assets, leaving investors with nothing in exchange for their deposits. (KGGT, 2020:35).

Investment fraud is also apparent at the international level. In early 2023, the UK Financial Conduct Authority (FCA) published that investment scams increased by 193% in the last five years. (FCA, 2023).

2.1.2 Fraud on sales portals

In this case, the perpetrators sell well-known branded goods at very low prices in internet shops. However, the goods ordered and paid for never reach the customer, or the goods turn out to be fake or inferior. In some cases, fraudsters use established Internet auction portals and offer goods there that do not belong to them at all. (KGGT, 2020:33). As also mentioned in an article by the Swiss Crime Prevention (SKPPSC[3]), the sellers often break off contact with the buyers immediately after receiving payment and transfer the funds received to partially foreign accounts, which makes it difficult for the victims to reclaim the transfer through a bank recall.

2.1.3 Advance fee fraud

Under this modus operandi, perpetrators send messages promising high profits or commissions to potential victims. However, in order to trigger this payment, an advance payment must be made. Victims are often lured by the perpetrators stating that the victim has inherited a large sum of money. However, in order to receive the inheritance, notary fees or other costs must first be paid. Another method is lottery winnings, where victims are fooled into believing that they have won a fictitious lottery prize. Here, too, the victim is required to pay an advance fee in order to receive the winnings. (KGGT, 2020:38).

2.1.4 Romance Scam

Romance scam is a type of online fraud in which criminals create fake profiles on dating sites, social media platforms, or mobile apps to target individuals seeking relationships. (KGGT, 2020:40).

Scammers build relationships with their victims, often using flattery, compliments and emotional manipulation to gain their trust. Once in a relationship, scammers usually demand money by making up emergency stories or gradually requesting small amounts

[3] N.B. This article has no publication date, however, it talks about data from the year 2021 and it can therefore be assumed that it was published after this time.

of money over time. (FCA, 2022). (SKPPSC, 2019). Romance scams are very effective because scammers are skilled at building trust and an emotional connection with their victims. This trend can also be observed internationally. In 2022, the Federal Trade Commission in the U.S. published an article in which they noted an 80% increase in reported romance scam cases in 2021 compared to 2020. However, romance scams are not just about stealing funds from victims. More and more, the perpetrators take advantage of its victims to make them do their alleged partner a favour and transfer funds. The fraudster often claims that he needs help in obtaining inheritance money or transferring funds for an important business. In fact, however, these transactions involve stolen funds, and just like that, the victims become perpetrators as well, by becoming so-called money mules. (FTC[4], 2022).

2.2 Money mules

The term money mule or financial agent refers to the people who have the task of laundering money obtained through crime. (SKPPSC, 2018). Often the money mules are not aware that they are involved in an illegal business, because they are lured by the criminals through bogus orders. The perpetrators usually publish job offers on online platforms, which promise high commissions and little work. The applicants are supposed to process payments from Switzerland or transfer donations to third countries as financial agents for apparently international companies. (KGGT, 2020:44). The transactions take place on the private bank accounts of the recruited financial agents. As banks and other financial institutions increasingly recognize and prohibit large numbers of payments from or to third parties, the money mules are hired to withdraw the funds in cash and send them by post or money transfer companies, or to exchange them for cryptocurrencies. (KGGT, 2020:44). (SKPPSC, 2018). The money mules are compensated for their services by receiving a few percent of the amount to be transferred. (KGGT, 2020:44). What the money mules often do not know is that anyone acting as a money mule, knowingly or unknowingly, is liable to prosecution for money laundering under Swiss criminal law. (SKPPSC, 2018).

2.2.1 Money laundering scheme

Money laundering is a complex process that involves concealing the illicit origins of funds and making them appear legitimate. This illicit activity typically unfolds in a series of three interconnected stages, each serving a distinct purpose in the money laundering scheme.

[4] US Federal Trade Commission

By understanding these stages, we can gain insight into the intricate methods used by individuals and criminal organizations to disguise the true source of their funds (Vision Compliance, 2021[5]).

1. Placement: Funds acquired through financial crime are introduced into the financial system and laundered by placing them into a legitimate financial account. Criminals can use methods such as smurfing to ease the placement. Smurfing describes the process of breaking up large sums of money into smaller amounts before depositing them into the bank accounts. Thus, these small sums do not draw attention and do not generate suspicion in the banks to carry out clarifications.

2. Layering: Once the funds enter the financial system, criminals create layers of financial transactions through wire transfers, currency exchanges, or the buying and selling of assets to disguise the true origin, ownership, and destination of the illicit funds. The goal is to make it difficult for law enforcement to trace the funds and to create a complex paper trail that obscures the illicit origin of the money. (FATF[6], 2018:18).

3. Integration: In a final phase, the funds are integrated into the economy through various investments such as real estate, luxury goods or businesses, and by means of forged invoices, contracts or the like.

2.3 Swiss system of combating economic crime

Since its establishment in 1877, the **Swiss Federal Audit Office (SFAO)** has held the position of the supreme financial supervisory body in Switzerland. As an independent institution, it is bound solely by the Federal Constitution of the Swiss Confederation and the applicable laws, as stated in Article 1, paragraph 1 of the Federal Act on the Swiss Federal Audit Office (FCA). The SFAO's primary responsibility is to conduct financial audits and assessments of the federal government, its entities, and other bodies under federal jurisdiction. (SFAO Website).

The **Office of the Attorney General of Switzerland (OAG)** is responsible for investigating and prosecuting criminal offenses at the federal level. With its four divisions

[5] Reference from the course material of the completed diploma "Compliance Officer AML Specialist" at Vision Compliance in Geneva in May 2022

[6] Financial Action Task Force (FATF)

it focuses different complex economic crimes. The OAG collaborates closely with domestic and international law enforcement agencies. (OAG Website).

The **Federal Department of Finance (FDF)** is one of the seven departments of the Swiss Confederation and is responsible for the country's financial and budgetary policy as well as for the supervision and regulation of the financial markets. Among other things, the FDF is responsible for the supervision of various financial institutions and financial market players. As a member of the Federal Council, Finance Minister Karin Keller-Sutter heads the FDF. (FDF Website).

The **Federal Office of Justice (FOJ)** is another key institution involved in combating economic crime. It oversees the administration of justice, including the enforcement of criminal penalties and the coordination of mutual legal assistance requests with foreign jurisdictions. The FOJ plays a crucial role in facilitating international cooperation in different matters. (FOJ, 2010).

The **Federal Office of Police (FEDPOL)** works closely with the enforcement agencies to investigate and combat serious and organized crime, including economic offenses. It gathers intelligence, conducts investigations, and supports the prosecution of complex cases. The FEDPOL's expertise in financial investigations, forensic analysis, and international cooperation contributes to the effective detection and disruption of economic crime networks. (FEDPOL Website). Within the FEDPOL, the **Money Laundering Reporting Office Switzerland (MROS)** operates as a specialized unit. MROS is responsible for receiving, analyzing, and disseminating reports of suspicious transactions from financial intermediaries, such as banks and other obligated entities. Its objective is to detect and prevent money laundering activities by identifying patterns, trends, and potential links to organized crime or other illicit activities. (FEDPOL Website).

The **Federal Criminal Court (FCC)** is a federal court with its seat in Bellinzona, which is divided into three chambers. It handles complex and significant criminal proceedings, ensuring fair trials and, among other, delivering verdicts on economic crimes. (FCC Website).

The **Swiss Financial Market Supervisory Authority (FINMA)** is an independent regulatory body responsible for overseeing and ensuring the integrity and stability of Switzerland's financial market. While its primary focus is on supervising banks, insurance companies, and other financial institutions, FINMA also plays a crucial role in combating money laundering and enforcing compliance with anti-money laundering (AML) regulations. It sets guidelines, conducts inspections, and imposes sanctions to ensure

the financial sector's adherence to AML and anti-terrorism financing measures. (FINMA Website).

In addition to these institutions, various groups affiliated with the **Federal Department of Foreign Affairs (FDFA)** and the **Federal Department of Justice and Police (FDJP)** contribute to the fight against economic crime. They engage in international cooperation, including the repatriation of illicit assets deposited in Switzerland and the recovery of proceeds from criminal activities abroad or within the country.

The **27 Cantonal Public Prosecutors' Offices** conduct criminal proceedings for felonies, misdemeanors and transgressions. Furthermore, they file charges, issue penalty orders and other final orders such as freezing of assets. (FDJP Website). (Public Prosecutor's Office of Basel-City Website).

In 2013, the Federal Council established the **Interdepartmental Coordination Group for Combating Money Laundering and Terrorism Financing (KGGT)** as a permanent institution. It is led by the Federal Department of Finance and consists of other departments, including the FDJP, the FDFA, as well as FINMA and the OAG. The KGGT is tasked with coordinating measures to combat money laundering and terrorism financing within the federal administration. Its responsibilities include the ongoing assessment of money laundering and terrorism financing risks, ensuring the identification of any necessary measures to mitigate these risks.

2.4 Swiss legal framework with regard to money laundering

Provisions

The Swiss Criminal Code contains anti-money laundering provisions designed to help prevent the illegal concealment of assets. These include Art. 305bis on money laundering.

Money laundering is act of concealing the existence, origin or use of money derived from a crime in order to introduce these illicit assets into the legal economy. (SCC[7], Art. 305bis).

It should be noted that for money laundering, the predicate offence must be a crime of any kind (Art. 10 para. 2 SCC) or a qualified tax offence (Art. 186 DGB[8] and Art. 59 para.

[7] Swiss Criminal Code

[8] Federal Act on Direct Federal Taxation

1 DGB) and not a misdemeanour (Art.10 para. 3 SCC). (Bürgi Nägeli Rechtsanwälte, 2012). (Lenz & Staehlin, 2015:1).

An actor of money laundering is punishable even if the predicate offense is committed abroad, provided that the predicate offense is incriminated in the country of the offense and the offense is considered a crime in Switzerland. (Art. 305bis para. 3 SCC).

Federal law

Legislation to combat money laundering is based on the one hand on the Federal Act on Combating Money Laundering and Terrorist Financing (AMLA). The aim of the AMLA is to prevent criminally obtained assets from entering legal circulation in order to be used, among other things, for the commission of crimes. (Bürgi Nägli Rechtsnawälte, 2012). The purpose of this law is to regulate the fight against money laundering in the sense of article 305bis SCC, the fight against terrorist financing in the sense of article 260quinquies paragraph 1 SCC and to ensure due diligence in financial transactions. (Art.1 AMLA). The AMLA contains general provisions which are substantiated by accompanying ordinances.

Federal Ordinance

The Swiss Anti-Money Laundering Ordinance (AMLO) on Combating Money Laundering and Terrorist Financing is an ordinance issued on the basis of the Swiss Money Laundering Act (AMLA). The Ordinance sets out the specific implementation requirements that must be met by the legal entities and natural persons concerned in order to comply with the legal requirements for combating money laundering and terrorist financing.

The ordinance has been updated and reinforced several times in recent years to meet the changing risks and challenges in the area of money laundering and terrorist financing. (SBA Website).

Memberships

Switzerland has committed to implementing the 40 Recommendations issued by the Financial Action Task Force (FATF) to combat money laundering and terrorist financing and is regularly reviewed by the FATF for compliance. The FATF is an intergovernmental organization that develops and promotes global standards to combat money laundering, terrorist financing and other threats to the integrity of the financial system. Switzerland has been a member of the FATF since 1990, during which time it has actively participated in the development and implementation of international standards to combat money

laundering and terrorist financing. (SBA Website). The FATF's regular country reviews serve to examine the implementation of standards in individual countries and, where necessary, make recommendations for improvement. In spring 2016, Switzerland was subject to a fourth country review by the FATF, which examined the implementation of the 2012 Revised Recommendations on Combating Money Laundering and Terrorist Financing. The results of this review were generally positive and Switzerland scored well. (FATF, 2016).

Furthermore, Switzerland has been a member of the Egmont Group since 1998, which is a global network of Financial Intelligence Units (FIUs) established in 1995 to facilitate the exchange of financial information between member countries in the fight against money laundering and terrorist financing, as well as to share financial information and to collaborate on investigations and prosecutions related to money laundering and terrorist financing. (Egmont Group Website). FIUs are national agencies responsible for collecting, analyzing, and disseminating financial information to relevant authorities. In Switzerland, this is the MROS. (MROS, 2020).

Agreements

The Swiss Bankers Association (SBA) is the umbrella organization of Swiss banks and financial institutions. It was founded in 1912 and today represents the interests of over 250 banks and financial institutions in Switzerland.

The Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CDB) is a set of guidelines developed by the SBA that governs the due diligence obligations of banks and other financial intermediaries with regard to combating money laundering and terrorist financing. The CDB was first introduced in 1977 and is regularly updated to reflect current developments and threats in the area of money laundering and terrorist financing. The CDB serves as a self-regulatory measure and specifies the identification of the contracting party and the determination of the beneficial owner. (SBA Website).

In accordance with Art. 35 AMLO-FINMA, Articles 1 to 57 CDB are in the nature of ordinances and therefore apply to all financial intermediaries, with the articles from Art. 58 CDB 20 onwards representing free self-regulation. (SBA Website).

2.5 International legal framework with respect to money laundering

2.5.1 European Union (EU)

The EU has established a comprehensive legal framework for combating money laundering and terrorist financing. This framework consists of several directives, regulations, and decisions, which set out the obligations and requirements for financial institutions and other entities involved in financial transactions.

The most important of the five EU directives aimed at combating money laundering and terrorist financing are the Fourth Anti-Money Laundering Directive (AMLD 4) and the Fifth Anti-Money Laundering Directive (AMLD 5).

The Fourth Anti-Money Laundering Directive, also known as Directive (EU) 2015/849, is an EU legislation that establishes the minimum rules and requirements for combating money laundering and terrorist financing within the EU. AMLD 4 requires Member States and financial institutions to use risk assessments in order to identify and mitigate money laundering and terrorist financing risks. (EUR-Lex, 2021).

One of the key innovations of AMLD 4 is the introduction of enhanced due diligence measures for high-risk third countries, including measures to be taken when dealing with politically exposed persons (PEP). (EUR-Lex, 2021).

The Fourth Anti-Money Laundering Directive was later updated by the Fifth Anti-Money Laundering Directive (AMLD 5) in 2018, which introduced further measures to strengthen the Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) rules within the EU. (Deloitte, 2018).

The European Union has established a regulatory agency known as the European Banking Authority (EBA) as part of its larger regulatory framework, the European System of Financial Supervision (ESFS), in 2011. Headquartered in Paris, the EBA is tasked with ensuring effective and consistent prudential regulation and supervision of the banking sector across the EU. In the context of AML/CFT, the EBA has issued a number of regulations and guidelines. (EBA, 2016).

