MINISTRY OF FINANCE

National risk assessment of money laundering and terrorist financing 2021

Financial Markets

Publications of the Ministry of Finance – 2022:41

Publications of the Ministry of Finance 2022:41

National risk assessment of money laundering and terrorist financing 2021

Essi Isoaho, Ida-Ellen Kaski

Ministry of Finance Helsinki 2022

Publication distribution

Institutional Repository for the Government of Finland Valto

julkaisut.valtioneuvosto.fi

Publication sale

Online bookstore of the Finnish Government

vnjulkaisumyynti.fi

Ministry of Finance

ISBN pdf: 978-952-367-267-3
ISSN pdf: 1797-9714

Layout: Government Administration Department, Publications

Helsinki 2022 Finland

Description sheet

30 May 2022

National risk assessment of money laundering and terrorist financing 2021

Publications of the Ministry of Finance 2022:41		**Subject**	Financial Markets
Publisher	Ministry of Finance		
Authors	Essi Isoaho, Ida-Ellen Kaski		
Editor			
Group Author			
Language	English	**Pages**	174

Abstract

The preparation of the national risk assessment of money laundering and terrorist financing 2021 was coordinated by the Ministry of Finance and the Ministry of the Interior. The document describes the threats, vulnerabilities and risks arising from money laundering and terrorist financing in all sectors of obliged entities and in the activities of non-profit organisations (NPO sector). The risk assessment also examines money laundering and terrorist financing risks in relation to specific phenomena.

The national action plan for the risk assessment of money laundering and terrorist financing has been prepared in conjunction with the risk assessment. The action plan presents the measures designed to mitigate the risks identified in the risk assessment. The risk assessment and the action plan reflect the approach to money laundering and terrorist financing risks in Finland and the means to control them.

Keywords	money laundering, terrorism, economic crime, risks, risk assessment		
ISBN PDF	978-952-367-267-3	**ISSN PDF**	1797-9714
ISBN printed		**ISSN printed**	
Reference number		**Project number**	VM018:00/2020
URN address	https://urn.fi/URN:ISBN:978-952-367-267-3		

Kuvailulehti
30.5.2022

Kansallinen rahanpesun ja terrorismin rahoittamisen riskiarvio 2021

Valtiovarainministeriön julkaisuja 2022:41		**Teema**	Rahoitusmarkkinat
Julkaisija	Valtiovarainministeriö		
Tekijä/t **Toimittaja/t** **Yhteisötekijä**	Essi Isoaho, Ida-Ellen Kaski		
Kieli	englanti	**Sivumäärä**	174

Tiivistelmä

Kansallinen rahanpesun ja terrorismin rahoittamisen riskiarvio 2021 on laadittu valtiovarainministeriön ja sisäministeriön koordinoimana. Riskiarviossa kuvataan rahanpesun ja terrorismin rahoittamisen uhkia, haavoittuvuuksia ja riskejä kaikilla ilmoitusvelvollissektoreilla sekä voittoa tavoittelemattomien organisaatioiden (NPO-sektorin) toiminnassa. Lisäksi riskiarviossa tarkastellaan rahanpesun ja terrorismin rahoittamisen riskejä liittyen valittuihin ilmiöihin.

Riskiarvion yhteydessä on laadittu kansallinen rahanpesun ja terrorismin rahoittamisen riskiarvion toimintasuunnitelma. Toimintasuunnitelmassa esitellään ne toimenpiteet, joilla riskiarviossa havaittuja riskejä pyritään pienentämään. Riskiarvio ja toimintasuunnitelma muodostavat kokonaisuuden, joka kuvastaa Suomen kansallista ymmärrystä rahanpesun ja terrorismin rahoittamisen riskeistä ja niiden hallintakeinoista.

