Tampere University of Applied Sciences

Combating money laundering and terrorist financing

Avan Jamil

BACHELOR'S THESIS
November 2022

International Business

ABSTRACT

Tampereen Ammattikorkeakoulu
Tampere University of Applied Sciences
Degree programme in International Business

Avan Jamil:
Combating money laundering and terrorist financing
Bachelor's thesis 50 pages,
November 2022

Money laundering refers to an activity whose goal is to hide the origin of certain assets or money. The funds that are the subject of money laundering are illegal because money laundering requires a predicate offence for money laundering, from which the funds originate. It is a global problem and various actors, and regulations are trying to influence it. When talking about money laundering, the financing of terrorism also often comes up. These crimes often have a similar method, the difference is the goal of the act. In money laundering, the goal is to get funds from criminal sources in to the legal financial system, while in terrorism, funds from legal sources are often used for illegal purposes.

The aim of this thesis is to give a comprehensive picture of the regulation related to combating money laundering and terrorist financing in Finland and the banking sector. The thesis describes the processes, legal regulations, theory and history of money laundering and terrorist financing. In addition to this, the thesis has dealt with various risk assessments, reporting obligations and administrative sanctions imposed on banks. Money laundering and the financing of terrorism is a topical issue, and these crimes have a great impact on society. Researching, summarizing the subject area, and bringing out the essential points for supervision is important for banks, so that the supervision of money laundering and terrorist financing could be carried out as required by the legislation.

The thesis was implemented as a theoretical thesis. The aim of the thesis was to find out what money laundering is, how does money laundering take place in practice and how is money laundering monitored and combated. The material is mainly based on official sources such as the publications and guidelines of the Financial Supervisory Authority and the police. Legislation has also been largely discussed in the thesis, focusing on the law on preventing money laundering and terrorism and the law on the Financial Supervisory Authority. The thesis ends with conclusions, which also includes an evaluation of the thesis process and one’s own learning.

Key words: money laundering, terrorist financing

CONTENTS

1 INTRODUCTION

1.1 Research topic and problem

The purpose of this thesis is to find out what money laundering and terrorist financing are and how it is combated and controlled in Finland, focusing especially on the banking sector. The incidence of the topic is also studied at the national level. The thesis deals with the history of money laundering, the definition of money laundering and terrorist financing, different methods of implementation and the fight against money laundering and terrorism. In addition to these, the thesis describes money laundering and terrorism supervisory authorities, banks' obligations, and measures to prevent and combat money laundering and terrorist financing, as well as administrative sanctions. Finally, there is a summary of the entire thesis. The thesis deals with questions such as:

- What is money laundering?
- How does money laundering take place in practice?
- How is money laundering monitored and combated?

The work is aimed at the banks doing business in Finland. The main focus of the thesis is on the theoretical part as the purpose of the thesis is to give the reader a comprehensive understanding of preventing money laundering and terrorist financing in the banking sector, which is why the chapters dig deeper into the topic thoroughly. The thesis was not done as an assignment, but the work is publicly available for everyone in the banking sector.

Several studies and theses have been done in the past about combating money laundering and terrorist financing. The increased coverage of the topic has certainly increased and the topic's popularity in theses as well. The thesis's have investigated the topic from the perspectives of different reporting parties, such as lawyers, accountants, and auditors. Previous studies have also been conducted from the perspective of the banking sector. The theses on money laundering and terrorist financing have included, for example, guides for bank employees, and examination of the issue through a risk-based approaches, and interviews with

employees of the bank's AML unit (Anti Money Laundering). However, in this thesis, the Combating money laundering and terrorist financing is studied at a general level, focusing on the banking sector.

Money laundering is an international and topical problem. The topic also receives a lot of attention in the media, and the reason for this is that the cases of money laundering and terrorist financing have increased year by year. The topic was chosen because of its topicality and my own interest. The topic is very close to me because I work in the Anti-money laundering team in the banking sector.

1.2 Research material

As a research method, I use qualitative research. My thesis is practical and easy to understand. The sources of the thesis have been obtained from literature dealing with the subject, official websites, legislation, and articles. The research material is mainly theory oriented. There is constantly new information about money laundering from the Police and other authorities. In the thesis, electronic sources are emphasized, because in them the latest information is published faster than in book versions. I consider the material I use to be reliable and useful for my work.

2 Money laundering and terrorist financing

2.1 The history of money laundering

Money laundering took off in the 1920s during the prohibition era in the US. After alcohol was made illegal in the US, a gainful black market soon developed to fill the gap and organized crime boomed as a result. (The history of money laundering, 2019) It has been said that the term "Money laundering" gained glamour when the mob boss Al-Capone set up laundromats across the city in order to disguise the source of the dirty money earned from alcohol sales and other criminal activities. (The history of money laundering, 2019)

Money laundering problems arose in the European Union in the early 1990s with the increase in drug crime. The funds that came from this were wanted to be investigated in more detail and to deal with the money obtained through criminal

means. The act included banks and other financial and credit institutions to verify customers identities and to keep records of their identities for at least five years after the end of the customer relationship. The act also included reporting suspicious transactions to the authorities. (Kananen 2009, 33.)

2.2 Definition of money laundering

Money laundering aims to hide the origin of property or money acquired through crime. The purpose is to make the money or property look like it was obtained legally. Money laundering is an intentional criminal activity. Central to this is the concealment of assets obtained through crime. Money laundering can also be committed, for example, by accepting such funds while being aware of the nature of the funds. Money laundering is an integral part of financial crime, the grey economy and organized crime, and as such is also an integral part of international crime. (Rahanpesu)

Money laundering can threaten the stability, reliability, and competitiveness of the financial system. Instability can increase the costs of, for example, loans, payment transactions and insurance, and the effects can be reflected in the wider economy.

The United Nation estimated in 2009 that the value of money laundering worldwide would be 1.6 trillion dollars a year, which would be 2.7 percent of the world's gross domestic product. According to the study, the authorities can confiscate or freeze only one percent of laundered funds. (Rahanpesu)

In September 2018, it became clear that more than 200 billion in money from suspicious sources had flowed through the Estonian unit of the Danish Danske bank. With this event, the public wondered whether other banks in the Nordic countries could have been guilty of the same. In 2017, Nordea founded a new Luminor bank with the Norwegian bank DNB. The head of Nordea's group at the time Casper Von Koskull, assured Helsingin Sanomat in an interview in October 2018 of the purity of Luminor bank, which he represents. Only one month after Von Koskull's statement, Luminor launched an extensive internal investigation into possible money laundering problems. (Hänninen 2022)

Luminor's own investigation revealed that at least EUR 3.9 billion of money from suspicious sources had passed through the accounts of the two merged banks. The problems particularly affected Nordea's Baltic operations. According to the leaked documents, for years the bank had customers whose activities met almost all the description of possible money laundering. Examples of these are, criminal suspicions, the absence of business reasons for the transfer of money and the use of tax havens and desk box companies. (Hänninen 2022)

In several cases, Nordea's customer had continued to make suspicious bank transfers for more than a decade, and the bank had not terminated the customer relationship. The documents that were leaked also made clear that Nordea's employee may have assisted their clients in potential money laundering. The suspicion was based on large cash deposits that the bank's employee had made at the same time as their customer had suspicious bank transfers. (Hänninen 2022) Section 6 of chapter 32 of the Criminal law (39/1889) defines money laundering in the following way:

" Whoever receives, uses, transforms, gives away, transfers, conveys or keeps possession of property acquired by crime, profit produced by crime or property that has replaced these in order to obtain a benefit for himself or another, or to cover up or hide the illegal origin of the benefit or property, or to assist the offender to avoid the legal sanctions of the crime, or conceals or conceals property acquired through crime, the proceeds of crime, or the true nature, origin, location of the property that has replaced them, or the enforcement actions or rights pertaining to it, or assists another in such concealment or concealment, shall be sentenced for money laundering to a fine or imprisonment for a maximum of two years. The attempt is punishable."

According to the criminal law, Luminor bank has committed the above-mentioned acts and therefore the bank should be punished for its act. Even though Luminor reported the case to the Estonian Financial Supervisory Authority, in the end, the whole case was swept under the carpet because the authorities were already overworked in sorting out the Danske Bank mess.

2.3 Different stages of money laundering

As a process, money laundering consists of different actions and different combinations of methods. Money laundering can be related to the execution of a pre-

crime or be a separate act from it or a series of separate sub-acts. There are three key stages that occurs commonly in the process of money laundering: placement, layering and integration.

The primary stage of money laundering is placement, during which “dirty” money is inserted into the financial and legal systems. Financial criminals steal, bribe, and influence people to obtain money that have been obtained unlawfully, then they relocate the money away from the source. The criminally obtained funds are “washed” and disseminated in this manner by being placed into a reputable financial system, such as offshore accounts. (Stages of money laundering explained 2021)

The second stage of money laundering is called layering. At this stage, the main attempt is to eliminate the origin of the money previously added to the financial system with a large number of financial transactions. These activities are usually bank transfers between branches, acquisition of cash for later sale, loans between shell companies and offshore companies with strong bank secrecy and can be done easily and quickly.