Like Switzerland, some EU countries are part of the 39 members of the FATF, including Germany, France, the United Kingdom, Italy, Spain, and the Netherlands. (FATF Website). Most EU member states perform well in FATF evaluations overall and have demonstrated a high level of compliance with international standards to combat money laundering and terrorist financing. However, in some cases, deficiencies and

improvement needs have been identified, particularly in relation to the implementation of regulations in practice. (FATF, 2018). This was also noted in the Cypriot country report, in which Cyprus was downgraded from "largely compliant" in 2019 to "partially compliant" in 2021. (FATF, 2022).

The Egmont Group has a strong presence in the EU with all it's member states being part of the group. This includes countries with diverse economic and political backgrounds, from the largest economies such as Germany and France to smaller countries such as Romania and Slovakia. (Egmont Group Website).

2.5.2 United States of America (USA)

The Bank Secrecy Act (BSA) is a federal law in the United States (US) enacted in 1970 that aims to combat money laundering and is considered the most important AML law. The law requires financial institutions to take certain measures to prevent money laundering and terrorist financing, including reporting suspicious transactions to the relevant authorities. The BSA applies to all financial institutions in the US and is enforced by the Financial Crimes Enforcement Network (FinCEN), an agency within the US Department of the Treasury. (Subsub, 2022).

Over the years, the BSA has been expanded and modified to address changing threats of money laundering and terrorist financing. For example, in 2001, the USA PATRIOT Act was enacted, which supplemented and strengthened the BSA. The USA PATRIOT Act is a federal law in the United States enacted in 2001 in response to the 9/11 terrorist attacks. The law expands the powers of US authorities in the area of national security, including the monitoring of financial transactions. (Subsub, 2022). (FinCEN Website).

Since January 1, 2021, the Anti-Money Laundering Act of 2020 (AMLA 2020) has come into effect intending to address the threats posed by new technologies and criminal methods. The AMLA 2020 includes, among other things, rules for international information exchange and increased penalties for money laundering. (Subsub, 2022).

The United States is one of the founding members of the Financial Action Task Force (FATF), and was evaluated by the organization in 2016. According to the mutual evaluation report, the United States has a well-established and effective framework for combating money laundering and terrorist financing. However, the report also identified certain areas where improvements could be made, including better coordination and information sharing between federal and state AML/CFT authorities. (FATF, 2016).

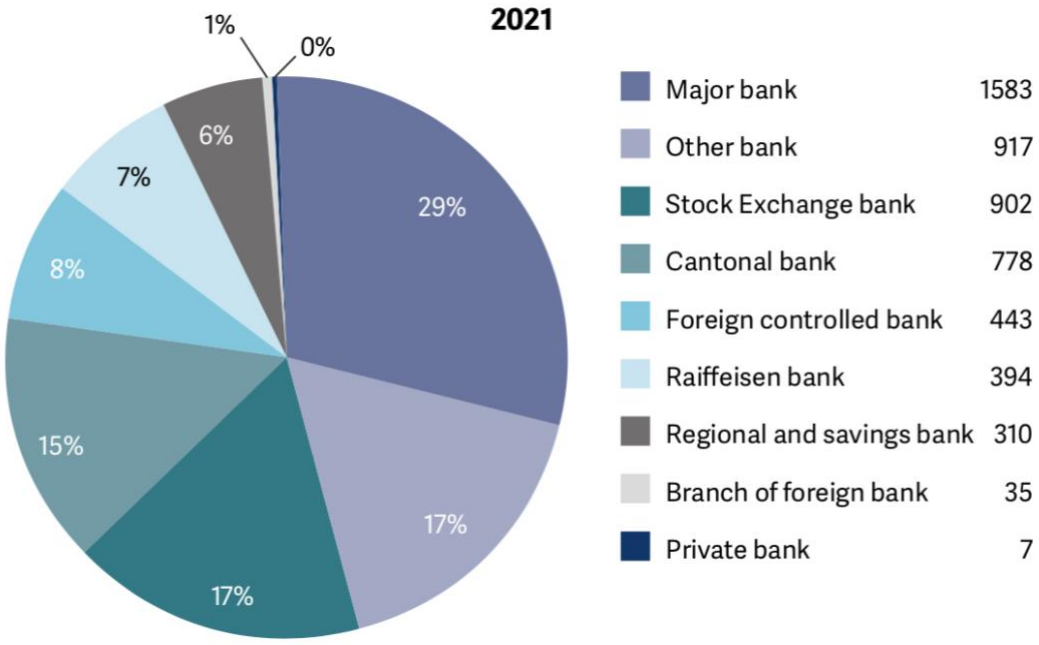
Furthermore, the United States is also a member of the Egmont Group 1995. (Egmont Group Website).

2.6 Reported suspicious cases in Switzerland and internationally

2.6.1 Switzerland

In 2021, a total of 5'964 reports were received by MROS, with 90% of them being reported by banks. Nearly one-third of these reports originated from major banks, including UBS and Credit Suisse (MROS Report 2021:18) (SBA Website). The second-largest share, accounting for 17%, was contributed by other banks. These banks do not fall into specific categories such as major banks, cantonal banks, stock exchange banks, regional banks and savings banks, Raiffeisen banks, or private banks, and they do not exhibit significant common characteristics (MROS Report 2021:18). (SBA Website).

Figure 1 - Number of SARs submitted to MROS in 2021 by type of bank

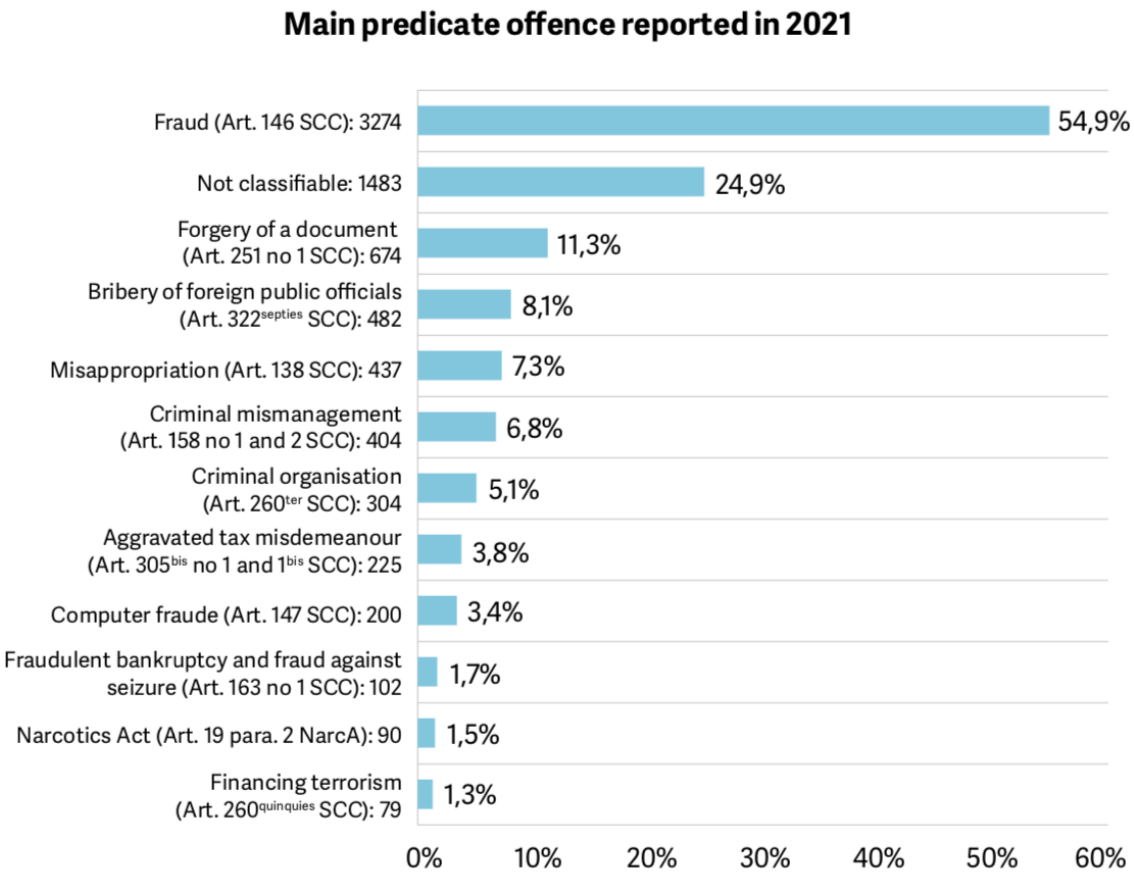


SOURCE: MROS Annual Report 2021 (2022, p. 18)

The most frequently reported predicate offense in the reported suspicion cases is fraud, accounting for 54.9% (MROS Report 2021:19), which is slightly lower than the previous year's percentage of 58% (MROS Report 2021:20). However, compared to 2019, when fraud constituted only 25% of the reported suspicions, it remains a consistently significant factor (MROS Report 2019:12). The MROS report describes that this high number of

fraud reports is only partially related, accounting for a total of 12%, to the granted COVID loans, where misappropriation and fraudulent misuse of loans from Swiss financial institutions with federal guarantees were suspected in connection with the Covid-19 pandemic. (MROS Report 2021:22). Whether other forms of fraud related to the COVID pandemic played a role in the increased percentage of fraud as a predicate offense has not been disclosed by the MROS.

Figure 2 - Main predicate offences suspected in the SARs submitted in 2021

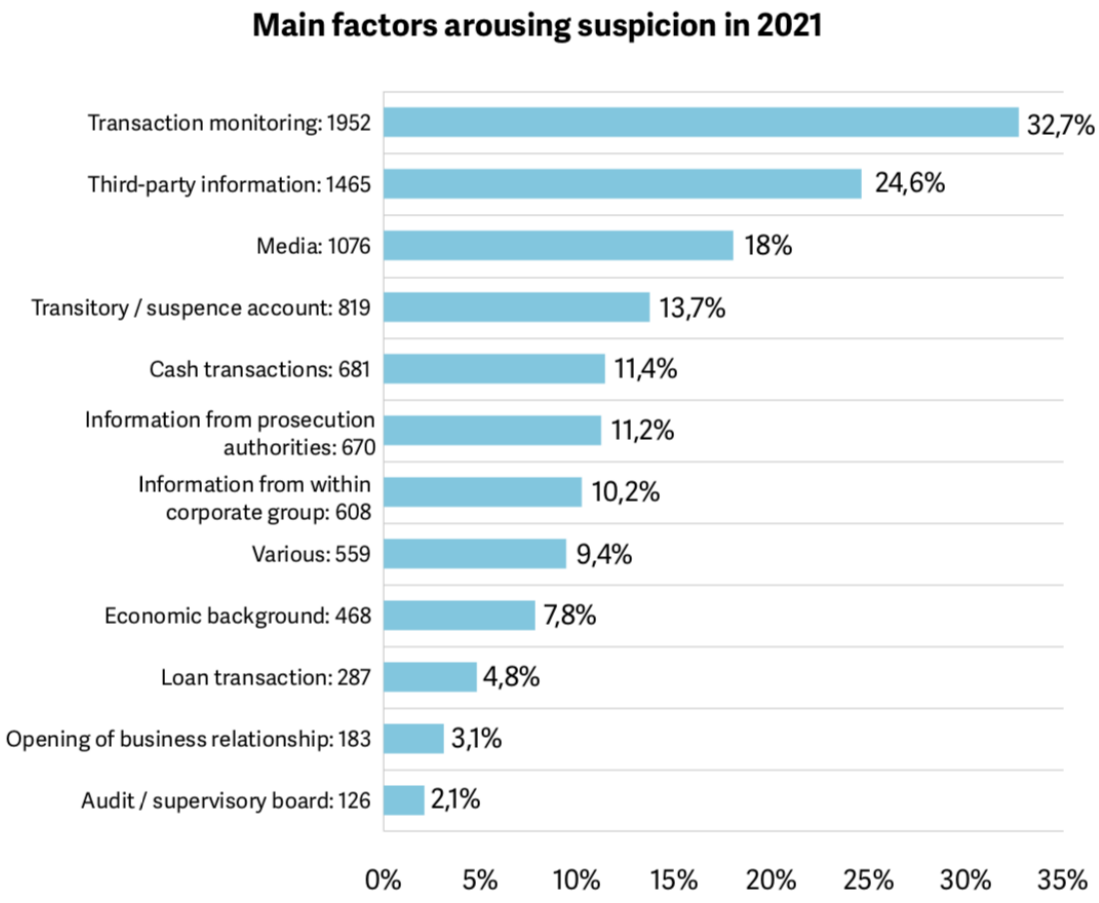


SOURCE: MROS Annual Report 2021 (2022, p. 19)

The methods through which financial intermediaries detect reported suspicions vary. The most significant trigger for suspicion in 2021 was transaction monitoring, accounting for 32.7% of the reported suspicions. (MROS Report 2021, 2022:20). In comparison to previous years, the trigger of suspicion from transaction monitoring was at 36.2% in 2020 and 31% in 2019. (MROS Report 2021, 2022:20). (MROS Report 2019, 2020:13). Since 2019, a change in the ranking of the most significant suspicion triggers can be observed. In 2019, media reports were the primary trigger for suspicion, which became the third most common reason in 2020 and 2021. Information from third parties was the third most common trigger for suspicion in 2019, but it became more frequent in the following two

years, landing it in second place. Information from third parties can include instances where victims report to financial intermediaries that they have made a transfer to a customer but did not receive the paid product or service. Another form of information from third parties can also occur when another bank recalls a transfer made by one of their customers, stating "fraud" as the reason.

Figure 3 - Main sources triggering suspicions in 2021



SOURCE: MROS Annual Report 2021 (2022, p. 20)

In 2021, the MROS received 304 suspicious activity reports (SAR) indicating a connection with a criminal organization. Fraud was the most common predicate offense mentioned in the suspicion reports, accounting for 37.8% of cases involving alleged links to a criminal organization. (MROS Report 2021, 2022:22). In comparison, fraud was the second most common predicate offense in 2020, accounting for 20.3%. (MROS Report 2020, 2021:22). According to Article 260ter of the SCC, a criminal organization is an organized group whose purpose is to commit violent crimes or to enrich themselves through criminal means, or to commit violent crimes with the intent to intimidate the population or to force a state or international organization to act or refrain from acting.