Asiasanat	rahanpesu, terrorismi, talousrikokset, riskit, riskinarviointi		
ISBN PDF	978-952-367-267-3	**ISSN PDF**	1797-9714
ISBN painettu		**ISSN painettu**	
Asianumero		**Hankenumero**	VM018:00/2020
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-367-267-3		

Presentationsblad

30.5.2022

Nationell riskbedömning av penningtvätt och finansiering av terrorism 2021

Finansministeriets publikationer 2022:41		**Tema**	Finansmarknaden
Utgivare	Finansministeriet		
Författare	Essi Isoaho, Ida-Ellen Kaski		
Redigerare			
Utarbetad av			
Språk	engelska	**Sidantal**	174

Referat

Den nationella riskbedömningen för penningtvätt och finansiering av terrorism 2021 har sammanställts under samordning av finansministeriet och inrikesministeriet. I riskbedömningen redogörs för hot, sårbarheter och risker som hänför sig till penningtvätt och finansiering av terrorism inom de rapporteringsskyldiga sektorerna och inom ideella organisationer (NPO-sektorn). Riskerna med penningtvätt och finansiering av terrorism i samband med vissa utvalda fenomen tas också upp.

En nationell handlingsplan för riskbedömningen av penningtvätt och finansiering av terrorism har utarbetats i samband med riskbedömningen. I handlingsplanen beskrivs de åtgärder som syftar till att reducera de risker som identifierats i riskbedömningen. Riskbedömningen tillsammans med handlingsplanen avspeglar Finlands nationella insikter i riskerna med penningtvätt och terrorfinansiering och hur de hanteras.

Nyckelord	penningtvätt, terrorism, ekonomiska brott, risker, riskbedömning		
ISBN PDF	978-952-367-267-3	**ISSN PDF**	1797-9714
ISBN tryckt		**ISSN tryckt**	
Ärendenummer		**Projektnummer**	VM018:00/2020
URN-adress	https://urn.fi/URN:ISBN:978-952-367-267-3		

Contents

Abbreviations 9

1 General part 10
1.1 Abstract 10
1.2 Money laundering and terrorist financing – risk assessment and concepts 11
1.2.1 Purpose of the risk assessment 11
1.2.2 Structure of the risk assessment 12
1.2.3 Risk formation 13
1.3 Money laundering and terrorist financing 14
1.3.1 Money laundering 14
1.3.2 Terrorist financing 17
1.4 Combating money laundering and terrorist financing in Finland 18
1.4.1 Structure of the preventive work 18
1.4.2 Supervisory authorities and the registers maintained by supervisory authorities 20
1.4.3 Resources allocated to the prevention of money laundering and terrorist financing 23
1.4.4 Financial Intelligence Unit 24
1.4.5 Other authorities 25
1.4.6 National FATF steering group and FATF group 26
1.4.7 National cooperation group for preventing money laundering and terrorist financing 26
1.4.8 Public private partnership (PPP) – expert work- ing group comprising the authorities and private sector and dealing with the prevention of money laundering and terrorist financing . 27
1.5 Regulation of preventing money laundering and terrorist financing 28
1.5.1 Supranational actors and regulation 28
1.5.2 National legislation 30

2 Money laundering 33
2.1 Key observations 33
2.2 General factors impacting money laundering risk 35
2.2.1 Money laundering predicate offences 35
2.2.2 Geographical location 42
2.2.3 Customer due diligence 44
2.2.4 Technological development 45
2.3 Insurance companies 47
2.3.1 Operating environment 47
2.3.2 Money laundering risks 48
2.4 Payment service providers (incl. currency exchange and hawalas) 49
2.4.1 Operating environment 49
2.4.2 Money laundering risks 51