Once the money is in the financial system, the criminals make it difficult for the authorities to find evidence of money laundering. They accomplish this by strategically layering financial transactions and engaging in dishonest bookkeeping to hide the audit trail. (Stages of money laundering explained 2021)

The third and last stage is integration, where the funds appear legally acquired. After being long enough in the international banking system, the funds can be invested at some point. Dirty money is preferred to be invested in fixed assets, as this guarantees the preservation of the funds. Establishing the illegality of an investment can be extremely difficult because the origin of the money cannot be ascertained. (Kananen 2009, 35)

It is important to notice that the three steps of money laundering sometimes overlap in practise. There is no necessity that the illegal funds even be “placed” as in some instances of financial crime. (Stages of money laundering explained 2021)

2.4 Definition of terrorist financing

Financing of terrorism refers to activities in which funds are directly or indirectly given or collected for terrorist activities. Financing or attempting to finance a terrorist group or an individual terrorist is punishable. (Terrorist financing)

Financing terrorism is its own crime, and it is not one of the methods of money laundering. Funds used to finance terrorism can be either legally or criminally acquired. Even small amounts can be involved in financing. Therefore, the focus is on the object for which the funds are used. (Terrorist financing)

At its simplest, Financing terrorism can be natural person financing a terrorist group by handing over their fund to the terrorist group. In general, various natural persons, i.e., so-called intermediaries, arrangements for acquiring and transferring funds, and communities are both directly and indirectly related to the financing of terrorism. The majority of the time it is impossible to identify fundraising methods, let alone distinguish from one another. There are many purposes for the funds in terrorist organizations. It could be for weapons but also training, travel and accommodation to plan and execute their attacks and develop as an organisation. (FATF N.d.)

In 2021 the Financial Intelligence unit received 35 reports regarding the financing of terrorism or indicating terrorist financing, in addition to which the FIU classified a large number of reports regarding suspicious transactions as potentially related to the financing of terrorism based on their substance or personal connections. Based on the reports, the Financial Intelligence Unit opened 76 investigation units related to the financing or terrorism. (Vuosikertomus Rahanpesun selvittelykeskus 2021, 23.)

2.5 Combating money laundering and terrorist financing

Combating money laundering is a significant part of crime prevention because this way the cycle of crime can be broken. In Finland, any crime that has caused financial gain to the perpetrator can be considered a predicate crime of money

laundering. (Rahanpesun torjunta.) The Law on Prevention of Money Laundering and Terrorist Financing (444/2017) defines the fight against money laundering in Finland. Money laundering usually aims to take advantage of private entrepreneurs, which is why the Money Laundering law designates businesses that have the opportunity to discover suspicious transactions and, through that, money laundering, in the context of their own business. Such companies and communities must report suspicious transactions to the National Bureau of Investigation. (Poliisi.) The National Bureau of Investigation is responsible for combating money laundering, which is also regulated separately in the act on the financial Intelligence unit (445/2017).

On June 1, 2013, a national asset freezing mechanism was introduced in Finland to combat terrorism. The Act on the Freezing of Assets to Combat Terrorism (325/2013) enables the freezing of assets of natural persons and legal entities with terrorist connections. The purpose of freezing funds is to prevent the subject of the decision from channelling funds into terrorist activities. The Financial Intelligence Unit is in practice responsible for the preparation of freezing decisions made on the basis of the law and clarification of their conditions, as well as the public list of freezing. (Vuosikatsaus Rahanpesun Selvittelykeskus 2021, 24.)

In order to combat the financing of terrorism, the reporting party must be aware of the obligations imposed by the asset freezing law. The reporting entity must also familiarize itself with international sanctions systems to the extent that they are necessary in the reporting entity's business. The aim is to fight the financing of terrorism by freezing funds and using international sanction systems, and by following the rules set by act of money laundering obligations. The reporting party has the obligation to be up to date on the activities of its customers, keeping an eye on transactions that refer to the financing of terrorism, as well as transactions that refer to money laundering. (Finanssivalvonta)

The Financial Intelligence Unit receives notifications regarding suspicious transactions and notifications regarding suspected terrorist financing from the reporting parties defined in the money laundering act. During the first half of 2022, the FIU has received a total of 80,291 notifications to the money laundering register,

of which 61,143 were reported by virtual currency service providers. The notifications concerned suspicious transactions and suspected terrorist financing. (Rahanpesun selvittelykeskuksen puolivuosikatsaus 2022)

The number of money laundering reports varies each year, but part of the variation is explained by changes in reporting practices and retroactive report. During the first half of 2022, of all notifications received by the Financial Intelligence Unit, 6,140 were made by banks. The most recent half-year report of the FIU shows that the notifications made by banks increased in 2021 compared to the previous years, so it can be assumed that at the end of 2022 the notifications will be higher than in 2021. (Rahanpesun selvittelykeskuksen puolivuosikatsaus 2022, 3-5)

Table 1. The number of reports on suspicious transactions and suspected terrorist financing by reporting category in 2019- 6/2022. (Rahanpesun selvittelykeskuksen puolivuosikatsaus 2022,5.)

Reporting class	2019	2020	2021	6/2022
Offering general payment brokerage	34 799	20 653	19 593	9 082
Credit and financial institution (other than a bank)	9 254	7 541	14 618	85
Credit and financial institution (Bank)	10 070	12 888	13 877	6 104
Gambling Community	11 896	11 551	12 303	3 561
Insurance company, association, or occupational pension insurance company	134	138	127	148
Bookkeeper	21	31	89	36
Authority in accordance with the duty of care	54	90	78	50
other categories of notifiers that procedure small amounts of notifications in total	22	22	37	15
Sale of goods in cash >€10,000	38	45	36	15
Other authority home country	47	18	32	14
Accountant	13	18	19	12
Real estate agent	10	12	16	21
Investment service company	9	15	12	3
A lawyer or other provider of legal services	13	10	12	1
Fund company or custodian	5	9	3	1
Total of the above credits	66 385	53 041	60 852	19 148
Virtual currency service provider	75	9 000	3 631 789	61 143
Total	66 460	62 041	3 692 641	80 291

3 Supervisors of Prevention of money laundering and terrorist financing

3.1 Financial supervisory authority

The goal of the Financial Supervisory Authority's activity's is the stable operation of credit, insurance and pension institutions and other entities regulated to be supervised, which is required for the stability of the financial markets, the safeguarding of insured interests and general trust in the functioning of the financial markets (Act on financial supervisory authority 2008, 1 §.) In simple words said, the task of the FSA is to monitor that entities operating in the financial market comply with the relevant regulations and provisions that have been set for the investigation and prevention of money laundering and terrorist financing. The FSA works in connection with the Bank of Finland. The handling of related matters in the Government Council belongs to the Ministry of Finance. In addition to the Act on the Financial Supervisory authority, the Act on Public Servant of the Bank of Finland and other provisions related to the Bank of Finland apply to the Financial Supervisory Authority, unless The Act on the Financial Supervisory Authority provides otherwise. (Act on Financial supervisory Authority 2008, 2 §.)

The responsibility of the Financial supervisory Authority is to carry out its supervision on a risk basis. Practically it means that the control is focused especially on the riskiest actors, products, and business models. The tasks of the Financial Supervisory Authority include financial markets and monitoring and analysing the state of the institutions they supervise, the quality level of customer and investor information, and financial market procedures. (Finanssivalvonta.)

As part of the supervisory work of the Financial Supervisory Authority, it is the implementation of analyses, investigations, surveys, and inspections. The goal of these measures is to help the supervisor find potential areas of problems or threats. Those supervised by the Financial Supervisory Authority also deliver regularly reports to the Financial Supervisory authority. The reports are used in evaluating the activities of those being supervised. (Finanssivalvonta.)
The aim of the supervision is to monitor that, among other things, the anti-money laundering systems of banks or other financial institutions are sufficiently effective

and in accordance with the law. In practice, this means that the Financial Supervisory Authority should monitor that the entities they supervise make reports sensitively enough to the Central Criminal Police's Money Laundering Investigation Center.

3.2 The Financial Intelligence unit

The Financial Intelligence Unit (FIU) established in 1998 by the National Bureau of Investigations operates in the tasks of preventing and investigating money laundering and terrorism. The operation of the unit is regulated according to § 2 of the Act on the Financial Intelligence unit. (Rahanpesun selvittelykeskus vuosikertomus 2021, 11.)

The Financial Intelligence Unit is divided into the following functions:

- Receiving notifications, which is responsible for checking incoming notifications and, in part, also prioritizing them.
- Investigation groups 1 and 2, which focus on investigating money laundering.
- A special investigation that specializes in combating the financing of terrorism and virtual currencies.
- Analysis group, which includes the FIU's IT and analysis functions. (Rahanpesun selvittelykeskus vuosikertomus 2021, 11.)