2.6.2 Germany

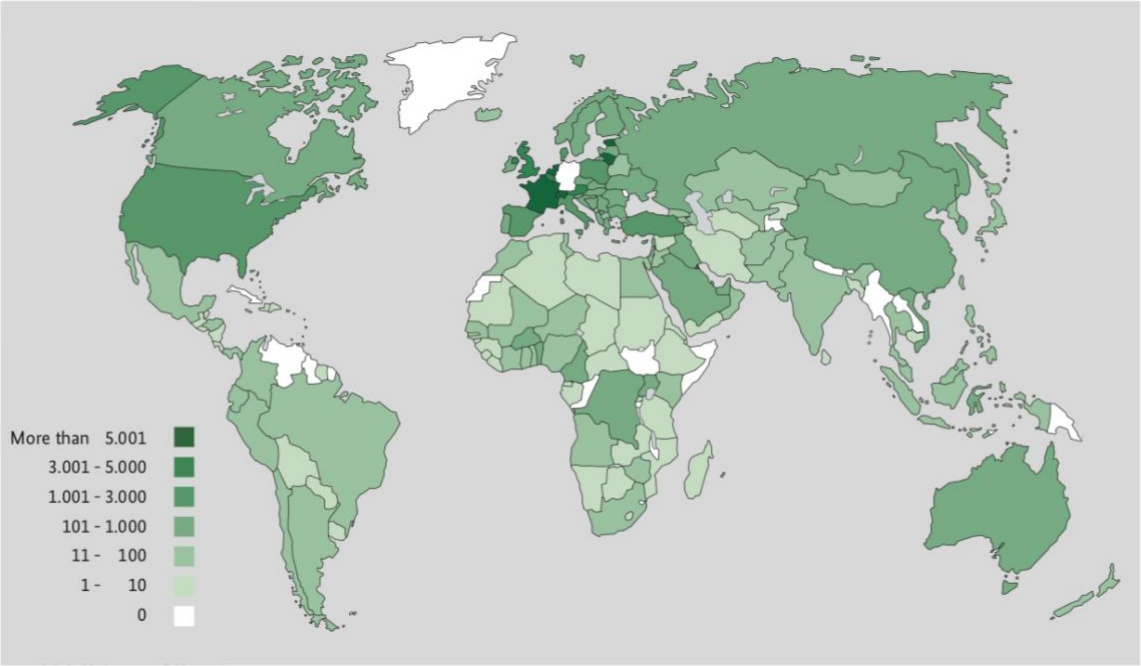
Internationally, an increase in reported suspicious cases can also be observed. However, this section serves as information about the international rise in money laundering and not as a comparison with Switzerland, as various elements such as different legal frameworks and reporting obligations in each country need to be considered.

According to the 2021 report of the FIU of Germany, a total of 298,507 reports were received, representing an increase of over 100% compared to the previous year. This increase can be attributed to various factors, including a new AMLA regulation regarding real estate matters and the development of cryptocurrencies (FIU Germany, Annual Report 2021, 2022:16). The financial sector plays a crucial role in combating money laundering, accounting for approximately 96.9% of all reported suspicions (FIU Germany, Annual Report 2021, 2022:17).

A significant number of reports received by the FIU, as also seen in Switzerland, involve suspicious transactions that play a crucial role in the detection and analysis of money laundering activities. These transactions include the transfer of assets between parties and often occur through banks or financial service providers. Typical examples of such transactions are bank transfers, cash withdrawals, and the transfer of cryptocurrencies between different electronic wallets. In 2021, the FIU declared having received approximately 958,000 suspicious transactions, nearly doubling compared to the previous year, which is in line with the increase in reports received.

An interesting change can be observed regarding domestic transactions within Germany. Their share of the total number of transactions increased to approximately 61% in 2021, compared to about half in the previous year. On the other hand, the proportion of transactions where Germany is listed only as the origin or destination country slightly decreased to around 31%. Particularly relevant for a national perspective are the flows of funds to and from Germany, illustrating the intensity of reported transactions involving Germany as the origin or destination country (FIU Germany Annual Report 2021, 2022:26).

Figure 4 - Number of suspicious transactions by country of origin submitted to the FIU Germany in 2021



SOURCE: FIU Germany Report 2021 (2022, p. 27)

In 2021, more than 104,000 suspicious transactions were reported to Germany, representing a 140% increase compared to the previous year. When examining the countries of origin for these transactions, the Netherlands stands out with over 28,000 transactions, followed by Switzerland with over 11,000 transactions, and France with over 9,200 transactions. (FIU Germany Annual Report 2021, 2022:27).

Based on the received suspicious cases, the FIU has established risk priorities, which are continuously reviewed and adjusted according to current developments and insights to ensure effective measures in combating money laundering and terrorism financing (FIU Germany, Annual Report 2021, 2022:30). One of the risk priorities under money laundering is, for example, organized fraud. Money laundering is often committed through organized fraud, particularly in the context of internet scams. Fraudsters exploit account opening procedures to operate fake online shops or redirect funds related to love scamming activities. Sometimes, the identity of other individuals is also abused to carry out these fraudulent acts. However, it is important to note that identity theft is not a mandatory criterion for organized fraud. The main objective is to repeatedly engage in fraudulent activities and generate a continuous source of income (FIU Germany, Annual Report 2021, 2022:31).

2.6.3 France

This section, like the previous two sections, does not serve as a direct comparison to Switzerland or Germany, but rather aims to illustrate the international trend.

Tracfin (Traitement du renseignement et action contre les circuits financiers clandestins) is the French FIU. It is a government agency responsible for receiving, analyzing, and disseminating financial information related to money laundering, terrorist financing, and other illegal financial activities. Tracfin operates under the supervision of the French Ministry of Finance, and its main objective is to contribute to the prevention and detection of financial crimes in France. (Tracfin Website).

In 2022, Tracfin published its annual report for the year 2021, revealing that it received a total of 160,952 SARs. This represents a 134% increase compared to the previous year. Of these reports, 95.4% were filed by financial intermediaries, with banks and credit institutions accounting for the largest share at 47.2%. (Tracfin, Annual Report 2021, 2022:106). Payment institutions, such as money transfer companies, also reported a significant increase, with 119% more SARs compared to the previous year.

The French National Agency for Fraud Prevention (ANR) recognizes fraud as a significant threat related to money laundering in France. The most common forms of fraud include false international transfer orders, fake investment scams, and fraud targeting local businesses. According to the Tracfin report, fraud cases reported in 2021 increased by 15% compared to the pre-COVID period. (Tracfin, Annual Report 2021, 2022:21). The proceeds from these frauds are laundered using various methods tailored to the amount of funds involved. Basic methods such as cash withdrawals, investments in savings accounts, and property purchases are supplemented by more complex networks that involve offshore e-money accounts or the gambling industry. (Tracfin, Annual Report 2021, 2022:22).

2.7 Cooperation between authorities, prosecution offices and banks in Switzerland

The collaboration between banks, prosecuting authorities, and MROS in Switzerland is of great importance in the fight against money laundering and other financial crimes. Banks have a legal obligation to report suspicious transactions and potential cases of money laundering to MROS. MROS collects and analyzes these reports and, if necessary, forwards them to the relevant prosecuting authorities. In 2021, MROS

submitted a total of 1,486 reports to prosecuting authorities, representing a 23% decrease compared to the previous year. (MROS, Annual Report 2021, 2022:24).

Prosecuting authorities play a central role in the criminal prosecution of money laundering and other financial crimes. They work closely with MROS to exchange information and insights. MROS supports prosecuting authorities in the investigation of cases and provides them with relevant financial information. Interestingly, the majority of MROS reports were once again directed to the cantons of Zurich, Vaud, and Geneva in 2021, indicating the influence of the financial sector and the presence of businesses in those areas. The OAG ranks fourth, primarily handling cases related to money laundering and foreign offenses. These cases are usually more complex and often involve information from various reports. (MROS, Annual Report 2021, 2022:24).

Because of the importance of these parties in combating economic crime, it is essential that they work well together. In the annual report 2022, the OAG highlighted the good cooperation between MROS and OAG. (OAG, Annual Report 2022, 2023:10).

3. Methodology

The main objective of this bachelor thesis is to develop approaches to help compliance departments of Swiss banks to mitigate the threats of emerging money laundering networks. To achieve this goal, a comprehensive approach was used to collect qualitative and quantitative data, including interviews and a survey.

The literature review provided interesting insights, but also led to some open questions that needed to be addressed as well as some knowledge gaps that needed to be filled. Therefore, three interviews were conducted. The first interview was conducted with a with a jurist who holds a doctorate in criminal procedure law and has extensive experience in compliance (hereinafter referred to as “Interviewee 1”). The purpose of this interview was to gain insight into the legal aspects and challenges of implementing anti-money laundering regulations. The second interview was conducted with Mr. Arnaud Beuret (hereinafter referred to as “Mr, Beuret”), owner of the law firm Advokatur Beuret, who previously worked for the FINMA and served as deputy head of the MROS. Thanks to his extensive and valuable experience, this interview provided important perspectives on the operational aspects of combating money laundering and the role of the supervisory authorities. In addition, an interview was conducted with the public prosecutor's office of the Canton of Aargau to gain insights from the perspective of the law enforcement authorities.

The goal of these interviews was to learn the interviewees' perspectives on the issue, to obtain their ideas for potential improvements, and to clarify any ambiguities that arose from the analysis.

To further deepen the investigation, a survey was conducted among five compliance officers working in various Swiss banks. The goal of this survey was to capture their experiences, challenges and best practices in implementing anti-money laundering measures.

Data was collected through face-to-face interviews that were recorded and transcribed to allow for comprehensive data analysis. An online form was created for the survey that allowed participants to anonymously complete their responses within minutes.

The transcribed interviews were analyzed, and all relevant information was extracted. Statistical analysis could be performed through the survey responses to better analyze the proportions and draw conclusions. The extracted interview and survey responses were considered in the "Results" and "Discussion" chapters.

4. Results

In accordance with the methodology described previously, three interviews and one survey were conducted in this study. The interviews were used to gain insights and opinions from subject matter experts, while the survey reflected the perspective of compliance officers on certain topics.

The results of this data collection are now detailed in this section. The information and insights from the interviews conducted were analyzed and processed to highlight key themes and trends.

4.1 Between regulation and efficiency: The impact of tighter anti-money laundering rules

The increasingly stringent regulations to combat money laundering pose significant challenges for banks in their implementation. Therefore, both interviewee 1 and Mr. Beuret were asked how the increasingly strict anti-money laundering regulations affect their implementation in banks.

As Mr. Beuret has experienced, this is an issue which is extensively discussed and considered both at the national and international levels. There is a general awareness that regulations in this area are necessary to protect financial markets from criminal activities. However, an excessive number of regulations can have counterproductive effects. Too many complex rules can impair the efficiency of banks and lead to increased administrative burden. As interviewee 1 also commented on this subject, compliance with these regulations requires substantial resources, such as the implementation of comprehensive compliance systems and training programs for employees.

The AMLA serves as a crucial legal framework governing the fight against money laundering in Switzerland. However, it is recognized that the AMLA is highly formalized, and the laws are sometimes broadly formulated. As Mr. Beuret also came to realise due to the events of the last few years, specific benchmarks and standards are often set retrospectively. This often occurs in response to exposed scandals, such as those involving corruption, as seen in cases like Petrobras or 1MDB. Due to this uncertain and ever-changing regulatory landscape, many banks are therefore increasingly adopting self-regulatory measures. They establish their own guidelines and procedures to minimize risks associated with money laundering and financial crime. A prime example of this is the regular review of High Risk Relation (HRR) and PEP customers, for which the law does not specify a precise periodicity. Banks make decisions based on their

individual risk appetite and available resources regarding the frequency and scope of these reviews.

According to the interviewee 1, however, the stricter regulations in the field of KYC practices did not necessary aggravate the implementation but have resulted in higher costs. Banks are now compelled to invest more in verifying and documenting customer information. This includes verifying identity documentation and analyzing customer profiles to detect and report suspicious activities.

The new regulations in reporting have actually simplified the implementation for banks as per the experience of the interviewee 1, as the MROS now treats the right to report (art. 305ter para. 2 SCC) and the duty to report (art. 9 AMLA) in a more consistent manner. Although banks had to make investments in this area, such as implementing goAML[9], ultimately, after successful implementation, it brings them certain added value.

4.2 Risk prevention measures

In the two interviews with the interviewee 1 and the Mr. Beuret, the question of how financial institutions can reconcile the need for anti-money laundering compliance with their obligation to provide financial services to their customers was discussed. The two interviewees showed similar views on this issue.

The interviewee 1 emphasized that the point is not to put obstacles in the way of banks. Ultimately, it is up to the financial institutions themselves to decide what risk they want to take, both in the short term and in the long term. This means that banks have a responsibility to assess their own risk appetite and take appropriate action to minimize risk. It is important that banks recognize that they need to act and comply in a way that balances the associated effort and return.

Mr. Beuret shared similar views and pointed out that the risk appetite of individual members of executive management also plays an important role. It depends on whether some executives are willing to take high risks to achieve short-term gains, even if they leave the company in a few years and those decisions may then have long-term consequences. However, it is already an important step that banks recognize that they need to take action and comply with regulations in a way that is worth the effort and return so at a certain point the company also self-regulates.

[9] goAML is a fully integrated software solution developed specifically for the work of FIUs and which, among others, banks use for the transmission of SARs. (FEDPOL, goAML Manual, 2022:7).

Furthermore, if a bank recognizes, for example, that its situation requires it to take more risks in order to survive, it is important that it simultaneously take the necessary measures to mitigate those risks, which, on the other hand, requires the necessary resources.

Overall, it's about striking a balance. Financial institutions need to assess their individual risk appetite while ensuring that they take the necessary steps to ensure compliance with anti-money laundering regulations. Through effective self-regulation and the implementation of appropriate risk management measures, financial institutions can meet their obligations to their customers while minimizing the risks associated with money laundering.

According to the Mr. Beuret, however, there is no miracle cure for protecting against the risks of organized money laundering networks. However, by taking a serious look at the Criminal Code and the AMLA and drawing up a clear internal risk policy, businesses should be able to find a way.

Which measures should be used and how to achieve this is discussed below:

4.2.1 Recognizing patterns in the transactional analysis

Over the past two years, transaction monitoring has been the most common trigger for reporting suspicious activities to the MROS. In light of this, the interviewee 1 and Mr. Beuret were asked whether banks can pay attention to patterns in transaction monitoring to detect money laundering and fraud. The results of the interviews provided interesting insights into this topic.

The interviewee 1 emphasized that it is possible to detect patterns in many cases, especially in fraud cases such as investment fraud. Furthermore, it is important to draw conclusions from existing cases and adjust transaction monitoring accordingly. However, there is also the challenge that many patterns cannot be effectively detected with electronic transaction monitoring. This could lead to a large number of false positive alerts[10]. This would make the work more difficult and require significant resources.

Using artificial intelligence (AI) could be an effective way to make transaction analysis more efficient. This emerging technology could help banks identify abnormalities outside of internal benchmark boundaries.

[10] False positive alerts are when the system classifies transactions as suspicious when they are actually legitimate. (Flagright, 2022).

Mr. Beuret emphasized that the fine-tuning of amounts in transactional analysis is only effective when it is tailored to the relevant business relationship. Business relationships can be broken down into segments, with more focus on those segments that are at higher risk of, for example, fraud. Like the interviewee 1, Mr. Beuret also mentioned the use of AI to detect deviations from internal benchmarks. In some countries, such as Austria, this is already enshrined in law and financial intermediaries can use this technology to efficiently analyze these abnormalities and deepen their benchmarks. In Switzerland, there are currently no specific legal requirements for the use of AI in banks. Banks are required to conduct clarifications in case of suspicion, but the concrete procedure is up to their discretion. However, it cannot be ruled out that regulations relating to the use of AI will follow in the future.