2.5 Gambling operators 54
2.5.1 Operating environment 54
2.5.2 Money laundering risks 56
2.6 Credit institutions 58
2.6.1 Operating environment 58
2.6.2 Money laundering risks 59
2.7 Financial institutions, other providers of financial services and debt collectors 61
2.7.1 Operating environment 61
2.7.2 Money laundering risks 64
2.8 Virtual currency providers 67
2.8.1 Operating environment 67
2.8.2 Money laundering risks 68
2.9 Expert services 69
2.9.1 Real estate brokerage agencies and letting agencies 70
2.9.2 Attorneys-at-law and other providers of legal services and tax advisory services or parties providing tax-related support directly or indirectly 72
2.9.3 Bookkeepers and auditors 75
2.9.4 Providers of business services 77
2.9.5 Pawnbrokers 79
2.9.6 Art dealers 80
2.9.7 Goods retailers 82

3 Terrorist financing 84
3.1 Key observations 84
3.2 General factors impacting terrorist financing risk 87
3.2.1 Terrorist financing in the Finnish context 87
3.2.2 Geographical location 88
3.2.3 Technological development 89
3.3 Terrorist financing risk associated with the insurance sector 90
3.4 Terrorist financing risks associated with payment service providers (incl. currency exchange and hawala systems) 91
3.5 Terrorist financing risks associated with gambling operations 94
3.6 Terrorist financing risks associated with credit institutions 95
3.7 Terrorist financing risks associated with financial institutions, other providers of financial services and debt collectors 96
3.8 Terrorist financing risks related to virtual currency providers 98
3.9 Terrorist financing risks associated with expert services 99
3.9.1 Terrorist financing risks associated with real estate brokerage agencies and letting agencies 99
3.9.2 Terrorist financing risks associated with attorneys-at-law, other providers of legal services and tax advisory services 100
3.9.3 Terrorist financing risks associated with bookkeepers and auditors 101
3.9.4 Terrorist financing risks associated with providers of business services 102
3.9.5 Terrorist financing risks associated with pawnbrokers 102
3.9.6 Terrorist financing risks associated with art dealers 102
3.9.7 Terrorist financing risks associated with goods retailers 103

4 Phenomena 104
4.1 Cash 105
4.1.1 Money laundering risks associated with cash 106
4.1.2 Terrorist financing risks associated with cash 108
4.2 Covid-19 pandemic 109
4.2.1 Impacts of the Covid-19 pandemic on money laundering 110
4.2.2 Impacts of the Covid-19 pandemic on terrorist financing 112
4.3 Trafficking in human beings 112
4.3.1 Links between human trafficking and money laundering 114
4.3.2 Links between trafficking in human beings and terrorist financing 115
4.4 Legal persons 116
4.4.1 Money laundering risks related to legal persons 119
4.4.2 Terrorist financing risks related to legal persons 122
4.5 Preventing the proliferation and financing of weapons of mass destruction (counter proliferation financing) 123
4.6 Other international phenomena 125
4.6.1 Professional football and match manipulation 125
4.6.2 Free ports 130
4.6.3 Investor citizenship and residence schemes 130

5 NPO sector 132
5.1 Abstract 132
5.2 NPO risk assessment 134
5.2.1 Purpose and background of the risk assessment 134
5.2.2 Scope of the NPO risk assessment 135
5.3 Definition of an NPO 136
5.3.1 Definition of an NPO in international context 136
5.3.2 Definition of an NPO in the national risk assessment 137
5.4 Finland's NPO sector and its operating environment 138
5.4.1 Administrative environment and national regulation 138
5.4.2 Registered NPOs in Finland 143
5.5 Money laundering and terrorist financing threats facing the NPO sector 146
5.5.1 Terrorist funding threats facing the NPO sector 146
5.5.2 Money laundering risks faced by the NPO sector 150
5.6 Money laundering and terrorist financing vulnerabilities faced by the NPO sector 151
5.6.1 Terrorist financing vulnerabilities faced by the NPO sector 151
5.6.2 Money laundering vulnerabilities facing the NPO sector 157
5.7 Risks facing the NPO sector 157