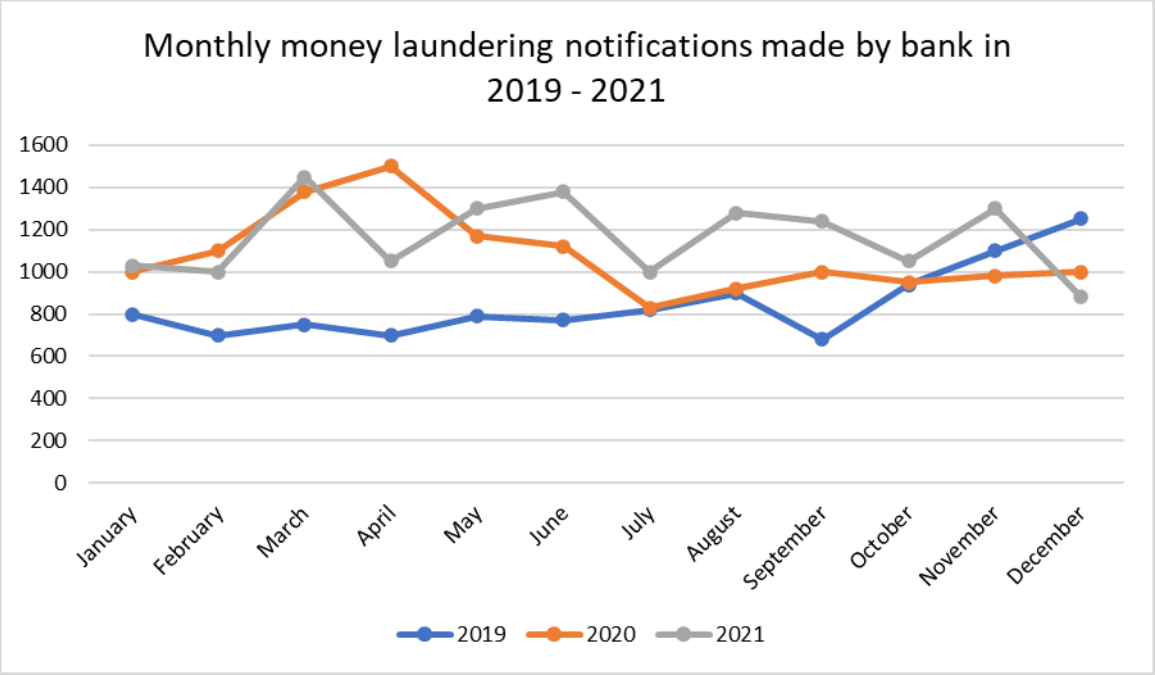
According to the law on the Financial Intelligence Unit, the FIU must prevent, reveal, investigate, and look into activities related to money laundering and terrorist financing. According to the anti-money laundering and terrorist financing legislation, the FIU is obligated to receive and analyse reports and give feedback on their effects. The Financial Intelligence Unit must cooperate with the authorities, as well as with foreign states and international organizations working in the fight again and investigation of money laundering and terrorist financing. The Financial Intelligence Unit must also cooperate with reporting entities. (Laki rahanpesun selvittelykeskuksesta 2017, 2 §.)

The Financial Intelligence Unit must keep statistics on the number of notifications and suspensions of transactions referred to in the Money Laundering Act, the number of information request received, answered, and denied, and the number of suspicious transactions brought under investigation. (Rahanpesun selvittelykeskus)

From 2022 to 2021, the total number of notifications increased radically. This is primarily explained by the exceptionally large numbers of notifications by virtual currency service providers in 2021. From other reporting groups a total of 60,852 notifications were received in 2021. This was 7.811 notifications (14.7 %) more than received from these groups of notifiers in 2020. (Rahanpesun selvittelykeskus vuosikertomus 2021, 12.)

In 2020, domestic credit institutions and branches of foreign credit and financial institutions made a total of 12,888 notifications. In 2021, their number of notifications was a total of 13,877. The growth was still around 7.7 percent on an annual basis, even though the number of notifications by banks increased for the seventh year in a row. (Rahanpesun selvittelykeskus vuosikertomus 2021, 13.)

When looking at the number of monthly notifications made by banks over the past three years, it is clear how big the increase has been from 2019 to 2021. In 2019, an average of 840 notification were made per month, and in 2020, the monthly average of notifications was around 1074 notifications. In 2021, the monthly number of notifications varied between December’s 866 notifications and March’s 1456 notifications, with the average being around 1156 notification per month. The number of notifications made by banks in 2021 has generally been above the monthly average of 2020. This stands out well in the following picture.



Picture 1. Monthly money laundering notifications made by banks in 2019 – 2021. (Rahanpesun selvittelykeskuksen vuosikertomus 2021, 14.)

3.3 The Financial Actions Task Force (FATF)

The Financial Actions Task Force (FATF) is a global action group against money laundering and terrorist financing, which was founded in 1989 under the OECD (The Organization for Economic Co-operation and Development). FATF currently has 37 member states and 2 regional organizations. Finland has been a member of the action group since 1991 after which Finland has also participated in international cooperation against money laundering and terrorist financing. (FATF n.d.)

FATF sets international standards for the prevention of money laundering and terrorist financing threats to various international financial systems in order to enhance legislation and the actions of authorities. The FATF monitors the progress of its member countries in the implementation of its recommendations, evaluates the techniques of money laundering and terrorist financing and countermeasures, and promotes the acceptance and implementation of FATF recommendations worldwide. (FATF n.d.)

FATF's tasks also include periodic country assessments. Finland's latest land assessment was issued in spring 2019 and the follow up report was issued at the FATF General Assembly in October 2022, according to which the fight against money laundering and terrorist financing is at a reasonably good level in Finland, although the report also notes some shortcomings. (FATF n.d.)

3.3.1 Other International Supervisory authorities

In addition to FATF, other parties involved in preventing international money laundering and terrorist financing are e.g.,

- European Commission
- Council of the European Union
- The European Securities and Markets Authority (ESMA)
- European Banking Authority (EBA)
- European Insurance and Occupational Pensions Authority (EIOPA)
- United Nations
- The counter – Terrorism Implementation Task Force, and,
- Terrorist Finance Tracking Program (TFTR)

As an Example, TFTR is an operational organization founded by the United States Treasury Department. The organization started after the WTC attacks on September 11,2001. TFTP's mission is to identify, track and monitor terrorists. The Operational organization is in a unique position in tracking terrorist money flows, and it assists the US government in exposing terrorist cells and maps terrorist networks in the US and internationally. (Terrorist Finance Tracking Program)

4 Legal Regulation

4.1 International Sanctions

International sanctions refer to limiting or suspending economic or commercial cooperation and, for example, transport and communication links or diplomatic relations with a certain state or groups of individuals and entities. The purpose on sanctions, as part of other foreign policy actions, is to influence the policy or activity of another state or group of people, which is considered to threaten international peace and security. This type of activity can be, for example, the spread of weapons of mass destruction, international terrorism, or extensive human rights violations. The selection of sanctions includes, for example, export and import restrictions, financial sanctions, and travel restrictions. (International Sanctions.)

International sanctions are based on the decisions and regulations of the Council of the European Union, which have also implemented the framework resolutions of the United Nations Security Council and the decisions of the Security Council and the sanctions committee under it. The United Nations Security Council sets globally binding sanctions, which the individuals states of the European union are also entitled to impose sanctions in their own county. Finland's international financial sanctions are published in the Official Journal of the European Union. The Ministry of Foreign Affairs of Finland is primarily responsible for ensuring that Finland complies with the financial sanctions imposed by the United Nations and the European Union. (International sanctions.)

4.2 Money laundering directives

In the European Union, the use of the financial system for money laundering and terrorist financing is prevented by the money laundering directive. This directive is known as the fourth money laundering directive, which started in 2015 and was implemented in Finland in 2017 with the new Money Laundering Act (28.6.2017/444.) After this, changes have been made to it with the fifth money laundering directive in 2018. (EU-lainsäädäntö.)

The fourth money laundering directive addresses the threat of money laundering. The obligations of the Council of Europe 91/308/EY to prevent money laundering were to set only for the financial sector and the topic was defined with narcotics crimes in mind. The scope of the above-mentioned directive was expanded by the European Council Directive 2001/97/EY. (EU 2015/849.) With the fourth Money Laundering Directive, the aim was to create a regulatory environment where companies can grow their business without spending a disproportionate number of resources on regulatory compliance. With the directive, the European union Commission, member states, national supervisory authorities and reporting entities and entrepreneurs were obliged to prepare risk assessments of money laundering and terrorist financing. The aim of this was to enhance the prevention of money laundering and the financing of terrorism in such a way that the measures related to prevention are mased on the prepared risk assessments and thereby it would be possible to allocate them effectively to the riskiest areas. With the risk assessments, the operators must also have at their disposal the operating principles, control measures and procedures related to their own operations, which effectively reduce and manage the risks identified at the level of the Union, Member States, industries, and those subject to notification. (Eu-lainsäädäntö.)

The fifth directive focused especially on financial services utilizing modern technology. The background for this was especially the terrorist attacks aimed at Europe, in connection with which new methods emerged for terrorist groups to finance and carry out their operations. The fifth money laundering directive made it mandatory for member states to introduce automated systems that allow information about the holders of bank and payment accounts to be submitted to the authorities. The directive also extended money laundering regulations to virtual currency providers and art dealers (when the payment is over 10,000 euros). The fifth money laundering directive was implemented in Finland with the Act on the Supervision System of Bank and Payment Accounts (571/2019) and the Act on Virtual Currency Providers (572/2019). With the directive, changes were also made to the Money Laundering Act, among other things. (EU-lainsäädäntö.)

The sixth Money Laundering Directive (AMLD6) is intended to retain the provisions of the current Money Laundering directive that were not transferred to the Money Laundering Regulation. The new directive would include, among other

things, provisions on the duties and powers of the competent authorities. In addition, there would be regulations on registers of beneficial owners and bank and payment accounts, national supervisors and Financial Intelligence unit, and co-operation between authorities. (EU-lainsäädäntö.)