4.2.2 Detect fraudulent accounts by means of system optimization

The detection of fraudulent accounts is not limited to transactions alone. Already during the account opening process, indications can point to fraud or money laundering, such as forged identity cards. According to the interviewee 1, neo-banks are particularly affected by this issue due to their simplified online account opening processes. This simplification allows fraudsters to open accounts quickly and with sophisticated methods. According to her, however, already the recognition of this systematic approach by banks and the resulting measures are an important step. To prevent such fraud, it is necessary to have technical safeguards in place. Tighter KYC measures could also contribute to an improvement. However, the interviews also showed that fraudsters continuously find new ways to circumvent security measures and are often technically one step ahead, as mentioned by the public prosecutor's office in Aargau.

It is important that banks recognize that these fraudulent practices are not isolated individual cases, but represent a systematic approach. By implementing effective security measures and continuously adapting to evolving fraud methods, banks can strengthen their countermeasure strategies.

In the conducted survey, 60% of the respondents indicated that they perceive their employer's current fraud detection system as either inefficient. Furthermore, when asked if they believe their employer's system could be enhanced to detect fraud more effectively, 3 out of 5 respondents answered with yes, expressing their belief in the potential for improvement.

4.2.3 Improved protection through employee training

In order to effectively detect and prevent fraud, it is essential to train employees on a regular basis. This finding was clearly emphasized in both interviews with the interviewee 1 and Mr. Beuret and underscores the importance of fraud detection training.

Training provides employees with the knowledge and awareness necessary to recognize potential fraud indicators, such as fake identity cards or suspicious transactions. By understanding common fraud methods and techniques, employees can identify early warning signs and take appropriate action to minimize potential harm.

In the survey conducted, it was notable that 60% of respondents indicated that they had not received sufficient training from their employers to detect and prevent fraudulent activity through ongoing training programs or prevention techniques. This indicates a potential gap in companies' efforts to equip their employees with the knowledge and skills necessary to effectively combat fraud.

In addition, 4 out of 5 compliance officers expressed a desire for more training by their employer to improve their understanding of money laundering issues. These survey results highlight the importance of ongoing education and training in fraud prevention and detection, as also indicated by the people interviewed.

4.2.4 Public awareness

It is of huge importance to inform the public about fraud and money laundering, as also illustrated by the response of the public prosecutor's office in Aargau. A large number of people repeatedly fall for fraud schemes and subsequently file charges, resulting in a considerable amount of work for law enforcement agencies. In recent years, the number of criminal investigations at the Aargau public prosecutor's office has even doubled.

Although the public prosecutor's office itself is less directly involved, as preventive measures fall under the jurisdiction of the police, the need for comprehensive education on these issues is emphasized. Prevention in these areas is being continuously expanded, especially due to the increasing threat to older people who have not grown up with the Internet.

The public prosecutor's office faces challenges in sharing information with the media, as it is not subject to the Principle of Publicity but to the Code of Criminal Procedure, and criminal proceedings are basically secret. The prosecutor's office strives for transparency, but it faces the issue that it is not able to provide the media with a concrete story when it asks for coverage of its work and to clarify the dangers to people.

Educating the public widely about fraud can not only better protect potential victims, but also reduce the workload for law enforcements and banks. By being better informed and detecting fraudulent activity early, people can help reduce the number of crimes committed and thus the number of criminal investigations that need to be conducted.

4.3 Successful cooperation and obstacles between MROS, public prosecutors' offices and banks

As also described in the literature review, cooperation between MROS, prosecutors and banks play a crucial role in combating money laundering. However, based on the responses from the interviews, a mixed picture emerges about the efficiency and effectiveness of this cooperation.

According to the interviewee 1, cooperation in complex cases often turns out to be inefficient. The reports forwarded by MROS do not seem to offer any added value to the prosecution offices according to her experience. This suggests that improvements may be needed in the way information is transmitted and used. However, considering less complex cases like simple fraud cases, the parties seem to have found an efficient solution and the cooperation is going well.

Mr. Beuret, on the other hand, describes cooperation as largely linear as long as banks make the required reports. However, inconsistencies occasionally occur when not all relevant information is reported by banks. Another obstacle is that there is a lack of exchange between the 27 prosecutors' offices due to federal structures. The interviewee 1 confirmed this finding and mentioned that the exchange of information between prosecutors' offices may only occurs when there are personal relationships with individual prosecutors.

On the other hand, the public prosecutor's office of Aargau emphasizes the good cooperation with MROS, which is described as efficient and smooth. However, there is a challenge to improve the cooperation with the banks in some cases to enable a more efficient operation.

These different perspectives indicate that there is room for improvement and greater collaboration between the parties involved. Better coordination and communication between MROS, prosecutors, and banks could help increase the efficiency of cooperation and improve information sharing.

5. Analysis

5.1 Current situation

Based on the literature review, interviews conducted, and the survey results, important insights derived for analysis.

An increase in fraudulent activities has been observed in Switzerland, as described in the literature review. This observation was further confirmed through interviews with the Aargau prosecution office, which mentioned that the overall number of cases has doubled.

The monitoring of transactions was identified as a key factor for detecting such activities, as highlighted in the previous annual reports of the MROS. In this regard, it was recommended in the interviews that banks should leverage emerging technologies such as AI. By analyzing previously detected fraud cases, conclusions can be drawn and patterns can be established, which AI systems can then analyze within a high volume of transactions. Mr. Beuret supported this recommendation and emphasized during the interview the effectiveness of breaking the business relationships down to segments, in order to better tailor the transactional monitoring.

It should be noted that not only the use of AI is suitable for this purpose, but also collaboration with data analytics and analysis companies can be helpful in obtaining effective insights from transactions.

Another important aspect that emerged from the literature review is that of the reported transactions to the FIU Germany, the second most transactions originated from Switzerland. Enhanced international cooperation could help improve information exchange with other countries, enabling better detection and combatting of fraud schemes, as mentioned by the public prosecutor's office of the Canton of Aargau. However, it was also emphasized that strengthened national collaboration among banks, MROS, and prosecution offices is crucial to better understand the tactics of organized money launderers and implement effective countermeasures.

The results of the interviews and the survey also highlight the high relevance of employee training in banks. It was found that there is still a significant need for improvement in this area. To effectively combat fraud and money laundering, it is crucial to raise employees' awareness of these issues and enhance their skills in dealing with suspicious incidents. Targeted trainings can better sensitize employees and provide support in recognizing and reporting fraudulent cases.

The current situation regarding public awareness of fraud and money laundering is of great importance. There has been a noticeable increase in the number of people falling victim to fraud, resulting in a significant workload not only for law enforcement agencies, but also for MROS and for banks.

While the prosecution is primarily involved in criminal prosecution, the need for comprehensive intelligence and prevention in these areas is emphasized. The responsibility for preventive measures lies primarily with the police. But also banks can have an important role to play in raising public awareness by informing their customers about current fraud schemes. Several banks already educate their customers via their website on these topics. UBS, for example, has published a report on investment fraud on its website, which provides valuable information for its clients. Similarly, Credit Suisse has also provided information on its website about the different typologies of fraud and gives its clients practical tips on how to protect themselves from these threats.

It is important that banks provide such information on their websites, as it gives their customers the opportunity to learn about these important issues and it also increases public awareness. However, these websites and documents are usually overlooked by customers unless they specifically search for them. Therefore, banks could take an even more active role in educating their customers about the risks of fraud.

5.2 Recommendations

Based on the insights from the analysis, the following recommendations for banks derived:

Employee Training

Targeted training for employees is of great importance to raise awareness of fraud and money laundering, and to enhance their skills in detecting suspicious transactions and activities. Banks should ensure that their employees receive regular training and have up-to-date knowledge of fraud practices and prevention measures.

Rising awareness

Prevention measures such as educating customers about current fraud schemes can serve to increase general public awareness and, among other things, reduce the number of money mules, which is also in the interest of banks. As an example, banks can send regular email updates to their customers informing them about current fraud schemes and giving them advice on how to protect themselves. In addition, they could add alerts

about this topic on their e-banking platforms. This way, customers can see the information directly, without having to look for it explicitly on the website.

Implementation of Segmentation

It is recommended to utilize segmentation techniques to analyze transactions and patterns more accurately. By breaking the business relationship down into segments and focusing on those segments that present a higher risk of fraud, banks can identify specific fraud patterns more effectively and take appropriate countermeasures.

Adoption of Artificial Intelligence

Banks should increasingly leverage AI technologies to enhance transaction monitoring and identify suspicious patterns more efficiently. By analyzing previously detected fraud cases, AI systems can gain valuable insights and help detect new fraud attempts at an early stage.

Collaboration with Technology Companies

Collaborating with companies specializing in data analytics and data analysis can provide insights on transactional patterns and serve as a preventive measure.

Ongoing Review and Adaptation of Policies

Given the constantly evolving fraud methods and regulatory requirements, banks should regularly review and adapt their internal policies and procedures. It is important to remain flexible and adapt to current challenges.

Enhanced Collaboration

It is recommended to strengthen collaboration and information sharing of banks with the prosecution offices and the MROS. By enhancing information exchange and jointly combating fraud schemes, more effective approaches can be developed.

6. Conclusion

In conclusion we can say that banks have a range of strategies at their disposal to detect and prevent money laundering stemming from fraudulent activities, enabling them to more effectively identify fraudsters and money mules. By implementing these recommendations, banks can strengthen their efforts in combating fraud, protecting their customers, and safeguarding the integrity of the financial system.

However, it is important to clarify that the mentioned proposals should be seen as complementary to each other rather than individual solutions. For instance, relying solely on AI-based methods may be less effective since fraudsters themselves employ AI for their activities. However, in conjunction with customer awareness initiatives and efficient employee training, AI can serve as an effective ally in combating fraudulent activities.

The analysis of MROS annual reports spanning the years 2019 to 2021 formed a key part of this research. Notably, just prior to the submission of this study, MROS published its 2022 annual report, which identified a rise in fraud as a predicate offense for money laundering, reaching 56% (MROS, Annual Report 2022, 2023:25). To provide context, the figure stood at 54.9% in 2021. This continued increase in money laundering through fraudulent activity underscores the need for robust detection and prevention measures in banks.

The implementation of the various measures may not only mean a reduction in the number of cases to be processed on the part of the banks, but may also benefit the MROS, which continues to be heavily overburdened. An interview with the MROS was requested to gain insights into various topics such as the current situation and their cooperation with banks, however, due to time constraints of the MROS, the interview had to be cancelled. By and large, the whole system would benefit accordingly, but most importantly, it would protect the citizens and our economy from the financial risks of such rising threats.

Drawing from personal experience as a compliance officer within a bank, I can confidently assert that the recommendations derived from this study will undoubtedly contribute to enhancing the efficacy of compliance departments and fortifying them against AML risks.

Bibliography

BUNDESGESETZ ÜBER DIE DIREKTE BUNDESSTEUER (DBG) of 14 December 1990.

BÜRGI NÄGELI RECHTSANWÄLTE, *LAWINFO - Geldwäscherei / Geldwäschereigesetz - Geldwäschereigesetz und Abgrenzungen,* 2012, update 2022, https://law.ch/lawinfo/geldwaescherei-geldwaeschereigesetz/geldwaschereigesetz-und-abgrenzungen/.

BÜRGI NÄGELI RECHTSANWÄLTE, *LAWINFO - Geldwäscherei / Geldwäschereigesetz - GwG - Gegenstand, Ziel / Zweck,* 2012, update 2022, https://law.ch/lawinfo/geldwaescherei-geldwaeschereigesetz/gwg-gegenstand-ziel-zweck/.

CONSUMER ADVICE, FEDERAL TRADE COMMISSION, *How to Recognize and Avoid Phishing Scams*, 2019, https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

CONSUMER ADVICE, FEDERAL TRADE COMMISSION, *What to Know About Romance Scams*, 2019, https://consumer.ftc.gov/articles/what-know-about-romance-scams.

CREDIT SUISSE SWITZERLAND, *Internet Security*, https://www.credit-suisse.com/ch/en/legal/internet-security.html

DAS PARLAMENT, *Risikoanalysen zu Korruption und Terrorismusfinanzierung. Welche Folgen?*, 2016, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161080#:~:text=Die%20interdepartementale%20Koordinationsgruppe%20zur%20Bek%C3%A4mpfung,Bundesrat%20Ende%202013%20eingesetzt%20wurde.

DELOITTE SWITZERLAND, *Impact of COVID-19 on Cybersecurity*, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html.

DELOITTE UNITED KINGDOM, *The 5th Anti-Money Laundering Directive*, 2018, https://www2.deloitte.com/uk/en/pages/financial-services/articles/fifth-anti-money-laundering-directive.html.

DER SPIEGEL, *Fahnder zerschlagen europäisches Netzwerk von Anlagebetrügern*, 2020, https://www.spiegel.de/wirtschaft/soziales/anlagebetrug-fahnder-zerschlagen-europaeisches-netzwerk-a-314dec3e-a823-46c8-88a1-efa89d1a239a.

EGMONT GROUP, *Members by Region*, https://egmontgroup.org/members-by-region/.

EUR-Lex, *Preventing abuse of the financial system for money laundering and terrorism purposes*, 2021, https://eur-lex.europa.eu/EN/legal-content/summary/preventing-abuse-of-the-financial-system-for-money-laundering-and-terrorism-purposes.html.

EUROPEAN BANKING AUTHORITY, *Anti-Money Laundering and Countering the Financing of Terrorism*, https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-countering-financing-terrorism.

EUROPEAN BANKING AUTHORITY, *The European Banking Authority at a glance*, 2016.

FATF, *Professional Money Laundering*, FATF Report, 2018.

FATF-GAFI, *Assessment of Member States Compliance with FATF Recommendations and Strategy on Combatting Terrorist Financing*, 2018, https://www.fatf-gafi.org/en/publications/Fatfgeneral/Speech-special-committee-terrorism-may-2018.html.

FATF-GAFI, *Cyprus' Progress in Strengthening Measures to Tackle Money Laundering and Terrorist Financing*, 2022, https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fur-cyprus-2022.html.

FATF-GAFI, *United States' Measures to Combat Money Laundering and Terrorist Financing*, 2016, https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-united-states-2016.html.

FATF-GAFI, *Who We Are*, https://www.fatf-gafi.org/en/the-fatf/who-we-are.html.

FCA, *Armchair Detective Investors Take Inspiration from Sherlock Holmes to Foil Investment Scams*, 2023, https://www.fca.org.uk/news/press-releases/armchair-detective-investors-take-inspiration-sherlock-holmes-foil-investment-scams.

FDF, Federal Department of Finance. *Tasks*. https://www.efd.admin.ch/efd/en/home/das-efd/aufgaben-ziele.html

FEDERAL ACT ON COMBATING MONEY LAUNDERING AND TERRORIST FINANCING (AMLA) of 10 October 1997.

FEDERAL ACT ON UNFAIR COMPETITION (UCA) of 19 December 1986.