Sources 159

Appendices 168

ABBREVIATIONS

AML	Anti Money Laundering
CFT	Combating the Financing of Terrorism
DNFBP	Designated Non-Financial Business or Profession
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
ML	Money Laundering
NRA	National Risk Assessment
NPO	Non-profit Organisation
OECD	The Organisation for Economic Co-operation and Development
SNRA	Supranational Risk Assessment
STR	Suspicious Transaction Report
TF	Terrorist Financing
TFR	Terrorist Financing Report

1 General part

Finland's national risk assessment of money laundering and terrorist financing 2021 is the second national risk assessment of the subject prepared in Finland. The preparation of the risk assessment was coordinated by the Ministry of Finance and the Ministry of the Interior. The risk assessment work was steered by a project steering group comprising the coordinating parties, Financial Intelligence Unit and the Finnish Security and Intelligence Service and a larger risk assessment working group comprising the national actors relevant to money laundering and terrorist financing[1]

1.1 Abstract

The key points of the national risk assessment of money laundering and terrorist financing 2021[2] are as follows:

- Many sectors of obliged entities rely too heavily on banks' monitoring systems and as a result, the actors in the sectors do not always adequately establish the background of the customer transactions or the source of the funds. If the funds are from Finnish banks, the parties involved may often trust the ability of the banks to detect suspicious transactions and to establish the source of the funds.
- The view is that there are inadequacies in the sharing of information, especially between obliged entities, which can make it more difficult to detect suspicious transactions. The obliged entities should check such details as the actual holder of the account given by the customer. However, establishing this is hampered by the unclarities concerning the regulation on information sharing.

1 In addition to the representatives of the ministries coordinating the work, the working group also included experts from the following bodies: Ministry of Justice, Ministry for Foreign Affairs, Ministry of Social Affairs and Health, Ministry of Economic Affairs and Employment, Financial Intelligence Unit of the National Bureau of Investigation, Finnish Security and Intelligence Service, National Police Board, Gambling Administration of the National Police Board, Finnish Patent and Registra- tion Office, Finnish Customs, Finnish Tax Administration, Regional State Administrative Agency for Southern Finland, Financial Supervisory Authority, Office of the Prosecutor General and the Finnish Bar Association.

2 The data available by the end of February 2021 has been considered in the risk assessment.

- Identifying the phenomenon of terrorist financing is difficult, which significantly impacts the actors' ability to detect suspicious activities.
- Hawala operators can be considered as the highest-risk actors in terms of money laundering and terrorist financing. In addition to Hawalas, virtual currency providers are also in the highest-risk category in terms of money laundering and terrorist financing.
- As a general risk facing legal persons, it has been noted that different types of front organisation are used in business activities. Moreover, the use of existing companies in general and the hijacking of inactive companies by criminals has been identified as a potential risk scenario.
- With the coronavirus pandemic, different types of fraud have become an increasingly common phenomenon in the criminal operating environment and they are also typical predicate offences of money laundering.

The first national risk assessment of money laundering and terrorist financing was produced as part of the RATERISK project of the Police University College in 2015. The following key observations of this risk assessment can be highlighted for comparison purposes:

- The key money laundering and terrorist financing risks involved real estate investments, transport of cash, front companies, increase in online transactions, online shadow financing markets and segregated accounts.
- Differences between the powers and sanctions available to the supervisory authorities were seen as a key vulnerability in the combating of money laundering and terrorist financing.
- The funds ordered to be forfeited to the State had been modest in relation to the estimated criminal proceeds and funds seized for security.

1.2 Money laundering and terrorist financing – risk assessment and concepts

1.2.1 Purpose of the risk assessment

A national risk assessment of money laundering and terrorist financing is required under the Act on Preventing Money Laundering and Terrorist Financing (444/2017; hereafter the '*Anti-Money Laundering Act*'). The purpose of the national risk assessment is to identify and assess money laundering and terrorist financing risks in different sectors in Finland. It also helps to strengthen the risk-based approach to the matter, to develop the supervision and carrying out of the measures to combat money laundering and terrorist financing and to focus the resources in an effective manner.