4.3 Regulation on transfers of funds

The Payer's Information Regulation establishes the provisions on the payer's and payee's information, which must be submitted in connection with money transfers involving any currency in order to prevent, disclose and investigate money laundering and terrorist financing, when at least one of the payment service providers participating in the money transfer has invested in the Union. The regulation in question applies to fund transfers in any currency sent or received by a payment service provider established in the Union or a payment service provider acting as an intermediary. The regulation is based on the international recommendations of the Financial Action Task Force (FATF). The purpose is to ensure that FATF's recommendation on electronic fund transfers is implemented in a uniform manner throughout the Union. (Lainsäädäntö.)

The fourth article of the Payer's Information Regulation stipulates the information to be submitted along with the fund transfers. According to that article, the obligation of the payment service provider used by the payer is to ensure that the payer's name, address, official identity document number, customer number or place of birth and date and payment account numbers, as well as the payee's name and his payment account number are delivered with the fund transfers. Before transferring the funds, the payment service provider used by the payer must verify the correctness of the payer's information mentioned above based on information and documents obtained from an independent and reliable source. The payment service provider used by the payer may not carry out the funds transfer until he has ensured that the provisions of the above-mentioned article are fully complied with, however excluding the application of the exceptions provided for in the fifth and sixth articles. (EU 2015/847.)

The fifth article provides for transfers of funds within the Union. According to the fifth article, the payer's payment service provider is the payee within three working days used by the payment service provider or the information to be made available on the request made by the payment service provider acting as an intermediary, when the transfer of funds, the amount of which is or are in the form of one payment or several payments that appear to be connected to each other or total more than one thousand euros, the information according to the fourth article concerning the payer or payee. In the case of a fund transfer, the amount of which does not exceed one thousand euros and which does not appear to be connected to other funds transfers, the amount of which, together with the transfer in question, exceeds one thousand euros, the payment service provider used by the payer must provide the payment service provider used by the payee or the payment service provider acting as an intermediary with the names and payment account numbers of the payer and the payee or a unique transaction ID. An exception to the above mentioned for fund transfers is a situation where the payment service provider used by the payer has received the funds to be transferred in cash or anonymous electronic money, or the payment service provider used by the payer has justified reason to suspect money laundering or terrorist financing in transfer of funds. (EU 2015/847.)

In the sixth article, the law on fund transfers outside Union applies, according to which in cases where the payment service provider used by the payee is located outside the Union and is involved in such fund transfers, the amount of which does not exceed one thousand euros and which do not appear to be connected to other funds transfers, which together with the transfer in question, amount to more than one thousand euros, the names of the payer and payee and the numbers of their payment accounts or a unique transaction ID must be submitted. (EU 2015/847.)

4.4 Act on the combating money laundering and the terrorist financing

In Finland, the prevention against money laundering and terrorism is regulated by the Act on the Prevention of Money Laundering and Terrorism. The aim of the law is to prevent money laundering and the financing of terrorism, as well as to investigate and expose the activity in question. The goal is to improve the tracking

and retrievability of the benefit gained from the crime. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, Chapter 1 section 1.) Before the Law on Prevention of Money Laundering and Financing of Terrorism, the Law on Prevention and Investigation of Money Laundering and Financing of Terrorism was in force. The reform of the money laundering legislation entered into force on July 3,2017. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 9 section 7.)

In 2019, the prevention of money laundering and terrorist financing was enhanced with new legislation. One of the reforms in the money laundering legislation was the obligation to register in the regional administrative agency's new control register, which entered into force on July 1st, 2019. The latest changes entered into force on April 1, 2022. The new changes partly concerned the obligations of knowing the customer. In the future, the person obliged to report must take sufficient measures to ensure that the funds of the parties in accordance with the EU sanctions regulation or the parties mentioned in the freezing decision of the financial intelligence unit are frozen and that no funds are handed over to these parties. In addition, there was an exception to the identification obligations, which concerns the verification of the identity of the general trustee and the retention of identification information. There were also changes to the definition of politically influential persons and the enhanced obligation to know them. (Lainmuutokset tehostavat rahanpesun ja terrorismin rahoittamisen estämistä 2022.)

4.5 Act on Freezing Funds to Combat Terrorism

In accordance with the decision of the Finnish Parliament, the law on the freezing of funds to combat terrorism provides for the United Nations Security Council on 28th of September 2001 in accordance with the resolution adopted by the United Nations, which is directed to the obligation of the member states. (Laki varojen jäädyttämisestä terrorismin torjumiseksi 2013, section 1.) In the law, the freezing of funds refers to measures that prevent all such movement of funds, conversion, transfer, processing, use that would change the amount, ownership, control, location, purpose, or nature of the funds. (Laki varojen jäädyttämisestä terrorismin torjumiseksi 2013, section 2.)

According to section 3§ of the Act on the Freezing of Funds, funds must be frozen from a natural person or a legal entity that is considered to be involved in acts of terrorism, the Council's position (2001/931/YUTP), from a person or an entity that has been convicted under section 34a of the Criminal Law to acts according to the chapter, i.e., terrorism or who is suspected of the said act. Assets that belong to a person or entity that has been requested to be frozen by the competent authority of another state must be frozen in accordance with article 3. If a person is suspected of having committed crimes of financing terrorism, the funds must be frozen. The assets must also be frozen if the person who fits the aforementioned points owns 50 percent of the entity or company or if the person has controlling power in the aforementioned. In addition, the assets of a private company can be frozen if it is responsible for the financing of terrorism for the full amount of its obligations as well as for its own debt. (Laki varojen jäädyttämisestä terrorismin torjumiseksi 2013, section 3.)

If the reporting party discovers that its customer is on the freezing or sanctions list, any ongoing transaction must be suspended, and funds may not be handed over to the person or entity in question. After this the matter must be reported to the Helsinki National Enforcement Authority without delay, even if it is unclear whether the client is the same person or entity as the person or entity subject to the sanctions or freezing decision. In addition, the funds of a person or entity subject to freezing or embargo may not be handed over to a third party. (International economic sanctions and domestic freezing decisions, 2018.) The enforcement authority is obliged to enforce certain international sanctions. The international sanctions that the enforcement agency implements are the freezing of assets in accordance with the Act on combating terrorism and the measures related to the freezing of assets in accordance with the Sanctions Act. (Kansainvälisten pakotteiden täytäntöönpano Suomessa)

In Finland, decisions to freeze funds are made by the Natural bureau of investigation under national law. The Natural bureau of investigation maintains a list to which suspension decisions apply. The Natural Bureau of Investigation must notify the Ministry of Foreign Affairs of Finland of a reasoned decision to freeze

assets. After receiving the notification, the Ministry of Foreign Affairs must inform the committee or working group of the Council of the European Union and the United Nations Security Council about the reasoned freezing decision. (Laki varojen jäädyttämisestä terrorismin torjumiseksi 2013, section 9.)

5 Reporting Obligation

5.1 Reporting Obligation in Money Laundering Legislation

The reporting obligation is stipulated in the Money Laundering Act for traders in certain industries. Those obligated to report must identify their customers, monitor their customers' activities, and report their customers' suspicious transactions. The notification must be made to the investigation center of the Financial Intelligence unit of Natural Bureau of investigation. The task of the reporting parties is to ensure that the obligations of the Money Laundering Act are known internally in the company and that they are followed in the company's operations. The authorities get the best information about suspicious transactions with the help of reporting agents, which is why their role in preventing money laundering and terrorism is significant. (Obligated entities.)

The Regional Administrative Agency of Southern Finland (AVI) supervises nationwide the implementation of legislation to prevent money laundering and the financing of terrorism. The Regional Administrative Agency (AVI) monitors that those who are obligated to report comply with the obligations set by the legislation on the prevention of money laundering and terrorist financing. Financial service providers that are not supervised by Finnish Financial Supervisory Authority are supervised by the Regional Administrative agency, such as debt collection agencies, consumer lenders, entities engaged in guaranteed activities and entities that offer financial leasing. (Rahanpesun valvontarekisteri)

According to the Chapter 4 § 1 of the Act on the Prevention of Money Laundering and Terrorist Financing, the person obligated to report has the obligation to request information. Suspicious transactions must be reported to the Financial Intelligence Unit without delay. The notification must be made in accordance with the legislation of the financial intelligence Unit (445/2017). According to section 4

of the financial intelligence Unit Act, the unit has the right to receive information and documents that are significant in terms of preventing and investigating money laundering and terrorist financing from the entity appointed to perform a public task, the authority, and those subject to notification free of charge. However, so that it does not violate business and professional secrets or the privacy of an individual, foundation or on the confidentiality of information about the financial conditions, financial status, or tax information of the community. (Laki rahanpesun selvittelykeskuksesta 2017, section 4.)

The reporting party can also file a money laundering report for a single payment or other performance that exceeds the threshold value set as the maximum amount or for unrelated performance or payment. Nevertheless, in the fifth paragraph of the first paragraph of Section 1 of the Payment Institutions Act, it is stated that the money transfer service provider should report each individual or several unrelated transactions on payments with a value of at least one thousand euros. The reporting party must submit all documents, information relevant to the suspicions of money laundering and respond to the financial intelligence unit's information request regarding money laundering within the time limit set by it, if the information request time is set to reasonable time limits. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 4 section1.)

The reporting party must ensure that the employees receive training for the job under the Money Laundering Act and the Act on the Prevention of Financing of terrorism, so that the provisions of the law are complied with during work. A person who is responsible for the internal control of this law and the regulations issued pursuant to it must be appointed to the workplace if it is necessary considering the nature of the reporting obligation. In addition to the above, reporting obligations that are part of a group or other economic association must follow the internal instructions and procedures of the group or other economic association in order to ensure the prevention of money laundering and the financing of terrorism issued under the legislation compliance with regulations. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 9 section 1.)