FEDERAL TRADE COMMISSION, *Reports of Romance Scams Hit Record Highs in 2021*, 2022, https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/02/reports-romance-scams-hit-record-highs-2021.

FEDERAL OFFICE OF JUSTICE, *Publication about the Federal Office of Justice*, 2010

FEDPOL, *Money Laundering Reporting Office Switzerland (MROS),* https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/geldwaescherei.html.

FEDPOL, *Tasks at Federal Level*, https://www.fedpol.admin.ch/fedpol/en/home/polizei-zusammenarbeit/national/polizeiarbeit_auf.html.

FEDPOL, MROS Annual Report 2019, 2020.

FEDPOL, MROS Annual Report 2020, 2021.

FEDPOL, MROS Annual Report 2021, 2022.

FEDPOL, MROS Annual Report 2021, 2022.

FEDPOL, MROS, goAML Web – Manual, 2022.

FINCEN, *USA PATRIOT Act*, https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act.

FINMA, *FINMA - an Independent Supervisory Authority*, https://www.finma.ch/en/finma/finma-an-overview/.

FINMA, *How investors can protect themselves against unauthorized financial market providers*, 2021.

FINMA, *Legal Basis for Combating Money Laundering*, https://www.finma.ch/en/documentation/legal-basis/laws-and-ordinances/anti-money-laundering-act-(amla)/.

FLAGRIGHT, *Understanding False Positives in Transaction Monitoring*, https://blog.flagright.com/understanding-false-positives-in-transaction-monitoring.

HYPOTHEKARBANK LENZBURG, *Money-Mule-Fälle haben deutlich zugenommen*, https://www.hbl.ch/de/ueber-uns/medien-news/blog/blogeintraege/2021/interview-bernhard-droz/.

INTERNATIONALE RECHTSHILFE, *Liste der kantonalen Zentralbehörden für die Rechtshilfe in Strafsachen,* https://www.rhf.admin.ch/rhf/de/home/strafrecht/behoerden/zentralbehoerden.html.

KANTONSPOLIZEI ZÜRICH, *Cybercrimepolice - Warnung vor Tryapp.de - Betrüger versuchen Nutzer zur Eröffnung von Bankkonten zu verleiten*, https://www.cybercrimepolice.ch/de/fall/warnung-vor-tryappde-betrueger-versuchen-nutzer-zur-eroeffnung-von-bankkonten-zu-verleiten/.

KANTONSPOLIZEI FRIBOURG, *Cyberkriminalität - Money muling*, https://www.fr.ch/de/polizei-und-sicherheit/praevention/cyberkriminalitaet/cyberkriminalitaet-money-muling.

LENZ & STAEHLIN, *Revision des Schweizerischen Strafgesetzbuches und des Geldwäschereigesetzes – Einführung qualifizierter Steuervergehen als Vortat zur Geldwäscherei und weitere Änderungen*, 2015.

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE, TRACFIN, *Operations and Analysis Report*, 2022.

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE, TRACFIN, *Website*, 2022, https://www.economie.gouv.fr/tracfin.

NATIONAL CYBER SECURITY CENTRE (NCSC), Semi-Annual Report 2021/2, 2022.

NATIONAL CYBER SECURITY CENTRE (NCSC), Semi-Annual Report 2022/1, 2022.

NATIONAL CYBER SECURITY CENTRE (NCSC), Semi-Annual Report 2022/2, 2023.

NEUE ZÜRCHER ZEITUNG NZZ, *200 Festnahmen bei Aktion gegen Geldwäscherei*, 2019, https://www.nzz.ch/schweiz/200-festnahmen-bei-aktion-gegen-geldwaescherei-ld

OFFICE OF THE ATTORNEY GENERAL, *Homepage*, https://www.bundesanwaltschaft.ch/mpc/en/home.html.

OFFICE OF THE ATTORNEY GENERAL. *Organisation*. https://www.bundesanwaltschaft.ch/mpc/en/home/die-bundesanwaltschaft/organisation.html.

PRICEWATERHOUSECOOPERS. *PwC's Global Economic Crime and Fraud Survey 2022*, 2022

SCHWEIZER RADIO UND FERNSEHEN (SRF), *Anstieg von Cybercrime-Fällen - Anlagebetrüger zocken immer mehr Schweizer ab*, 2020,

https://www.srf.ch/news/schweiz/anstieg-von-cybercrime-faellen-anlagebetrueger-zocken-immer-mehr-schweizer-ab.

STAATSANWALTSCHAFT BASEL-STADT, *Willkommen bei der Staatsanwaltschaft,* https://www.stawa.bs.ch/.

STADT ZÜRICH, *Anlagebetrug*, https://www.stadt-zuerich.ch/pd/de/index/stadtpolizei_zuerich/praevention/Blog/alle/anlagebetrug.html.

SUMSUBER, *Anti-Money Laundering Laws 2023 in the US - Requirements and Penalties*, https://sumsub.com/blog/aml-guide-usa/.

SWISS BANKERS ASSOCIATION, *Combating Money Laundering*, https://www.swissbanking.ch/en/topics/regulation-and-compliance/the-fight-against-money-laundering.

SWISS BANKERS ASSOCIATION, *Financial Centre Participants*, https://www.swissbanking.ch/en/financial-centre/financial-centre-participants.

SWISS CRIME PREVENTION, *Romance Scam*, https://www.skppsc.ch/de/themen/internet/romance-scam/.

SWISS CRIME PREVENTION, *Schwerpunkt Betrug*, https://www.skppsc.ch/de/schwerpunkt/betrug-betrug/.

SWISS CRIME PREVENTION, *Phishing - How to protect yourself against phishing attacks*, 2022.

SWISS CRIMINAL CODE of 21 December 1937.

TESSIAN, *Why We Click on Phishing Scams - How to Avoid Being Hacked*, 2020, https://www.tessian.com/blog/why-we-click-on-phishing-scams/.

THE ECONOMIST INTELLIGENCE UNIT, *Tackling Illicit Trade, Deliver Change - PMI*, https://impact.economist.com/projects/deliver-change/article/tackling-illicit-trade/.

TRIBUNAL PENAL FEDERAL, *Overview*, https://www.bstger.ch/en/il-tribunale/il-tribunale-penale-federale-in-breve.html.

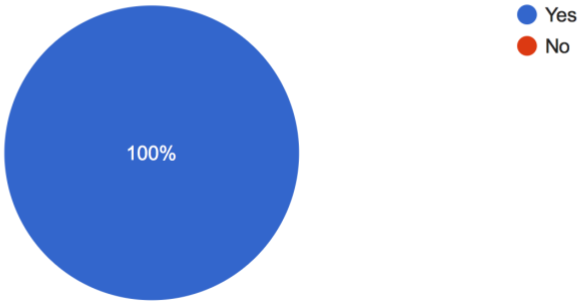
UBS SWITZERLAND, *Promises of Dream Returns? Beware*!, https://www.ubs.com/ch/en/private/accounts-and-cards/information/magazine/2023/cyber-investment-fraud.html.

VENKATARAMAKRISHNAN, SIDDHARTH, *Investment Scam Reports Rise by 193% in Five Years*, Financial Times, 2023.

Appendix 1: Survey results

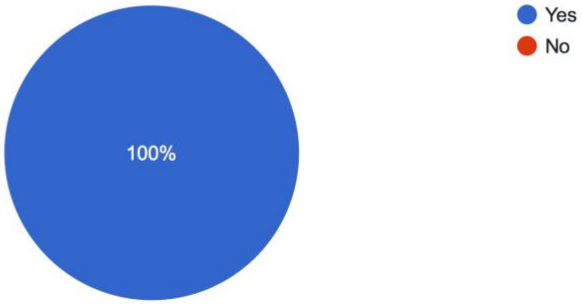
Do you work in a bank or another financial institution based in Switzerland?

5 responses



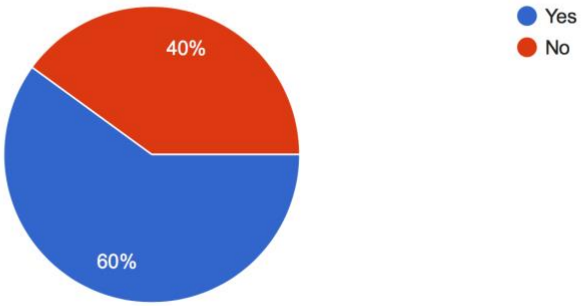
Are you currently working in compliance or in a compliance related job?

5 responses



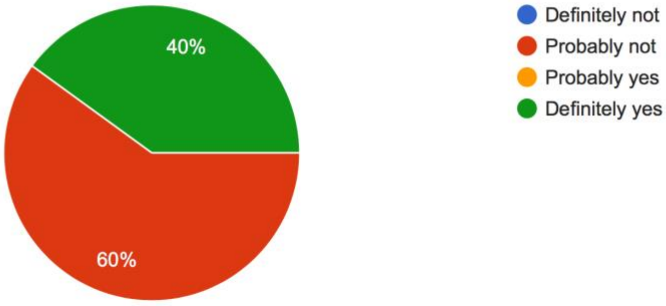
During your employment, has a fraud case of a client ever been discovered?

5 responses



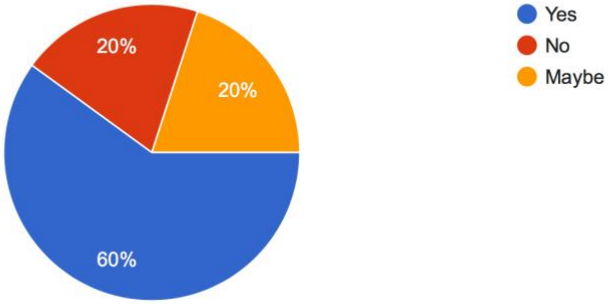
Do you think that the current fraud detection system of your employer is efficient?

5 responses



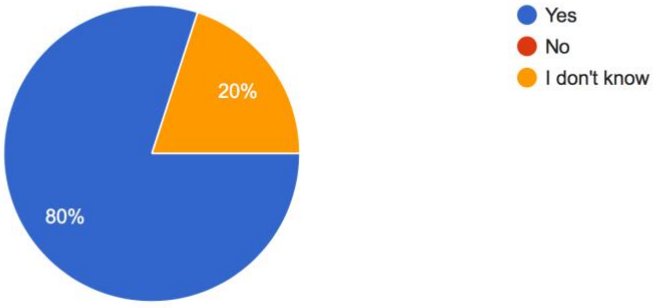
Do you think your employer's system could be improved to detect fraud more efficiently?

5 responses



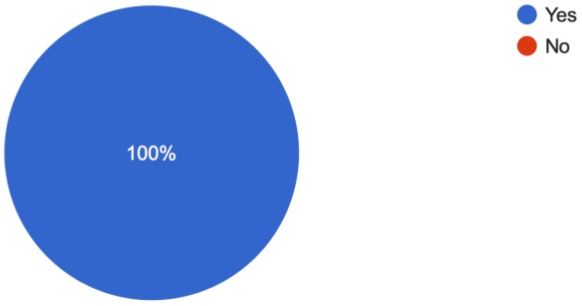
Is your employer already taking steps to improve the system?

5 responses



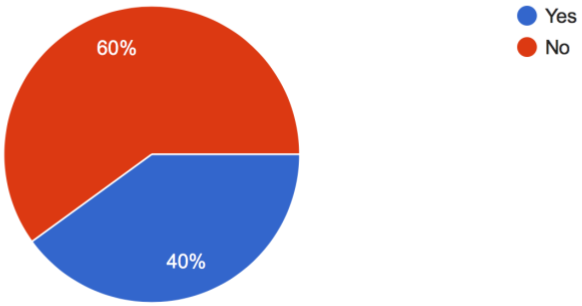
Do you have a team dedicated to handling cases related to money laundering?

5 responses



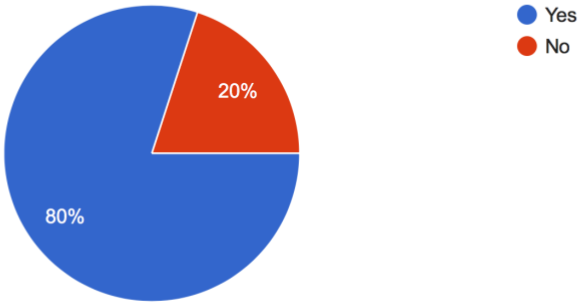
Are you trained by your employer to detect and prevent fraudulent activities through ongoing training programs or prevention techniques?

5 responses



Would you like your employer to provide you with more training to help you better understand cases of money laundering?

5 responses



Appendix 2: Interview 1

Inwieweit erschweren die immer strenger werdenden Vorschriften zur Bekämpfung der Geldwäscherei den Banken deren Umsetzung?

Ich denke, es kommt darauf an, um welches Thema es sich handelt. Insgesamt denke ich, gerade im Bereich der Identifizierung, der Feststellung des wirtschaftlichen Berechtigten und der KYC (Know Your Customer)-Revisionen, wird es zwar nicht schwieriger, es erfordert aber sicherlich mehr Ressourcen. Das ist bei jeder neuen Verpflichtung normal. Man muss neue Prozesse etablieren, Tools analysieren und implementieren. Das erfordert Ressourcen und kostet Geld.

Im Bereich des Meldewesens habe ich das Gefühl, dass es sich möglicherweise etwas vereinfacht hat, indem das Melderecht und die Meldepflicht nun mehr oder weniger gleich behandelt werden. Ich denke, am Ende wird es etwa im Gleichgewicht sein.

Was das Thema goAML betrifft: Ich denke, die gesamte Umsetzung war in den letzten Jahren für bestimmte Institute sehr teuer, aber ich gehe davon aus - ich kenne die genauen Zahlen nicht -, dass jene, die es nun einmal implementiert haben, auch einen gewissen Mehrwert daraus ziehen.

Wie können sich Banken besser gegen die Risiken von organisierten Geldwäschenetzwerken schützen?

Wahrscheinlich bin ich nicht ganz die richtige Person, um diese Frage zu beantworten. Jedoch weiss ich aufgrund meiner Kunden, die genau dieses Problem haben, dass die ganzen Neo-Banken mit ihren Video- und Online-Identifizierungsprozessen mit diesem Problem zu kämpfen haben. Sie haben so viele Fälle von Money Mules wie noch nie zuvor. Ich habe das Gefühl, dass es durch die technischen Möglichkeiten einfacher geworden ist. Man muss nicht mehr zum Schalter gehen und sich den Fragen der Bankangestellten aussetzen und ihnen ins Gesicht lügen. Das erleichtert es als Money Mule, ein Konto zu eröffnen. Ich denke, es wäre wichtig, sich hier technisch zu schützen, aber ich wüsste nicht genau, wie das gemacht werden könnte.

Wie wirksam ist Ihrer Meinung nach das derzeitige Meldesystem bei der Bekämpfung der Geldwäscherei?