The supranational risk assessment (SNRA) prepared by the European Commission must be considered in the national risk assessment.[3] Under the Anti-Money Laundering Act, one purpose of the national risk assessment is to support competent supervisory authorities, the Finnish Bar Association and obliged entities in the preparation of their own risk assessments. According to the European Commission, the supranational risk assessment, the national risk assessments of the Member States and sector-specific risk assessment are equally important and complement each other.[4]

The national risk assessment must be updated on a regular basis.[5] Finland's national risk assessment is updated every two years unless otherwise provided in national or international obligations. The risk assessment updating cycle is not specified by FATF (Financial Action Task Force); however, as the supranational risk assessment of the European Commission is updated every two years, this cycle should also be applied to the national risk assessment. The risk assessment work is evolutive in nature and this second national risk assessment will thus also serve as a basis for future risk assessments both in terms of methodology and in the surveying of information needs.

After the risks have been identified and the risk levels determined, the measures to combat money laundering and terrorist financing should be applied in a manner that is in proportion to the identified risks. FATF and the European Commission require that measures should be taken to mitigate the risks[6] and these measures are listed in the action plan based on the findings of the national risk assessment. The action plan sets out the national-level measures that should be taken to react to identified risks. The action plan primarily details targeted legislative and operational measures to mitigate identified risks.

1.2.2 Structure of the risk assessment

The national risk assessment has five parts. The first part (general part) contains a description of the national and international framework of the risk assessment, legislation and documents guiding the process, risk formation and the purpose of the risk assessment. The second part discusses money laundering risks and the third part the risks of terrorist financing in terms of threats and vulnerabilities. Current phenomena associated with money laundering and terrorist financing are discussed in the fourth part.

3 Under Article 7 of the fourth anti-money laundering directive ((EU) 2015/849), Member States must make use of the findings of the supranational risk assessment when carrying out measures set out in their own national risk assessments.

4 EU SNRA 2019 – Commission Staff Working Document, p. 5.

5 Under Article 7 of the fourth anti-money laundering directive (2015/849), Member States must keep their national risk assessments up to date.

6 FATF 2012—2020, p. 8.

The fifth part discusses the NPO sector[7] in the Finnish context. The methodology used in this risk assessment is described in the appendix at the end of the document.

1.2.3 Risk formation

The risk of money laundering and terrorist financing means the factor combining a threat, vulnerability and consequence. According to the FATF definition:

- **A threat** is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society or the economy. In the ML/TF context this includes criminals, terrorist groups and their facilitators and funds. Money laundering predicate offences can also constitute threats. Threat typically serves as an essential starting point in developing an understanding of money laundering/terrorist financing risk.[8]
- **Vulnerabilities** comprise things that can be exploited by the threat or that may support or facilitate its activities. In the risk assessment context, looking at vulnerabilities means focusing on, for example, the factors that represent weaknesses in AML/CFT systems or controls or certain features of a country. Vulnerabilities may also include the features of a particular sector, a product or type of service that make them attractive for money laundering or terrorist financing purposes.[9]
- **Consequence** refers to the impact or harm that money laundering and terrorist financing may cause. The consequences include the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally. The consequences of money laundering or terrorist financing may be short or long term in nature.[10]

A risk can be characterised as a concrete operating model or method, such as cross border cash transport. A risk may also be a concrete factor such as a geographical location or matters related to technological development. However, the risks presented in Finland's national risk assessment may in some cases be weighted towards vulnerabilities or threats.