5.2 Obligation to Obtain Information

When detecting an abnormal or suspicious transaction, the reporting party must find out the basis and purpose of the transaction in question, this is called the obligation to obtain information. Based on the report received, the reporting party can assess whether it is necessary to report the transaction to the financial intelligence unit. The reporting party must find out the background of the transaction, for example, when the transaction does not have an obvious financial purpose, the transaction deviates from its usual structure or size. The background of the transaction must also be clarified when the transaction does not match customer's transaction or financial situation. If an unusual or suspicious transaction is only noticed later, the report must be made regardless. The notification is not affected by whether the customer relationship has been cancelled or refused, or whether the transaction has been completed or suspended. Failure to report is always a punishable act. When suspecting the financing of terrorism, the supervised person has the same obligations as when detecting a suspicious transaction that may be related to money laundering. The difference, however, is that the funds used to finance terrorism can be legal in origin. In this case, the person being supervised must pay attention to the purpose of using the funds. (Obligation to obtain information and to report 2021.)

The reporting party is not responsible for possible financial damage to the customer caused by the suspension and settlement of the transaction. The reporting party is also not responsible for financial damage caused by refusing the assignment or reporting to the financial intelligence Unit. It is therefore a release from the liability of the person being supervised, which, however, requires that the person liable to report has taken the circumstances reasonably into account and has observed the necessary diligence. (Obligation to obtain information and to report 2021.)

5.3 Obliged Entities (Reporting party)

The obligation to report is stipulated in Section 2 of the Money Laundering act, which applies to entities and entrepreneurs affected by the scope of the law.
Such companies and communities are

- Credit, finance, and investment sectors as a whole.
- Pawn shops, real estate brokers, insurance companies and insurance brokers are also obligated to report.
- Various associations engaged in betting, parimutel betting and gambling casinos, such as Veikkaus Oy and Ålands Penningautomatförening (PAF), which engages in gambling activities in Åland, belong to within the scope of the reporting obligation.
- Operators offering accounting, auditing, tax advice and legal services are also obligated to report if the business or professional sells or forwards goods where payment is made in cash and is at least 10,000 euros.

In money laundering, large amounts of cash are considered a big risk. (Obligated entities)

5.4 Suspension and refusal of the transaction

The transaction must be suspended if the reporting party judges it to be suspicious or suspects that the related funds are being used to finance terrorism or its attempt. The exception is that transactions cannot be left unfinished or refusing or interrupting the transaction would make it difficult to find out the actual beneficiary. In such a case, the reporting party can complete the business contrary to the law. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 4 section 5.)

The Financial Intelligence unit can directly, at the request of the authority responsible for combating foreign money laundering or the financing of terrorism , issue an order to the person obliged to report to suspend the transaction for a maximum of ten business days, if suspension of the transaction is necessary to prevent crime, money laundering and terrorist financing so that the targeted property, the benefit from the crime can be investigated, revealed and prevented. (Laki rahanpesun selvittelykeskuksesta 2017, section 6.)

In 2018, the police searched properties owned by Airiston Helmi, which is a company owned by a Russian billionaire. The company was suspected of money

laundering, gross tax evasion, gross employment pension insurance payment fraud and covert payment of wages. The banks reacted to the event by closing the accounts of Airiston Helmi Oy. The bank is under no obligation to open an account for business customers, as entering into a transaction is based on the banks' own risk analyses and contractual terms. According to Pekka Vasara, the head of money laundering at the Financial Supervisory Authority, the law does not directly say that a bank can terminate a customer relationship upon detecting a suspicious transaction. However, information provided by the customer that is found to be incorrect, linked to other risks related to money laundering, gives the bank grounds for terminating the business relationship. (Malkoc 2019.)

6 Risk Assessment

The risk assessment related to preventing money laundering is a multidisciplinary concept. Risk assessments are made both at the EU level and also for individual customers. The requirement to prepare risk assessments comes from the fourth money laundering directive enacted by the European Union. Even before the fourth money laundering directive, the preparation of a risk assessment has been strongly recommended including by the FATF, although it was not mandatory. Risk assessments are divided into supranational, national, supervisor-specific and risk assessment of obliged entity. All these risk assessments are connected to each other. (Risk assessment.)

6.1 National risk assessment

Finland's national risk assessment is prepared by the Ministry of the Interior every three years. The purpose of the national risk assessment is to map risks that threaten the environment, various people, critical systems, and services. The above mentioned are all risk that the authorities must prepare for at the national level. The risk assessment must cover all threat models considered in the society's security strategy. The national risk assessment is based on the European one to the obligation set by the Union, according to which member countries must periodically assess risks that may require rescue measures from other member countries if the risk materializes. (Risk assessment.)

6.2 Supranational risk assessment

The European Commission is obligated to prepare an assessment of them for the for the European Union's international market about the significant money laundering and terrorist financing risk associated with cross-border activities. This risk assessment is called Supra National Risk Assessment (SNRA). The first transnational risk assessment was published by the commission on 26th of July 2017 and the second on 24th of July 2019. The commission's obligation is to update the report at least every two years or more often if necessary. (Risk assessment.)

6.3 Supervisor-specific risk assessment

The supervisor-specific risk value means that the competent supervisory authority and the bar association must prepare a risk assessment of the money laundering and terrorist financing threats of the reporting entities under their supervision. When creating a risk assessment, the competent supervisory authority and the bar association must consider the European Union's money laundering and terrorist financing risk assessments prepared by the Commission and the risks of money laundering and terrorist financing formed from them. The national risk assessment must also be considered, the risk related to the supervised reposting entities and their customers, services, products, and the aforementioned risk of money laundering and terrorist financing. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 2 section 2.)

When planning the risk assessment, the competent supervisory authority and the bar association must consider the frequency and scope of the supervision. Supervisor-specific risk assessment should be updated by the competent supervisory authority and the bar association continuously or when there are changes or other relevant facts affecting the supervisor's risk assessment in the reporting party's operations. The competent supervisory authority and the bar association are obligated to publish a summary of the risk assessment. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 2 section 2.)

6.4 Risk assessment of obligated entity

In order to identify and evaluate money laundering and terrorist financing, the reporting party must prepare a risk assessment, which must be updated regularly. Changes made to the risk assessment must be submitted to the competent bar association or supervisory authority at their request and without undue delay. (Laki rahanpesun ja terrorismin estämisen rahoittamisesta 2017, chapter 2 section 3.)

When preparing as risk assessment, the notifier must consider the size and scope of the operation and character. Taking in to account the above, the reporting party must have the required procedure, operating principles, and supervision to effectively manage and reduce the risks of money laundering and terrorist financing. Operating principles, procedures and supervision must include at least the development of internal operating principles, procedures and supervision, and an internal audit, if this is justified considering the nature and size of reporting obligation. (Laki rahanpesun ja terrorismin estämisen rahoittamisesta 2017, chapter 2 section 3.)

The task of the risk value is to make the reporting party understand why the reporting party's activities are within the scope of the anti-money laundering and terrorist financing legislation. The risk assessment helps the reporting entity to define its own procedures, operating principles, and supervision in such a way that they are proportionate to the risk of money laundering and terrorist financing affecting the reporting entity's activities. The purpose of the risk assessment is to avoid unnecessary procedures when there is a small risk and accordingly, to make sure that the procedures are sufficient when the risk is high. (Risk assessment.)

7 Know Your Customer (KYC)

7.1 Responsibilities of knowing the customer

In customer relations, the reporting party must consider geographical areas, risks related to money laundering and terrorist financing to countries, services, transactions, and distribution channels. This is called a risk-based assessment. The person obliged to report must be able to demonstrate to the supervisory or supervisory authority that in that case operating procedures related to knowing the customer and continuous monitoring prescribed by law are valid in terms of the risk of money laundering and terrorist financing. If the reporting party is not able to fulfil the regulations required in this law to know the customer, then it is not possible to establish a customer relationship, conduct business or maintain a business relationship. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 3 section 1.)

Among other things, banks must be able to identify their customer's activities and backgrounds as widely as the customer relationship requires. Knowing the customer is also the fact that the service provider is aware of whose funds and on whose behalf, transactions are made. In addition to the Prevention of Money Laundering and Terrorist Financing Act, the following laws oblige you to know the customer:

- The Insurance Company Act
- The Investment Fund Act
- The Payment Institution Act
- The Act on the Share-of-Value System
- The Act on Alternative Fund Managers
- The Act on Credit Institution Operations. (Customer due diligence and customer identification 2020.)

The criteria for the duty to know the customer can also be met by an operator responsible for reporting obligations that has received a business license or registered in an EEA state (European Economic Area), if the operator is established in a state whose system for preventing and investigating money laundering and

terrorist financing does not, according to the assessment of the European Union Commission, pose a major risk to the internal market of European Union. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 3 section 7.)

7.2 Simplified customer due diligence

If the reporting party assesses that the risk of money laundering and terrorist financing related to the customer relationship or individual transaction is low, a simplified procedure for getting to know the customer can then be followed. In order to detect unusual and exceptional business activity, the reporting party must monitor the customer sufficiently in relation to the quality and scope of the customer's activities, the permanence and duration of the customer relationship. This ensures that the customer's activities correspond to the information and experience of the reporting party. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 3 section 8 - 4.)