Was ich auch von den Staatsanwälten höre, ist, dass es in diesem Bereich von kleinen, nicht komplexen Fällen offenbar gut mit der Zusammenarbeit läuft und es scheint, dass sie dafür einen Weg gefunden haben. Diese Art von Fällen wird relativ unbürokratisch gemeldet und danach auch relativ unbürokratisch weitergeleitet. Die Staatsanwälte

wissen aufgrund ihrer Erfahrung, wie sie dabei vorgehen müssen, da sie es schon unzählige Male gemacht haben. Daher habe ich das Gefühl, dass die Zusammenarbeit, wenn sie irgendwo funktioniert, genau in diesen Fällen gut läuft. Ich habe eher das Gefühl, dass bei den komplexen Fällen die Effizienz nicht sehr hoch ist.

Sind Sie der Meinung, dass die Zusammenarbeit zwischen der MROS, den Banken und den Staatsanwaltschaften effizienter gestaltet werden könnte, um Geldwäscher oder Geldwäschenetzwerke besser bekämpfen zu können?

Ich denke, dass es in den komplexen Fällen nicht sehr effizient ist. Ich habe Einblick in alle drei Bereiche und sehe, dass Banken derzeit extrem viel melden. Die MROS ist nach wie vor sehr überlastet. Von den Staatsanwälten höre ich, dass aus den MROS-Analysen nicht wahnsinnig viel Mehrwert entsteht und dass es relativ lange dauert. Für Staatsanwälte, die nicht auf diese Fälle spezialisiert sind, ist es sehr mühsam und sie wissen oft nicht, was sie damit anfangen sollen. In Bezug auf die komplexen Fälle habe ich also das Gefühl, dass sehr viele Ressourcen in dieses System fliessen, ohne dass viel dabei herausschaut.

Hingegen ist die Zusammenarbeit bei Betrugsfällen sehr effizient.

Denken Sie, dass die Zusammenarbeit in solchen Fällen effizient ist, wenn es ein ganzes Netzwerk von hunderten Money Mule Konten gibt, die z.B. eine transaktionelle Verbindung zueinander haben?

Ich kann Ihnen keine statistischen Informationen geben, aber ich kenne es aus Erfahrungsberichten und weiss von Fällen, in denen die Zusammenarbeit ziemlich effizient war. Allerdings gibt es auch Fälle, die sehr komplex sind und bei denen die Hälfte der beteiligten Parteien nicht bereit ist, diese zu untersuchen. Die andere Hälfte ist interessiert an einer Untersuchung, da es sich eigentlich um einen grossen Fall handelt, aber jeder sieht nur seinen kleinen Teil und so funktioniert es nicht.

Was definitiv in der Schweiz fehlt, da sind sich auch alle einig, ist die technische Möglichkeit für die verschiedenen Staatsanwaltschaften zu wissen, was bei den anderen Kantonen anhängig ist. Abgesehen von der Staatsanwaltschaftskonferenz gibt es auch kein geeignetes Forum für den Informationsaustausch. In Einzelfällen, wenn man Glück hat, kennt man sich noch zwischen den Staatsanwälten und es findet ein gewisser Informationsaustausch statt. Daher erscheint es mir nicht effizient.

Wie können die Finanzinstitute die Notwendigkeit der Einhaltung der Vorschriften zur Bekämpfung der Geldwäscherei mit ihrer Verpflichtung zur Erbringung von Finanzdienstleistungen für deren Kunden in Einklang bringen?

Ich denke, es liegt an den Banken, wie sie dies umsetzen. Es gibt durchaus Möglichkeiten, die bestehenden Vorschriften auf eine Art und Weise umzusetzen, die es den Banken ermöglicht, Kunden abzulehnen, die sie eigentlich nicht annehmen sollten und langfristig gesehen auch für sie nicht von Vorteil wären. Daher habe ich nicht wirklich das Gefühl, dass den Finanzintermediären per se Steine in den Weg gelegt werden mit den Sorgfaltspflichten. Das grosse Problem liegt jedoch darin, dass die meisten Banken ineffiziente Prozesse und keine effektiven Ausbildungsprogramme haben. Unter den heutigen Umständen könnte man dies meiner Meinung nach effizienter gestalten.

In den letzten zwei Jahren war die Transaktionsüberwachung der häufigste Auslöser für eine Verdachtsmeldung an die MROS. Gibt es angesichts des hohen Transaktionsvolumens Muster, auf welche die Banken bei der Transaktionsüberwachung achten können, um Geldwäsche durch Betrug zu erkennen? Was sind die Herausforderungen dabei?

Grundsätzlich denke ich, dass es bei vielen Fällen möglich ist, dies innerhalb des Transaktionsmonitorings festzustellen. Bei Betrug kommt es ein bisschen darauf an, um was es geht. Bei den klassischen Investitionsbetrügereien, die es immer mehr gibt, auch im Zusammenhang mit Kryptowährungen, denke ich schon, dass man bei einer Vielzahl von Eingängen von Drittpersonen ein Muster erkennen kann. Das ist etwas, was von vielen nicht überwacht wird. Insgesamt muss man jedoch feststellen, dass man zu wenig Schlüsse aus bestehenden Fällen zieht und das Transaktionsmonitoring entsprechend anpasst, wie ich es immer wieder erlebt habe. Es gibt bestimmte Regeln, die sicherlich vernünftig sind, aber oft führen sie dazu, dass man etwas nicht entdeckt. Wenn man es dann aufgrund eines anderen Auslösers erkennt und meldet, sollte man zurückgehen und überprüfen, worauf man in Zukunft achten sollte, um es frühzeitig zu entdecken. Insgesamt denke ich jedoch, dass viele Muster mit zumindest einer elektronischen Transaktionsüberwachung nicht effizient überwacht werden können. Das Kostenproblem dabei ist die grosse Anzahl von false positive alerts, und wenn man alles abdecken würde, würde man nichts anderes mehr tun als Transaktionsüberwachung.

Was sind effektive Methoden, die Banken einsetzen können, um die Transaktionsanalyse effizienter zu gestalten?

Ich bin überzeugt, dass es Methoden für eine automatisiertere Transaktionsanalyse gibt, insbesondere angesichts der Fortschritte in künstlicher Intelligenz in den letzten Monaten. Allerdings ist dies nicht mein Fachgebiet, und ich kann Ihnen keine konkrete Lösung bieten. Ich kann mir jedoch nicht vorstellen, dass es nicht möglich wäre, einem System anhand bekannter Fälle beizubringen, wonach es suchen soll.

End of interview

Appendix 3: Interview 2 – Advokatur Beuret

Inwieweit erschweren die immer strenger werdenden Vorschriften zur Bekämpfung der Geldwäscherei den Banken deren Umsetzung?

Das ist tatsächlich eine Problematik, die auch auf internationaler Ebene bereits erkannt wurde. Im Zusammenhang mit Finanzkriminalität, insbesondere Geldwäsche und Terrorismusfinanzierung, haben wir als Standard die GAFI-Richtlinien. In den letzten 10 Jahren haben wir festgestellt, dass je mehr Vorschriften erlassen werden, desto unproduktiver können wir sein. Eine Arbeitsgruppe wurde eingerichtet, um sich mit diesem Thema zu befassen und die Regulierungen zu lockern, die über das Ziel hinausgehen oder kontraproduktiv sind, weil sie schlichtweg überflüssig sind. Bei den Plenartreffen ist mir aufgefallen, dass zwar viele Diskussionen stattfinden, aber sehr wenig umgesetzt wird. Dies ist generell ein Trend, dass die Problematik zwar erkannt wird, aber nicht umgesetzt wird. In einem kürzlich veröffentlichten Dokument mit dem Titel "unintended consequences" hat die GAFI in diesem Zusammenhang bestimmte Elemente identifiziert, die qualifiziert werden müssen und andere von Anfang an entfernt werden sollten. Es ist eine Tatsache, dass bei zu viel Regulierung eine kontraproduktive Wirkung entstehen kann. Auf der anderen Seite bin ich persönlich der Ansicht, dass es in die richtige Richtung geht, jedoch nicht in Form einer Überregulierung. Man muss es ein bisschen im historischen Kontext betrachten: Ursprünglich hatten wir gar keine Regulierungen. Dann hatten wir einige Massnahmen, die jedoch nicht ausreichend waren und zu einigen Skandalen führten. Danach begann man mit punktuellen Massnahmen wie dem Umgang mit PEP und KYC. Im Jahr 1998 wurde dann das GwG (Geldwäschegesetz) eingeführt, das unter anderem die Sorgfaltspflichten vorschrieb. Zu dieser Zeit wurde alles hauptsächlich formal-rechtlich geregelt. Es wurde identifiziert und der wirtschaftlich Berechtigte ermittelt. Materiell galt lediglich die Anforderung, dass man die Plausibilität überprüfen und gegebenenfalls melden musste. Fast niemand hat gemeldet, und die Überprüfungen waren eher pro forma und nicht wirklich gründlich. Bis wieder ein Skandal aufkam. Heutzutage ist der Trend und das Fazit, dass das materielle Recht stark aufgewertet wird. Die jüngsten regulatorischen Massnahmen im schweizerischen GwG betreffen insbesondere die Verpflichtung, den wirtschaftlich Berechtigten zu überprüfen (nicht nur ein Formular ausfüllen zu lassen) und KYC- oder GwG-Dokumente zu aktualisieren. Es muss überprüft werden, ob sie auch tatsächlich aktuell sind, d.h., es werden nicht einfach nur Unterlagen eingeholt und beiseite gelegt, sondern sie müssen auch inhaltlich Bestand haben. Das sind gute Beispiele dafür, dass wir in die richtige Richtung gehen. Es ist zwar wieder mehr, aber es ist mehr mit

materiellem und richtigem Inhalt. Wenn also Kreuzchen in Formularen gesetzt werden, müssen die entsprechenden Dokumente auch überprüft werden. Der Nachteil liegt auf der Seite der Ressourcen, der Risikobereitschaft und -politik, d.h., der Finanzintermediär ist bereit, mehr Risiken einzugehen.

Denken Sie denn auch, dass das Gesetz einigermassen aktuell bleibt? Wenn man zum Beispiel betrachtet, ob klare Richtlinien vorhanden sind, um beurteilen zu können, wann eine Transaktion verdächtig ist und somit eine Verdachtsmeldung gemacht werden sollte, wenn man einen Verdacht oder eine verdächtige Transaktion hat. Vor kurzem gab es einen Bundesgerichtsentscheid, bei dem verdächtige Transaktionen nicht erkannt wurden (es wurde zwar geprüft, aber nicht als verdächtig eingestuft und erst im Nachhinein entdeckt). Ist das Gesetz in diesem Bereich nicht ziemlich weit und daher unklar formuliert?

Doch, das Gesetz ist weit gefasst und auch für die Anwendung, insbesondere für die FINMA, relevant. Das sieht man auch anhand der neuen Vorschriften im Zusammenhang mit den Finanzdienstleistungen. Es ist immer die gleiche Geschichte: Man trifft Massnahmen, meistens mit einem speziellen Hintergrund, manchmal aber auch aufgrund des Drucks seitens der GAFI. Dann passiert etwas und erst dann setzt man den Massstab. Dies ist ein erkanntes Problem im Schweizer Finanzmarktrecht. Man darf einfach nicht das Pech haben, der Erste zu sein, der in die Risikofalle tappt. Wenn man alles sauber plant, ist das Risiko zwar eingedämmt, aber es kann dennoch nicht restlos ausgeschlossen werden. Auch hier ein konkretes Beispiel im Zusammenhang mit den zuvor erwähnten Änderungen zu Beginn des Jahres: Die regelmässige Überprüfung der gesamten Dokumentation wurde erstmals im Parlament diskutiert, und es stellte sich die Frage, ob dies notwendig sei. Die zweite Reaktion war, dass wir uns darauf vorbereiten mussten, da es so oder so auf uns zukommt. Wenn es kommt, müssen wir jedoch klare Massstäbe haben. Und was hat die FINMA gemacht? Nichts. Es gab keine entsprechende Verordnung, sondern jeder wurde sich selbst überlassen. Interessanterweise gibt es mittlerweile so viele Marktteilnehmer, die Compliance-Spezialisten sind und effektiv einen Massstab gesetzt haben, der sich mehr oder weniger etabliert hat. Es reguliert sich ein Stück weit selbst, nicht nur im GwG. Das ist aus rechtsstaatlicher Sicht nicht unbedenklich. Es ist ein Balanceakt zwischen zu viel und zu wenig. Das zeigt sich auch an den vielen Skandalen, sowohl den aktuellen als auch den älteren. Die FINMA wird nun proaktiver. Alle sind besser informiert. Dennoch muss der Finanzintermediär fast hellseherisch in Bezug auf Risikobewertungen handeln. Auch die Gerichte hinken bei der Beurteilung der Fälle oft jahrelang hinterher, obwohl sich die Rechtsprechung mittlerweile geändert hat.

Wie können sich Banken besser gegen die Risiken von organisierten Geldwäschenetzwerken schützen?

Es stellt sich eher die Frage, ob das überhaupt möglich ist. Es gibt nämlich kein Wundermittel. Wenn etwas gut gemacht ist und auch der Wert nicht hoch ist, dann interessiert das niemanden und es fällt nicht auf. Aber auch hier muss man den historischen Kontext berücksichtigen: Was ist das GwG? Es ist wie das Strafgesetzbuch. Man will krassen Verfehlungen vorbeugen. Wie gesagt, gibt es kein Wundermittel. Die Botschaft besteht jedoch darin, dass man konsequent die Vorschriften durchsetzen muss. Dies erfolgt wiederum über die Risikopolitik. Das bedeutet, dass man auch über die notwendigen Ressourcen verfügen muss. Positiv ist hierbei die Verknüpfung zum materiellen Recht. Es wäre viel einfacher, wenn man nur die formalen Elemente hätte. Wenn man plötzlich für jeden Fall Plausibilitätsprüfungen durchführen muss, müssen die entsprechenden Personen auch entsprechend geschult werden. Das GwG ist zudem gut strukturiert, da die beiden Kernstücke des GwG (Melde- und Abklärungspflichten) den Zusammenhang zwischen den formalrechtlichen Bestimmungen und den materiellrechtlichen Kriterien herstellen. Als Beispiel: Ein neuer Kunde, Fotokopien und Angaben werden gemacht, das Konto wird eröffnet und es geht los. Aus bestimmten Gründen müssen Abklärungen getroffen werden. Hier enden die formalen Elemente, und es wird zur materiellen Prüfung übergegangen. Wenn dies ordnungsgemäß durchgeführt wird, kommt sehr wenig durch. Vor kurzem hatte ich einen Fall im Zusammenhang mit Kryptowährungen, einem ICO mit Masseninvestoren. Durch Zufall bemerkte eine Person, dass ein bestimmtes Dokument mit den anderen übereinstimmte. Sie unterschieden sich nur durch Fotos usw. Dann haben wir uns die 1000 Dokumente angesehen. Sieben davon waren identisch. Und diese waren eindeutig betrügerische Machenschaften (Urkundenfälschung usw.). Hier zeigt sich gut, dass man dies aufgrund der Beträge und der Menge nicht ohne Zufall entdeckt hätte. Es wird jedoch auch gerügt, weshalb man nicht genauer hingeschaut hat. Die Meldung ist der Link zwischen der Tätigkeit des Finanzintermediärs und der Behörde. Das Mindset hat sich geändert: Banken sind mittlerweile zu 95% soweit, dass sie sagen, im Zweifelsfall melden wir. Finanzintermediäre sind noch nicht so weit. Das GwG ist mittlerweile auch kohärent aufgebaut, da man nun auch die Pflicht hat, über das eigene Risikowissen zu verfügen. Man muss seine eigenen Risiken kennen. Dies kommt direkt von der Arbeitsgruppe GAFI. Man kann nur sauber arbeiten, wenn man sich selbst analysiert hat. Dann erkennt man möglicherweise, in welcher Tätigkeit man besonders einen Risikobereich erkennen kann, sodass man darauf besser achtet. Auch hier befinden wir uns im materiellen Recht.

Wie wirksam ist Ihrer Meinung nach das derzeitige Meldesystem bei der Bekämpfung der Geldwäscherei?

Ich muss hier kurz ausholen: Das Meldesystem hatte bis vor kurzem in der Schweiz noch einige Schwächen. Bis in die 90er Jahre hatte man nicht viel. Danach hatte man das StGB. Erst vor etwa 25 Jahren kam das GwG mit dem Melderecht. Es wurde aus verschiedenen Gründen als lächerlich erachtet (Anzahl Fälle, Fläche des Finanzplatzes, Mehrwert der Meldestelle). Heute haben wir tatsächlich Banken, die das ernst nehmen und es richtig machen wollen. Das ist erst seit etwa 10 Jahren der Fall, seit Branson 2016 gesagt hat, dass es so nicht weitergehen kann. Ein begründeter Verdacht liegt schon vor, wenn man ein Indiz hat. Das war illegal, denn das stand so nicht im Gesetz. Mittlerweile ist das Gesetz auch auf dem neuesten Stand. Der Finanzintermediär bringt aber zuerst den Mehrwert und meldet, weil etwas in der Luft liegt. Danach bringt MROS ebenfalls einen Mehrwert (z.B. Möglichkeit zur Herstellung von Verknüpfungen ins Ausland). Das funktioniert. Aber nur im Zusammenhang mit den Banken. Im Para-Banken-Sektor ist das noch nicht angekommen, da sie weniger exponiert sind. Ich glaube, dass die FINMA dort demnächst die Schraube anziehen wird, weil es nur ein oder zwei Beispiele braucht, damit die anderen mitziehen.

Global gesehen belegt die Schweiz diesbezüglich einen schlechten Platz. Meldungen wurden nur gemacht, weil der private Sektor, die Finanzindustrie selbst, die Abklärungen durchgeführt hat. Kanada hat ein anderes System, das automatische Meldungen kennt. Ein gesetzlicher Benchmark von z.B. $1000 wird gesetzt und völlig undifferenziert gemeldet. Wahrscheinlich ist keines dieser Systeme das Beste. Man kann darüber streiten. Ich persönlich finde es besser, den Sektor einzubeziehen. Aber mit entsprechender Kontrolle (FINMA) und sicher nicht so weit außerhalb, sondern in der Nähe irgendwo. Ich bin daher überzeugt, dass das sinnvoll ist. Denn wenn interne Abklärungen durchgeführt werden, fragt man zuerst den Relationship-Manager, weil er zusätzliche Informationen hat und am nächsten dran ist. Danach holt man möglicherweise noch Dritte dazu. Zuerst lässt man diejenigen handeln, die das Wissen haben, dann lässt man überprüfen.

Das Meldesystem ist also zu einem wichtigen Bestandteil geworden. Aber ich denke, dass noch ein massiver Aufwand erforderlich sein wird, weil zum Beispiel der Para-Banken-Sektor nicht darin enthalten ist und wir immer noch nicht dort sind, wo wir sein sollten, auch im Zusammenhang mit Überwachung usw. Schwachpunkte sind hier, dass der Benchmark immer noch zu hoch ist (es gibt immer noch zu wenige Meldungen, auch

von den Banken), die Meldestelle hinkt ebenfalls hinterher, und auch die Strafverfolgungsbehörde (z.B. in Korruptionsfällen und die Bundesstaatsanwaltschaft).

Sind Sie der Meinung, dass die Zusammenarbeit zwischen der MROS, den Banken und den Staatsanwaltschaften effizienter gestaltet werden könnte, um Geldwäscher oder Geldwäschenetzwerke besser bekämpfen zu können?

Man muss hier zwei Dinge unterscheiden: als erstes die Amtshilfe oder die polizeiliche Arbeit mit Strafverfolgung, wo völlig andere Grundsätze gelten. Im Vorfeld gibt es Audit-Tätigkeiten, noch bevor das formelle Strafverfahren eröffnet wird. Dabei gelten keine Parteirechte wie gemäß StPO. Es gibt jedoch einige gesetzliche Grundlagen wie das Bankkundengeheimnis, die jedoch nicht mehr gelten, sobald man im GwG-Geltungsbereich ist. In diesem Bereich kann die Abwicklung effizient gestaltet werden. Es wird gemeldet und die Meldestelle tauscht Informationen mit anderen Finanzintermediären aus. Die Meldestelle kann auch Informationen mit anderen Stellen im Ausland im Rahmen der Amtshilfe austauschen. Dieses Stadium ist formell gesehen relativ einfach und ohne Parteirechte. Die betroffenen Personen sind sich dessen gar nicht bewusst. Wenn jedoch die Strafverfolgungsbehörden eingeschaltet werden, gilt ein anderer Maßstab: Zuerst muss sichergestellt werden, dass sie ein Verfahren eröffnen können, und deshalb werden Vorermittlungen durchgeführt. In einer idealen Welt wäre der Meldebericht der Meldestelle so verfasst, dass keine Vorermittlungen erforderlich sind und das Verfahren direkt gegen die betroffene Person eröffnet wird. Das wird jedoch nie passieren, da die Strafverfolgungsbehörden ihre eigenen Vorschriften haben und sie nicht einfach aufgrund von Informationen handeln können, die im Rahmen des GwG oder der Amtshilfe gesammelt wurden. Die Tendenz geht jedoch in die richtige Richtung: Die Strafverfolgungsbehörde eröffnet das Verfahren irgendwann und dann müssen alle vorherigen Schritte nochmals formell durchgeführt werden, damit die betroffene Person sich jederzeit äußern und Akteneinsicht haben kann.

Es ist also rechtsstaatlich sehr schwer umsetzbar. Ursprünglich war es jedoch genau so gedacht: Erst Informationen sammeln und dann das Beweisverfahren durchführen. Es gibt jedoch auch Diskrepanzen. Zum Beispiel wird eine Geschäftsbeziehung mit Russland gemeldet. Mit Russland wird auf der Ebene von MROS mit den notwendigen Vorbehalten usw. ausgetauscht. Die Staatsanwaltschaft prüft das Verfahren und die Sachlage ist klar. Trotzdem wird kein Verfahren eröffnet, da keine Rechtshilfe von Russland zu erwarten ist. Es ist also möglich, etwas zu beweisen, aber es ist auch Hilfe für die Durchsetzung erforderlich. Deshalb wird es wahrscheinlich immer zweigleisig bleiben.

Du hast zuvor das Ping-Pong-Spiel erwähnt. Ich würde es nicht unbedingt so bezeichnen. Die beiden Phasen verlaufen relativ linear miteinander. Auf der anderen Seite gibt es partiell immer noch ein gewisses Hin und Her, da beispielsweise Finanzintermediäre oft nicht so häufig melden, wie sie sollten, weil sie selbst viel filtern oder bestimmte Geschäftsbeziehungen einfach nicht melden möchten. In solchen Fällen sind die einzelnen Akteure selbst schuld.

Es ist wichtig zu erwähnen, dass es neben den Finanzintermediären, Strafverfolgungsbehörden und der Meldestelle noch viele weitere GwG-Behörden gibt, wie z.B. die FINMA, CIF (als Koordinator), andere Aufsichtsbehörden und Gerichte. Hier muss es auch vorangehen. Vorher hatten wir das Beispiel, als die FINMA keinen Benchmark für regelmäßige Updates gesetzt hatte. Innerhalb der KGGT-Gruppe hat CIF die Führung. CIF führt keine operativen Tätigkeiten aus. Die anderen Behörden, die operativ tätig sind, machen mit, aber stellen die Legitimität in Frage. Es ist eine Partie, die noch nicht richtig gestartet ist. Es gibt das Spielfeld und die Spieler, aber es findet kein Spiel statt, da jeder etwas anderes mit dem Ball macht. Die Behörde muss auch die operativen Aspekte ansprechen können. Heute ist KGGT eher unbekannt, obwohl es sofort präsent sein sollte, wenn es um das GwG-Thema geht. Es ist nicht wie eine interdepartementale Arbeitsgruppe (IDAK usw.), wo man sich einfach trifft und dann irgendwann wieder tagt. KGGT ist eine GwG-Behörde und mehr als nur eine Arbeitsgruppe, aber immer noch zu schwach. Es wäre wünschenswert, ihre Effizienz zu steigern. Das geschieht jedoch nur mit Mitteln und dafür ist ein politischer Konsens erforderlich, der wahrscheinlich einen Skandal oder ähnliches voraussetzt. Wenn der Vorschlag, KGGT aufzuwerten, ins Parlament gebracht würde, wären wahrscheinlich drei Viertel dagegen. Wenn die Schweiz jedoch auf eine graue Liste käme, würde es wahrscheinlich implementiert werden. Die Schweiz verfolgt nun einmal eine Tröpfchen-Politik, die nicht immer schlecht sein muss.

Der Föderalismus in der Schweiz trägt nicht unbedingt zu einer effizienten Strafverfolgung bei, sondern verlangsamt diese eher.

Wie können die Finanzinstitute die Notwendigkeit der Einhaltung der Vorschriften zur Bekämpfung der Geldwäscherei mit ihrer Verpflichtung zur Erbringung von Finanzdienstleistungen für deren Kunden in Einklang bringen?

Die Aufwand/Ertrags-Relation in der Bank stimmt hier meistens nicht. Als einzige Möglichkeit bleibt, das Konto bei der PostFinance zu eröffnen. Die Einschränkungen sind jedoch dermaßen groß, dass wir letztendlich eine Lösung mit Neo-Banken gefunden

haben. Die Erschwernis entspricht der Realität. Ist man an einem gewissen Punkt angelangt, können sich Banken dann jedoch wieder selbst regulieren.

Problematisch wird es auch, wenn der Klient mit einer Milliarde kommt: Er kann noch so risikoreich sein, man wird versuchen, ihn aufzunehmen. Die gute Nachricht ist, dass man wirklich genau hinschauen muss und die notwendigen Abklärungen getroffen werden müssen. Die Banken nehmen heute keine Klienten mehr einfach so auf, ohne sich materiell-rechtlich abgesichert zu haben.

Zur Geldwäscherei muss als Vortat ein Verbrechen jeglicher Art oder ein qualifiziertes Steuerdelikt vorliegen. Sogenannte „Money Mules“ oder „Geldkuriere“ sollen Kriminellen helfen, unrechtmässig erworbenes Geld zu waschen. In einigen Fällen tun sie dies jedoch unwissentlich, weil sie auf ein vermeintliches Jobangebot oder einen Liebesbetrug (Romance Scam) hereingefallen sind. Dennoch machen sie sich wegen Beihilfe zur Geldwäsche strafbar. Was sind die Vortaten von den unwissentlich handelnden Money Mules, damit sie sich wegen Geldwäsche strafbar machen?

Es gibt hier viele verschiedene Elemente. Ein konkretes Beispiel für Money Mules im Zusammenhang mit Phishing (Jobangebote): Eine Person antwortet auf ein solches Angebot und stellt ihr Konto zur Verfügung. Danach werden CHF 10'234 auf das Konto eingezahlt. Der vermeintliche Arbeitgeber gibt dann den Auftrag, das Geld in bar abzuheben und per Money-Transfer an einen anderen Ort zu schicken. Es sind verschiedene Akteure involviert. In den meisten Fällen wurde das Geld "gehackt" (von einem Konto auf ein anderes). Dies stellt per se eine Vortat nach beispielsweise Artikel 147 StGB oder Urkundenfälschung dar. Geldwäsche selbst kann auch eine Vortat für Geldwäsche sein. Es ist wichtig zu beachten, dass die Money Mule-Person vorsätzlich handeln muss. Wenn zumindest bedingter Vorsatz vorliegt, kann der Money Mule gemäß Artikel 305bis StGB strafrechtlich verfolgt werden. Man kann nicht einfach annehmen, dass Money Mules einfach nur Opfer sind, denn die Sachlage ist ziemlich klar, wenn die soeben erwähnten Schritte stattfinden. Alle Phishing-Fälle wurden unter Artikel 147 StGB subsumiert. Bei Romance Scams ist insbesondere der Betrug und die Arglist relevant. Wenn das Opfer jedoch selbst einwilligt, kann man nicht mehr von Arglist sprechen.

In den Jahren 2020 und 2021 ist ein deutlicher Anstieg der Verdachtsfälle bei den Vortaten Betrug gemäss Art. 146 StGB und Urkundenfälschung nach Art. 251 Ziff. 1 StGB festgestellt worden. Inwieweit hängt dies Ihrer Meinung nach mit der

Zunahme der Betrugsfälle im Zusammenhang mit Geldwäscherei seit COVID-19 zusammen?

Es gibt drei Aspekte: In den Vorjahren, also vor den Korruptionsgeschichten, stand Betrug relativ weit oben auf der Liste. In den 2010er-Jahren war Korruption aktuell, aber nun ist sie wieder abgestiegen, weshalb Betrug wieder an erster Stelle steht.

Ein weiterer Zusammenhang besteht mit COVID: In den Jahresberichten der MROS wurden explizit Fälle von gefälschten COVID-Zertifikaten erwähnt. Das ist damit belegt.

Der dritte Faktor ist sicherlich die Tatsache, dass viele Menschen während der Pandemie viel mehr zu Hause waren und daher anfälliger für Betrugsfallen wurden. Wahrscheinlich hängt dies auch damit zusammen, dass man sich im Internet schneller mit fremden Personen anfreunden kann.

Allerdings liegen uns keine Studien vor. In Bezug auf einen Ausblick wird das Problem mit den Zertifikaten wahrscheinlich nicht mehr im Vordergrund stehen. Allerdings wird sich das neue PC-Verhalten wahrscheinlich unverändert fortsetzen. Es wäre auch interessant zu wissen, ob die Zahlen steigen werden und ob Art. 9-Meldungen die häufigsten Meldungen sein werden.

In den letzten zwei Jahren war die Transaktionsüberwachung der häufigste Auslöser für eine Verdachtsmeldung an die MROS. Gibt es angesichts des hohen Transaktionsvolumens Muster, auf welche die Banken bei der Transaktionsüberwachung achten können, um Geldwäsche durch Betrug zu erkennen? Was sind die Herausforderungen dabei?