The reporting party must maintain and identify accurate, sufficient, and up-to-date information about the customer's actual beneficiaries and, if necessary, verify their identity. To the extent of the risks of money laundering and terrorist financing, and in an appropriate manner, the reporting party must find out whether someone else exercises control over the customer. (Laki rahanpesun ja terrorismin estämisestä 2017, chapter 3 section 6.) The reporting party also has a statutory obligation to contact the customer during the calendar year to check the necessary information regarding the actual beneficiaries. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 3 section 1.)

7.3 Enhanced customer due diligence

The reporting party must use an enhanced customer familiarization procedure, if on the basis of the risk assessment, it can be assessed in the manner prescribed in Chapter 2, Section 3 of the Money Laundering and Terrorist Financing Act, that a single transaction or customer relationship involves a higher than usual risk of money laundering and terrorist financing. The enhanced due diligence procedure can also be used if the customer or business is linked to a state whose money laundering and terrorist financing prevention and investigation system, according

to the Commission's assessment, poses a significant risk to the EU international market or complies with international obligations. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 3 section 10.)

The customer must be identified remotely if the customer is not present for identification and identity verification. This reduces the risk of money laundering and terrorist financing. The customer's identity can be verified by acquiring remote identification additional information or documents from a reliable source. Another way to verify the customer's identity remotely is to ensure that the payment related to the transaction comes from the credit institution's account or the payment is paid to an account opened in the customer's name. The third way to verify the customer's identity in remote identification is to use electronic identification device, which is regulated by law for strong electronic identification and electronic trust services, or with a certificate that accepts an electronic signature. The customer can also be identified remotely by using secure and evidence-based electronic identification technology. (Laki rahanpesun ja terrorismin estämisestä 2017, chapter 3 section 11.)

Financial and Credit institutions can enter into an agreement with a financial or credit institution outside the EEA (European Economic Area) to handle payments and other assignments. This is called a correspondent relationship, but before a correspondent relationship can be established, the financial or credit institution must obtain the necessary information from the counterparty financial or credit institution. The counterparty's financial or credit institution must be assessed for its methods of preventing money laundering and terrorist financing, as well as its reputation and quality of supervision. The top management of the finance or credit institution approves the correspondent relationship, and the agreement is agreed to fulfil the customer-knowing obligations and to provide the relevant information to the counterparty finance or credit institution if they request it. A financial or credit institution may not start or continue a correspondent relationship with non-operating bank. They may also not start an agreement with banks whose accounts are used in the non-operating banks. (laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 3 section 12.)

The reporting party must be aware of whether the customer or the customer's actual beneficiary or whether she/he was politically influential person, a politically influential person's family member or a politically influential person's business partner. The customer's political influence must be determined whenever the reporting party assesses, based on the risk assessment, that an individual transaction or customer relationship involves a higher than usual risk of money laundering and terrorist financing. A politically influential customer or a customer's beneficial owner or a family member of a person who is known to be a business partner of a politically influential person, the customer relationship is approved by the senior management of the reporting entity. Those obliged to report must obtain from such a person an explanation of such wealth and its origin, which is related to the transaction or customer relationship in question and enhanced continuous monitoring of the customer relationship must be organized. A person who has not held a significant public position for at least a year is no longer a politically influential person according to money laundering legislation. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 3 section 13a.)

When the reporting party makes payments or transactions to countries outside of Europe and, according to the Commission's assessment, to countries with a high risk of money laundering and terrorist financing, then the reporting party must obtain additional information about the customer and the actual beneficiary, the business relationship to be established, the origin of the funds and the reasons for the transaction. The reporting party must constantly monitor the customer in an enhanced manner by increasing the number of inspections and timings as well as a selection of transactions that should be investigated more widely. The reporting party obtained the approval of customer relationship from senior management. According to its risk assessment, the reporting party must, if necessary, apply enhanced customer familiarization procedures, use necessary transaction reporting methods, limit customer relationships and transactions in high-risk countries. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 3 section 13.)

8 Customer due diligence

The reporting party must identify and verify the identity of its customer before establishing a new customer relationship, or at latest when the customer has gained control over the funds, other assets, or before the transaction in question has been completed. When establishing a customer relationship with a legal entity or a foreign express trust referred to in Article 3 section 7 d of the Money Laundering Directive, it must be ensured that their real beneficiary is entered in the register used to identify and verify the identity of the customer subject to notification. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2019, chapter 3 section 2.)

8.1 Customer identification and authentication obligations

The customer's identity must be identified and verified if a single transaction or interconnected transaction total at least ten thousand euros and it is an occasional customer or the amount of the transfer of funds exceed one thousand euros. The customer's identity must also be recognized when the amount of the sale or the amount of related transaction is at least ten thousand euros in cash. The reporting party has the obligation to identify and verify the identity of its customer also when it is a question of a suspicious transaction, or the reporting party suspects that the purpose of using the funds included in the transaction is the financing of terrorism or its attempt. The reporting party may re-verify the identity of a previously authenticated customer if She/He doubts the adequacy and reliability of the customer's authentication information. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 3 section 2.)

If the customer has a representative, then the reporting party must also identify and authenticate the customer's representative and ensure the representative's right to act on behalf of the customer. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 3 section 2.) A customer subject to notification can also be identified by another reporting entity or another reliable partner. Documentation related to the customer relationship must be delivered to the reporting party or must be available to the reporting party without delay. (Customer due diligence 2018.)

8.2 Retention of customer due diligence data

After the end of the customer relationship, the reporting party must keep information related to knowing the customer in a reliable manner for at least five years after the end of the customer relationship. The customer's personal information must also be kept for at least five years after the end of the transaction if the transaction or related transactions are at least ten thousand euros and the customer's customership is occasional or the transfer of the customer's funds is a total of ten thousand euros. (laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 3 section 3.) If the customer is identified remotely, then the information about the sources and procedures used in the authentication must be kept. (Customer due diligence 2018.)

The reporting party must keep the customer's name, social security number, date of birth, address, bank or payment account number, account opening and closing date and the name of the account owner or user right holder. The name of the renter and the length of the rental period must be kept of the customer who rents the safe. Other identifying information related to the account or safe deposit box may be stored about the customer who owns a bank or payment account or the customer who rents a safe deposit box, if it is necessary to store the data considering the nature of the activity subject to notification and there is no legal obstacle to obtaining the data. The number of the document used to verify the customer's identity, -name or any other identifying information and its issuer must be kept. The necessary information acquired in order to fulfil the enhanced duty to know must be kept about the politically influential customer. If a politically influential customer has a representative, then the reporting party must keep the representative's name, social security number and date of birth. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 3 section 3.)

If the customer is a legal person, the reporting party must keep the following information about legal person:

- Full name
- Articles of association
- Date of registration
- Registration number

- Registration authority
- Industry
- Full names, nationalities, and dates of birth of the members of the decision-making board
- Names, date of birth, Finnish social security number or, if not available, citizenship of the actual beneficiaries.

If necessary, a more detailed description of the beneficial owner's control and ownership structure can be kept if the beneficial owners of the legal entity have not been identified. If only some of the members of the legal entity's decision-making body are entered in the register because the legal entity is subject to other legislation, personal information can be stored if the reporting party justifies its retention with its risk assessment. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 3 section 3.)

The European Parliament and the Council have issued regulation (EU) No. 910/2014 on the electronic transfer of payment transaction in trust services in the internal market and the repeal of Directive 199/93 EC (European Community), according to which the person obliged to report must keep the identification data obtained through remote or electronic identification functions and the national data of relevant or trust services that belong to them identification or approval regulated by authorities, as well as the prescribed electronic identification methods. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2019, chapter 3 section 3.) In addition to the name, date of birth and personal identification number, information about the customer's nationality and her/his travel document must be kept in the contact information of a foreign customer who does not have a Finnish personal identification number. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 3 section 3.)

In addition to keeping information about the customer's identity, the reporter party must inform its customers that their identity information or other information may be used to investigate, reveal, and combat money laundering and terrorist financing. With this, the proceeds of crime or the property belonging to money laundering and terrorist financing can be investigated. The customer's personal information and contact information may not be used for any purpose other than to

prevent money laundering and terrorist financing if the information has been acquired only for this purpose. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, section 3 section 3.)

9 Administrative sanctions

Administrative sanctions are stipulated in the fourth chapter of the Financial Supervisory Authority Act. The contents of the chapter are discussed in the following subsections.

The Financial Supervisory Authority has imposed public warnings, administrative fines and penalty payments as follows in the year 2012-2022H1.

Table 2. requests for police investigation and administrative sanctions 2012 – 2022H1. (Sanctions, requests for investigation and cases of securities market inspections 2022.)

	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	6/2022
Public warning	3	2	2	-	2	5	3	1	1	1	2
Administrative fine	14	6	2	19	2	3	-	-	1	-	-
Penalty payment	-	-	1	-	3	4	3	5	2	2	3

9.1 Public warning

Section 39 of the Financial Supervisory Authority Act provides for a public warning. According to it, a public warning can be ordered in situations where an administrative fine or penalty payment is not involved, and provided that the matter does not give rise to more severe measures. A public warning can also be given to the person being supervised if they intentionally or negligently act in violation of the terms of their business license or the rules governing their activities. A public warning may not be given if there is none made within five years from the time the breach or neglect occurred. (Administrative sanctions 2022.)

9.2 Administrative fine

The supervisory authority of the administrative fine can order a person subject to notification who, due to carelessness or wilfully, violates or neglects the obligations set by the Law on the Prevention of Money Laundering and Financing of

terrorism. The Financial Supervisory Authority is entitled to issue an administrative fine to a supervised person who, due to negligence or wilfully, does not document the necessary information regarding the payer or the payee in accordance with the fourth, fifth and sixth articles of the Payer's information regulations. (Laki rahanpesun ja terrorismin estämisestä 2017, chapter 8 section 1.)

Administrative fine may be received by a person liable to report who systematically, repeatedly, or seriously neglects his duty to ensure the storage of data in violation of the Payer's Information regulation 16 and does not implement effective risk-based procedures and acts on the basis of it in violation of articles 8 or 12 of the said regulation. If the reporting party has seriously neglected the obligation laid down in Article 11 of the aforementioned regulation, where the reporting party should establish procedures to detect information about the payer or payee, or the obligation stipulated in Article 12 of this same regulation to establish risk-based procedures for fund transfers, the related information of which is incomplete regarding execution, suspension, or rejection. (Laki rahanpesun ja terrorismin estämisestä 2017, chapter 8 section 1.)

For legal person, the administrative fine can be a minimum of 5,00 euros and a maximum of 100,00 euros, and for a natural person a minimum of 500 euros and a maximum of 10,000 euros. The amount of the administrative fine is based on the supervisory authority's overall assessment of the seriousness of the violation. When assessing the amount of the fine, the supervisory authority must take in to account the scope, quality, and duration of the procedure. The person who received a fine must pay the said sanction to the Finnish State. If the negligence or act of the reporting party can be considered particularly objectionable, a penalty payment can be imposed on the person being supervised instead of an administrative fine. (Administrative sanctions 2022.)

In the press release published in August 2022, it has been announced that the Financial Supervisory Authority has imposed a 60 000 euros administrative fine on S-Pankki. In the spring of 2021, the Financial Supervisory Authority had discovered that the number and total nominal value of derivative contracts reported to S-bank's trade data registers were suspiciously small compared to the scope of the bank's business. According to the statement received from the bank. it had

mistakenly assumed that the settlement broker it used from June 2019 would report derivative contracts to the trade data register on behalf of the bank. However, it would have been the bank's responsibility to ensure that the information is reported in accordance with the regulations. The amount of the administrative fine of 60,000 euros is based on the overall assessment, which was mentioned above. (S-Pankki Oyj:lle rikemaksu laiminlyönneistä johdannaissopimuksia koskevassa raportoinnissa 2022.)

9.3 Penalty payment

The supervisory authority can impose a penalty payment on a supervised person who, through serious negligence or intentionally, systematically, or repeatedly neglect or violates the same obligations that are a prerequisite for the imposition of an administrative fine. The supervisory authority cannot impose a penalty payment on a natural person for negligence or an act that is punishable by law. If the supervisory authority assesses the act or omission as harmful enough and the perpetrator guilty, considering the benefit obtained from the act and other aspects related to the act or omission, this may impose a penalty payment and leave the matter unreported to the preliminary investigation authority. In addition to the penalty payment imposed on the legal entity, a penalty payment may also be imposed on a person belonging to the management of the legal entity who is responsible for the act or omission. The condition for imposing such a penalty payment is that the person in question has influenced the act or omission in a significant way. (Laki Finanssivalvonnasta 2008.)

The size of the penalty payment is based on the supervisory authority's overall assessment, which must consider the scope, quality, duration of the procedure and the benefit achieved, and damage caused by it, if they can be defined, as well as the possible effects of the procedure on the stability of the financial system. The size of the payment is based on the financial status of the subject and whether the perpetrator has cooperated with the Financial Supervisory Authority to clarify the matter or prevent the violation from recurring. The person who received the penalty payment must also pay the penalty to the Finnish state. (Administrative sanctions 2022.)

9.4 Failure to impose an administrative sanction

The supervisory authority decides not to issue a public warning or fine if the reporting party takes the necessary measures on its own initiative to correct the violations it has committed. However, measures must be taken as soon as the violations have been detected and after that the errors have been reported to the competent supervisory authority without delay. This can decide not to issue a public warning or fine even when the violation or public warning can be considered minor or the imposition of a fine can otherwise be considered clearly unreasonable. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 8 section 6.)

If the person liable to report is suspected of a violation in a preliminary investigation, prosecution or in a criminal case open in court, the supervisory authority cannot impose an administrative fine or a penalty payment on the person liable to report. Nor can the order be given to a reporting party who has been given a final verdict for their violations. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 2017, chapter 8 section 6.)

10 Conclusion

The aim of the thesis was to investigate the prevention of money laundering and terrorist financing in general in Finland, but the work has mainly focused on the banking sector. The purpose of the work is to give the reader a comprehensive understanding of the fight against money laundering and terrorism in the banking sector.

The most typical form of money laundering is smuggling and recycling money from bank accounts in different countries to others. It is also common for funds obtained from money laundering to be broken into smaller amounts so that they do not attract too much attention from the reporting parties and authorities. Money laundering is monitored by reporting parties. The law obliges reporting entities to know their customer and to identify their customers and their reasons for products and services in many different ways. Money laundering is combat-ed by the actions of the Financial Intelligence unit, to which reporting parties can report suspicious transactions. The Financial Intelligence unit work together with other authorities. Prevention is the best way to break the cycle of crime and eradicate the infiltration of organized crime close to normal transaction

In recent years, more and more cases have come to light where criminals try to launder money by systematically exploiting the weaknesses of various banking systems. Normal foreign trade has been exploited and the origin of the funds has been obscured by complex business arrangements. FATF's country inspections have also found that there are differences between countries in the regulation and supervision of money laundering prevention. According to the former head of the Financial Supervisory Authority, Anneli Tuominen, there is a clear need in the European Union to establish a joint anti-money laundering supervisory body, which would ensure uniform supervisory practices, high quality supervision and an undivided flow of information between EU countries. The fight against money laundering is done at the national level in Europe and the supervisory authorities already cooperate, but the cooperation is not sufficient if it is based on voluntariness. In order to make anti-money laundering supervision more effective, it is planned to increase the powers of the European Banking Authority, as well as to increase the cooperation and exchange of information between the European

Central Bank and other national anti-money laundering supervisors. (Financial Supervisory Authority strengthens anti-money laundering supervision – European supervision will also be enhanced 2019.)

Based on the above, it can be stated that the fight against money laundering and terrorist financing is not without gaps. Today, banking systems are electronic, and all activity remains on them. However, criminals always come up with new ways to carry out crimes related to money laundering and terrorism, which makes the work of the authorities challenging. Simple ways of money laundering, such as depositing large sums into a bank account or several bank accounts but different persons, are becoming history. These days criminals try to find gaps in financial systems and use them to commit a crime, for example by conducting business activities that allow so-called dirty money to pass through the company and look like it was legally earned, or by using virtual currencies in money laundering, the origin of which is difficult for the authorities to trace. Country-specific borders and the different measures taken by states to prevent and combat money laundering and terrorist financing is a significant factor. The European Union has imposed obligations on its member states in terms of combating money laundering and terrorist financing, but the member states can also influence the matter themselves by adjusting their legislation to make supervision more effective. This poses a certain risk that the supervision and procedures are not in uniform in all EU countries, which in turn makes it easier for criminals to commit the crime, for example by using shell banks or shell accounts for money transfers: shell corporation is a company or corporation, in this case a bank, that has no active business operations or assets. These corporations are not certainly illegal but might be used illegitimately, such as to disguise business ownership from law enforcement or the public. (Investopedia 2022.)

In the future, in terms of combating money laundering and terrorist financing, it will be important that supervision and methods are of high quality at an international level, in which case it would be more difficult for criminals to find gaps in financial systems and engage in crime. All in all, prevention of money laundering and the financing of terrorism is topical, and the crimes related to the topic in question have a great impact on society. In the future, banks should pay attention to knowing, identifying, and monitoring customers, and banks should unify their

policies so that there is no opportunity for crime. In addition to updating risk management methods, banks should spend time training their staff. Guides made on the subject will be even more necessary for banks that are obliged to report, because banks and their employees are the first to encounter money laundering and terrorist financing. The topic guides ate especially important for smaller banks and their employees, who may not have the same resources to implement anti-money laundering and terrorist financing procedures as larger banks.

Prevention and control of money laundering definitely require continuous work, and in order to break the cycle of crime, it is absolutely important to intervene in money laundering at an early stage. Combating money laundering and the financing of terrorism is a broad and constantly changing topic, which is why it is important to study the topic, summarize it and highlight the relevant points for banks, so that supervision can be carried out exactly as required by legislation and money laundering and terrorist financing can be eradicated. In the future, the fight against money laundering and terrorist financing legislation will become more effective and with the development of technology and the ways in which crimes are committed become more complex, it is good to do further research on the subject. Money laundering is a very diverse and broad topic, which gives the opportunity to study it continuously.

10.1 Evaluation

The thesis has been written in the fall of 2022. The initial plan took the most time when thinking about the research problem and the scope of work. The topic of the work changed a few times before the writing phase and also during the initial phase of writing. Delimiting the work turned out to be challenging at first and the most challenging part of writing the work was bringing out the key issues in terms of the topic, because due to the topicality of the topic, many sources were found for it. Finding cases and information suitable for the topic to be used in the thesis was a bit difficult as some of them were from few years ago so, finding a similar but more recent case for the thesis was challenging as there was not as much information and articles about these cases yet. In the thesis, documents published by different authorities were used in a variety of ways, which helped in writing the thesis. With the help of these, the goal of the thesis was succeeded

as the aim of the thesis was to give the reader an overall picture of money laundering and terrorist financing and the fight against them. The topic was chosen because of the writers' own interest, experience, and familiarity to the topic. What helped to build the thesis topics and find information for it was through the knowledge gained from the work place. Eventually the topic was broader than thought and it did cause some difficulties at the beginning and at some parts during the writing. Writing the thesis did help to gain more information and knowledge about the topic. Although planning and writing the thesis was difficult and time-consuming, the end results of the thesis was nevertheless successful.