Eine endgültige Antwort kann ich nicht geben. Meiner Einschätzung nach handelt es sich um Feinabstimmung. Danach kann die Geschäftsbeziehung wieder in Segmente aufgeteilt werden. Es ist nicht erforderlich, jede Geschäftsbeziehung im Detail zu prüfen. Das heißt, der Benchmark für die Abklärungspflicht ist die Ungewöhnlichkeit, also etwas, das aus dem Rahmen fällt. Das führt dann zur eigentlichen Arbeit. Das bringt mich zu einem weiteren Gedanken: Im österreichischen GwG erlaubt ein neuer Artikel den Finanzintermediären, künstliche Intelligenz dafür einzusetzen. Und das wird Realität werden, denn derzeit wird dies noch manuell erledigt. Das bedeutet, dass der Maßstab vertieft werden könnte. Banken denken bereits über solche Lösungen für Teilbereiche nach.

Braucht es in der Schweiz auch eine gesetzliche Grundlage, wenn man KI einsetzen möchte?

Ab einem gewissen Zeitpunkt wird das wahrscheinlich der Fall sein. Derzeit schreibt das Gesetz jedoch nicht vor, WIE die Abklärungen durchgeführt werden müssen, sondern lediglich, dass sie durchgeführt werden sollen. Es ist wahrscheinlich, dass die Plausibilisierung dennoch von einer Person durchgeführt werden muss, da Verantwortung übertragbar sein muss.

End of interview

Appendix 4: Interview 3 - Public Prosecutor's Office of the Canton of Aargau

Haben Sie seit dem Ausbruch von Covid-19 eine Zunahme der Fälle von Betrug als Vortat zur Geldwäsche festgestellt?

Wir haben eine deutliche Zunahme der Fälle bemerkt. Wir können jedoch keinen direkten Zusammenhang feststellen. Es gibt jedoch diverse Soziologen und Gesellschaftsforscher, die behaupten, dass sie einen direkten Zusammenhang sehen, was auch logisch erscheint. Die meisten Menschen, die mehr zuhause waren und im Homeoffice arbeiteten, haben auch mehr Zeit im Internet verbracht, und dadurch haben sich viele Straftaten ins Netz verlagert. Allerdings handelt es sich hierbei lediglich um Vermutungen und Schlussfolgerungen, da es keine eindeutigen Beweise dafür gibt. Um dies zu beweisen, müsste man die tatsächlichen Hintermänner von grösseren kriminellen Strukturen finden, die dies zugeben. Bisher haben wir aber keine solche Beweise gefunden, und entsprechende Aussagen sind äusserst selten zu lesen.

Wie effektiv ist die Zusammenarbeit zwischen der Staatsanwaltschaft, der MROS und den Banken bei der Bekämpfung der Geldwäscherei im Zusammenhang mit Betrug?

Die Zusammenarbeit mit der MROS ist sehr gut. Sie ist schnell und effizient. Insbesondere in Bezug auf COVID-Kreditbetrugsfälle funktioniert dies hervorragend. Die Zusammenarbeit mit den Banken gestaltet sich jedoch eher schwierig. Wir verstehen, dass die Banken das Kundengeheimnis wahren möchten, und dabei bemerkt man, dass Banken anders funktionieren als beispielsweise Migros oder Coop. Wenn wir beispielsweise Informationen benötigen, wie Videoaufnahmen einer Überwachungskamera eines Geschäfts, erhalten wir diese relativ schnell und unkompliziert. Im Kanton Aargau fordern wir diese durch eine Editionsverfügung an. Hierbei handelt es sich um dasselbe Dokument und dieselbe rechtliche Grundlage wie bei einer Editionsverfügung für eine Bank. Die angeforderten Informationen erhalten wir zwar ziemlich schnell von den Banken, aber die Art und Weise, wie wir sie erhalten, ist etwas anders.

Gemäss dem Jahresbericht der MROS sind bei der Staatsanwaltschaft Aargau seit 2020 deutlich mehr Verdachtsmeldungen weitergeleitet worden. Was glauben Sie hat zu dieser Zunahme geführt? Ist dies eventuell COVID bedingt?

Leider können wir diesen Zusammenhang nicht bestätigen. Der Verdacht besteht jedoch. Was man auch nicht ausser Acht lassen sollte, ist die Tatsache, dass Plattformen wie Teams und Skype im Zusammenhang mit dem Homeoffice eine hohe Anzahl an Nutzern gewonnen haben. Diese Zunahme wurde auch auf anderen Plattformen beobachtet, wie zum Beispiel Ebay oder Ricardo, die während der COVID-Pandemie viele neue Nutzer verzeichneten. Dies darf nicht ignoriert werden, da wir bei Wirtschaftsdelikten im Bereich der Geldwäsche oft über Online-Betrügereien sprechen, wie zum Beispiel Vorschussbetrügereien über Ricardo. Die technischen Möglichkeiten in diesen Bereichen wurden ausgebaut, Serverkapazitäten wurden erhöht und Apps wurden verbessert, was sicherlich auch Auswirkungen hat. Es ist also nicht nur der menschliche Wille, sich ins Internet zu begeben, sondern auch die Tatsache, dass die technischen Möglichkeiten während dieser Zeit deutlich verbessert wurden, was dazu geführt hat. Dennoch handelt es sich hierbei ebenfalls um Vermutungen.

Glauben Sie, dass die nationale und internationale Zusammenarbeit und der Informationsaustausch zwischen verschiedenen Behörden verbessert werden können, um die Geldwäsche wirksamer zu bekämpfen?

Man kann diese Zusammenarbeit wirklich weiter verstärken. Man muss jedoch auch immer beachten, wenn man jetzt Leute befragt, ob sie möchten, dass die Schweiz der EU beitritt, dann nennen die meisten Menschen als Antwort auf die Frage, warum sie dafür oder dagegen sind, eine Begründung, die sich nicht auf die Strafverfolgung oder das Netzwerk der Strafverfolgung in Europa bezieht. Mit anderen Worten, es gibt noch viele Möglichkeiten zur Verbesserung der Verbindungen zwischen den Ländern. Man muss auch feststellen, dass man im digitalen Raum der eigentlichen Täterschaft weit hinterherhinkt. Diese haben technische Errungenschaften, die schnell genutzt und im privaten Rahmen ausprobiert werden. Wenn sie funktionieren, werden sie verwendet. Als Behörde muss man eine Vorbildfunktion wahrnehmen, die besagt, dass man die Systeme gründlich prüfen muss, um festzustellen, ob man sie nutzen kann, welche Folgen dies hat und ob wir Informationen darüber erhalten können, wie die Nutzung einer Software die Strafverfolgung für die Gesellschaft verändert und wie die Gesellschaft danach über die Strafverfolgung denkt und ob sie noch Vertrauen darin hat oder nicht, und ob dies rechtlich erlaubt ist. Es liegt in der Natur der Strafverfolgung und der Behörden, dass die Dinge länger dauern. Es entsteht jedoch ein Ungleichgewicht der

Macht. Die Verbesserung muss kontinuierlich stattfinden. Wie die Technologisierung fortschreitet, muss sich auch die Strafverfolgung bemühen, sich jedem Phänomen anzupassen.

Wie verfahren Sie typischerweise in Fällen, in denen die Möglichkeit besteht, dass es sich bei der beschuldigten Person nicht um den eigentlichen Betrüger handelt, sondern um jemanden, dessen Identität gestohlen und für illegale Aktivitäten verwendet wurde?

Es ist vielschichtig. Auf Anhieb fallen mir drei separate Teilfolgerungen ein, die man bei dieser Frage beachten muss. Erstens besteht die Möglichkeit von Identitätsdiebstahl. Zweitens handelt es sich nicht um Identitätsdiebstahl, sondern beispielsweise um den missbräuchlichen Einsatz einer Datenverarbeitungsanlage im Zusammenhang mit Diebstahl oder Raub, wie z.B. bei einer gestohlenen Bankkarte. Dabei muss man berücksichtigen, wo man sich befindet. Schlussendlich versucht man in Bezug auf die Vorgehensweise entweder dem Geld nachzugehen oder, wenn mit der vermeintlichen Täterschaft kommuniziert wurde, der Kommunikation selbst. Es kann jedoch auch vorkommen, dass die Daten auf andere Weise als durch direkte Kommunikation mit dem Opfer übertragen wurden. In solchen Fällen versucht man, den Informationsaustausch nachzuverfolgen, also zu ermitteln, zu welchem Zeitpunkt die Täterschaft diese Daten überhaupt abrufen konnte, um einen Ansatzpunkt zu finden. Dies stellt jedoch eine grosse Herausforderung im Bereich der Cyberkriminalität dar.

Vor welchen Herausforderungen stehen Sie bei der Untersuchung von Geldwäschenetzen?

Es ist sehr anspruchsvoll. Die Herausforderung liegt in der Struktur der Täterschaft. Oftmals handelt es sich um Länder, die nicht den gleichen hohen Lebensstandard wie die Schweiz haben. In diesen Ländern gibt es ganze Branchen oder Arbeitszweige, in denen Call Center betrieben werden und Menschen angeworben werden, um Anrufe in die Schweiz zu tätigen. Dabei geht es nicht nur um Geldwäsche, sondern um verschiedene Phänomene, bei denen Täter Menschen dazu bringen, Dinge zu tun, die sie eigentlich nicht möchten. Oft handelt es sich um menschliche Manipulation. Um Ihre Frage zu beantworten: Ja, wir haben das grosse Problem, dass die Zusammenarbeit mit den Strafverfolgungsbehörden vor Ort in diesen Ländern sehr schlecht funktioniert. Der Bund führt eine Übersicht über die Länder, mit denen die Zusammenarbeit in den verschiedenen Ländern möglich und empfohlen ist und bei welchen sie als aussichtslos gilt. Oftmals befinden sich die Täter in genau jenen Ländern, in denen die Zusammenarbeit als wenig erfolgreich angesehen wird. Hinzu kommt, dass es eine

Herausforderung darstellt, wenn man Länder mit ähnlicher Gesetzgebung betrachtet. Die Gesellschaft weltweit steht vor der Aufgabe, mit unterschiedlichen Gebieten und Kulturen umzugehen, die unterschiedliche Wertvorstellungen haben. Wenn es unterschiedliche Wertvorstellungen gibt, kann sich auch die Gesetzgebung unterscheiden. Wenn man dann ein Phänomen wie die strukturelle Entwicklung des Internets hat, das von jeder Person weltweit in gleicher Weise genutzt werden kann, wird deutlich, dass Behörden, die auf Gesetze spezifisch für ein bestimmtes Land arbeiten, auf Probleme stossen. Die Gesellschaft als Ganzes ist gefordert: Wie gehen wir in einer globalisierten Welt vor und welche Regeln gelten allgemein? Es wird versucht, Rahmenbedingungen für eine Zusammenarbeit zu schaffen. Diese Rahmenbedingungen werden jedoch nicht von den Strafverfolgungsbehörden festgelegt, sondern von der Gesellschaft durch Gesetzgebung. Ich denke, wir werden wahrscheinlich nicht darum herumkommen, den Menschen zu sagen, dass es an der Zeit ist, mehr Eigenverantwortung zu übernehmen.

Wie wichtig ist es, dass die Öffentlichkeit über Betrug und Geldwäsche informiert wird, und welche Massnahmen ergreifen Sie, um die Öffentlichkeit über dieses Thema aufzuklären?

Als Kurzantwort: Es ist enorm wichtig. Wir als Staatsanwaltschaft sind relativ wenig involviert, da alles, was präventiven Charakter hat, der Polizei obliegt. Wir haben keine eigene Präventionsstelle wie die Polizei und auch keine Beratungsstelle. Es ist sinnvoll, dass dies bei der Polizei angesiedelt ist. Diese Bereiche werden kontinuierlich ausgebaut, insbesondere weil immer mehr Senioren ins Visier genommen werden, die nicht mit dem Internet aufgewachsen sind. Wir würden gerne mehr tun, stehen aber vor einer Mauer in Bezug auf dieses Problem. Als Staatsanwaltschaft unterliegen wir nicht dem Öffentlichkeitsprinzip, was die die Medien betrifft, sondern der Strafprozessordnung. Strafverfahren sind grundsätzlich geheim. Art. 74 verdeutlicht jedoch, in welchen Bereichen wir entsprechend informieren sollten, was auch gut so ist, da wir transparent sein möchten. Das führt uns zu dem Problem, dass wir zu den Medien gehen können und sie um einen Artikel über unsere Arbeit bitten, über die Gefahr für die Menschen, aber keine konkrete Geschichte liefern können. Die Medien sagen dann, dass sie das nicht veröffentlichen können, da sie eine Geschichte benötigen. Bei der Polizei funktioniert dies besser, da sie die Uniform tragen und den Auftrag zur Prävention haben. Das bedeutet, wir als Staatsanwaltschaft können das nicht tun, aufgrund gesetzlicher und historischer Gründe haben wir nicht die Möglichkeit, so gut informieren zu können. Man muss auch politisch denken, denn wenn wir einen Cyberdelikt haben und sagen, dass die Täterschaft in Algerien zu suchen ist, aber wir keine Möglichkeit

haben, dies zu tun, da die Zusammenarbeit mit Algerien als erfolglos eingestuft wird, dann stehen wir in der Medienwelt schlecht da. Wenn wir jedoch sagen, dass wir am Anfang stehen und von diesen Delikten wissen, aber nicht wissen, wie sie ausgehen, also dass wir bei der Prävention sind, kommt dies bei der Bevölkerung besser an. Es bedeutet nicht, dass wir bei der Strafverfolgung nichts tun, aber es erfordert leider eine sehr vorsichtige Kommunikation.

Es handelt sich um ein enorm wichtiges Thema, und auch die Polizei steht vor diesem Problem, da die Medien diesen präventiven Charakter ungern aufgreifen. Im Kanton Aargau werden sogenannte Cybertage veranstaltet, Informationsveranstaltungen für Bürger, bei denen ein halber oder ganzer Tag den Cyberdelikten gewidmet ist, was sehr gut ist. Wie man jedoch bemerkt, sind diese Cybertage spezifisch organisiert. Wenn wir jedoch die Menschen erreichen wollen, müssen wir auch bei der Polizei eine Geschichte bieten.

Wie gängig ist es inzwischen geworden, dass Sie gegen Geldwäschenetzwerke ermitteln müssen, und um welche Arten von Delikten handelt es sich üblicherweise dabei?

Es ist natürlich durchaus so, dass es kriminelle Netzwerke gibt, die neben anderen Tatbeständen auch Geldwäsche betreiben.

Wir wissen, dass sich die Anzahl der Geldwäschefälle im Aargau in den letzten Jahren verdoppelt hat. Bei diesen Fällen handelt es sich natürlich um Betrug. Es gibt gewerbsmässigen Betrug, auch im Zusammenhang mit dem Vorschussbetrug, Beihilfedelikte, die eigentliche Geldwäsche als Tatbestand und Urkundenfälschung.

End of interview