11 REFERENCES

Administrative sanctions. Updated 7.4.2022. Finanssivalvonta. https://www.finanssivalvonta.fi/en/about-the-fin-fsa/powers-and-funding/powers-and-authority/administrative-sanctions/. Read on 27.10.2022

Customer due diligence. Updated 15.12.2018. Finanssivalvonta. https://www.finanssivalvonta.fi/en/insurance/prevention-of-money-laundering-and-terrorist-financing/customer-due-diligence/. Read 27.10.2022

Customer due dilingence and customer identification. Updated 28.02.2020. Finanssivalvonta. https://www.finanssivalvonta.fi/en/Consumer-protection/customer-due-diligence-and-customer-identification/. Read on 26.10.2022

Euroopan parlamentin ja neuvoston asetus (EU) 2015/847. Euroopan unionin virallinen lehti. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32015R0847&from=NL. Read on 18.10.2022.

FATF N.d. Terrorist Financing. https://www.fatf-gafi.org/publications/fatfgeneral/documents/terroristfinancing.html. Read 7.10.2022

FATF N.d. Who we are. Read on 10.10.2022. https://www.fatf-gafi.org/about/whoweare/.

FATF N.d. What we do. Read on 10.10.2022. https://www.fatf-gafi.org/about/whoweare/.

FATF N.d. Members and Observers. Read on 10.10.2022. https://www.fatf-gafi.org/about/membersandobservers/.

Finanssivalvonta. Tietoa Finanssivalvonnasta. https://www.finanssivalvonta.fi/finanssivalvonta/.

Financial Supervisory Authority strengthens anti-money laundering supervision – European supervision will also be enhanced 2019. Finanssivalvonta 16.4.2019. https://www.finanssivalvonta.fi/en/publications-and-press-releases/Press-release/2019/financial-supervisory-authority-strengthens-anti-money-laundering-supervision--european-supervision-will-also-be-enhanced/. Read on 30.10.2022

Hänninen, J. 2022. Analyysi: Nordea ummisti silmänsä rahanpesulta vuosikausia – jättimäinen sisäinen selvitys tehtiin vasta, kun pankki luopui Baltian toimistaan. Yle Uutiset 13.6.2022. Read 24.09.2022. https://yle.fi/uutiset/3-12475350

Obligated entities. Rahanpesu.fi. https://rahanpesu.fi/en/obliged-entities. Read on 23.10.2022.

International Sanctions. Ministry for Foreign Affairs in Finland. https://um.fi/international-sanctions. Read on 11.10.2022.

Kenton, W. 2022. What is a Shell corporation? How It's used, examples and legality.17.07.2022 Investopedia. https://www.investopedia.com/terms/s/shell-corporation.asp.

Jass. 2019.The History of money laundering. Kyc-Chain 25.4.2019. https://kyc-chain.com/the-history-of-money-laundering/. Read on 10.9.2022.

International economic sanctions and domestic freezing decisions. 6.9.2018. Finanssivalvonta. https://www.finanssivalvonta.fi/paaomamarkkinat/rahanpesun-estaminen/terrorismin-rahoittamisen-estaminen/. Read on 18.10.2022

Kansainvälisten pakotteiden täytäntoonpano Suomessa. 10.3.2022. Ulosottolaitos. https://www.ulosottolaitos.fi/fi/index/ulosottolaitos/ajankohtaista/verkkouutisetjatiedotteet/2022/kansainvalistenpakotteidentaytantoonpanosuomessa.html. Read on 18.10.2022.

Kananen, J. 2009. Vientikaupan maksuliikenne ja rahoitus. Rahanpesu. Tampereen Yliopistopaino Oy- Juvenes print.

Lainmuutokset tehostavat rahanpesun ja terrorismin rahoittamisen estämistä 13.1.2022. Valtioneuvosto. https://valtioneuvosto.fi/-/10623/lainmuutokset-tehostavat-rahanpesun-ja-terrorismin-rahoittamisen-estamista. Read on 18.10.2022.

Lainsäädäntö – rahanpesun ja terrorismin rahoittamisen estäminen. Rahanpesu.fi. https://rahanpesu.fi/lainsaadanto. Read on 17.10.2022

Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2017/20170444#L4. Read on 18.10.2022

Laki rahanpesun ja terrorismin rahoittamisen estämisestä 26.4.2019/573. Finlex. https://www.finlex.fi/fi/laki/alkup/2019/20190573. Luettu 27.10.2022

Laki varojen jäädyttämisestä terrorismin torjumiseksi. 3.5.2013/325. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2013/20130325?search%5Btype%5D=pika&search%5Bpika%5D=Laki%20varojen%20j%C3%A4%C3%A4dytt%C3%A4misest%C3%A4. Read on 18.10.2022

The Act on the Financial Supervisory Authority 19.12.2008/878. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2008/20080878#a878-2008. read on 27.10.2022

Malkoc, Timo 2019. Yritysasiakkaan tilin sulkeminen voi liittyä pankin vastuuseen rahanpesun torjunnasta. Kauppalehti. https://www.kauppalehti.fi/uutiset/yritysasiakkaan-tilin-sulkeminen-voi-liittya-pankin-vastuuseen-rahanpesun-torjunnasta-fivan-rahanpesuyksikon-paal-likko-ulkopuolista-varmistusta-ei-ole/ad215222-df36-4329-9e42-d1d23f42d3b3. Read on 26.10.2022

Risk assessment. Updated 30.04.2021. Finanssivalvonta. https://www.finanssivalvonta.fi/en/prevention-of-money-laundering-and-terrorist-financing/riskiarvio/. Read on 26.10.2022

Obliged entities. Rahanpesu.fi. https://rahanpesu.fi/en/obliged-entities. Read on 26.10.2022

Obligation to obtain information and to report. 07.04.2021. Finanssivalvonta. https://www.finanssivalvonta.fi/en/banks/prevention-of-money-laundering-and-terrorist-financing/obligation-to-obtain-information-and-to-report/. Read on 23.10.2022

Sanctions, requests for investigation and cases of securities market inspections. Edited 26.8.2022. Finanssivalvonta. https://www.finanssivalvonta.fi/en/statistics/Sanctions-requests-for-investigation-and-cases-of-securities-market-inspections/. Read 27.10.2022

ST Paul's Chambers. 2021. Stages of Money Laundering Explained. Released 21.02.2021. ST Paul's Chambers. Read on 12.09.2022. https://www.stpaulschambers.com/stages-of-money-laundering-explained/

Finanssivalvonta 25.8.2022. Lehdistötiedote, S-Pankki Oyj:lle rikemaksu laiminlyönneistä johdannaissopimuksia koskevassa raportoinnissa. https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/lehdistotiedotteet/2022/s-pankki-oyjlle-rikemaksu-laiminlyonneista-johdannaissopimuksia-koskevassa-raportoinnissa/. Read on 30.10.2022

Terrorist Finance Tracking Program. U.S Department Of The Treasury. https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/terrorist-finance-tracking-program-tftp. Read on 11.10.2022.

Terrorist financing. Rahanpesu.fi. https://rahanpesu.fi/terrorismin-rahoittaminen. Read on 26.09.2022

Rahanpesun torjunta. Poliisi. https://poliisi.fi/rahanpesu Read on 26.09.2022

Rahanpesu. Poliisi. https://poliisi.fi/rahanpesu. Read on 06.09.2022

Rahanpesun valvontarekisteri. Aluehallintovirasto. https://avi.fi/asioi/henkiloasiakas/luvat-ilmoitukset-ja-hakemukset/raha-ja-omaisuus/rahanpesulain-valvonta. Read on 23.10.2022

Rahanpesu. Rahanpesu.fi. https://rahanpesu.fi/rahanpesu. Read on 06.09.2022

Rahanpesun ja terrorismin rahoittamisen estäminen. Finanssivalvonta. https://www.finanssivalvonta.fi/rahanpesun-estaminen/. Read 26.9.2022

Rahanpesun selvittelykeskuksen puolivuosikatsaus 2022. Keskusrikospoliisi. https://poliisi.fi/documents/25235045/67733116/Rahanpesun-selvittelykeskus-puolivuosikatsaus-2022.pdf/e6b6d0d7-8ae4-d6e8-53e5-c87f3899ebcc/Rahanpesun-selvittelykeskus-puolivuosikatsaus-2022.pdf?t=1659075148282. Read 30.09.2022

Rahanpesun selvittelykeskus vuosikertomus 2021. Poliisi. https://poliisi.fi/documents/25235045/67733116/Vuosikertomus-Rahanpesun-selvittelykeskus-2021.pdf/0772e42d-776d-992c-96cc-3a22d3e0f365/Vuosikertomus-Rahanpesun-selvittelykeskus-2021.pdf?t=1654673945126. Read 08.10.2022

Laki Rahanpesun Selvittelykeskuksesta 28.6.2017/445. Finlex. https://www.finlex.fi/fi/laki/ajantasa/2017/20170445. Read on 27.10.2022