7 NPO sector means non-profit organisations. For more details of the definition, see section 5.3 of the risk assessment.

8 FATF 2013, p. 7.

9 FATF 2013, p. 7.

10 FATF 2013, pp. 7–8.

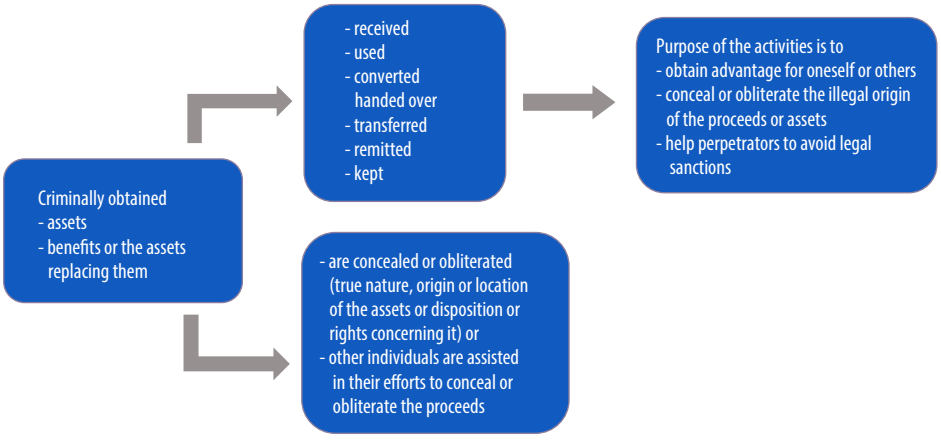
According to FATF, given the challenges in determining or estimating the consequences, it is accepted that when preparing their risk assessments, countries focus primarily on achieving a comprehensive understanding of their threats and vulnerabilities. The key is that the risk assessment adopts an approach that attempts to distinguish the extent of different risks to assist with prioritising mitigation efforts.[11] This approach was also adopted in the Finnish national risk assessment. The approach was adopted because, as a rule, the economic and societal consequences of money laundering and terrorist financing are serious and money laundering and terrorist financing generate significant negative impacts on a continuous basis. This approach is also supported by the European Commission.[12]

1.3 Money laundering and terrorist financing

1.3.1 Money laundering

Money laundering means activities referred to in chapter 32(6) of the Criminal Code (39/1889), in which criminal proceeds are transferred through legal payment systems to conceal or obliterate the true nature, origin or owners of the funds. Money laundering must be preceded by a predicate offence generating criminal proceeds.

Figure 1. Structure of money laundering.



11 FATF 2013, p. 8.

12 12 EU SNRA 2017 – Commission Staff Working Document, p. 235.

Money laundering comprises three stages: placement, layering and integration. In the first stage, the criminal proceeds are placed in the financial system. In the second stage, measures are taken to conceal or obliterate the origin of the funds and in the third stage, the proceeds of crime are returned to legal financial markets. These three stages may also occur simultaneously.[13]

According to Statistics Finland, a total of 449 cases of money laundering, aggravated money laundering, negligent money laundering and money laundering violation were reported to the authorities in 2019. Of these cases, 235 involved money laundering and 186 aggravated money laundering. In the preparations of the act and in case law, the minimum for criminal proceeds in aggravated money laundering has been set at EUR 13,000[14] but this limit is not absolute.

In 2019, charges for money laundering offences were brought in 303 cases.[15] In 134 of these cases, charges were brought for money laundering and in 168 cases for aggravated money laundering. Data on sentences and punishments compiled by Statistics Finland (Table 2) lists all charges brought for money laundering offences between 2015 and 2018. It should be noted that a sentence may be in the form of a combined punishment, which also includes other offences.

Table 1. Charges brought for money laundering offences between 2015 and 2019.

Type of crime	2015	2016	2017	2018	2019
Money laundering	37	61	205	70	134
Aggravated money laundering	77	178	262	241	168
Negligent money laundering	2	17	6	1	-
Money laundering violation	1	-	6	1	1
Total	117	256	479	313	303

13 FATF: 'What is Money Laundering?', referred to on 5 August 2020.

14 Government Proposal No., p. 38

15 Money laundering, aggravated money laundering, negligent money laundering and money laundering violation.

Table 2. Sentences for money laundering offences between 2015 and 2019.

Type of crime	2015	2016	2017	2018	2019
Money laundering	120	168	278	286	290
Aggravated money laundering	19	39	50	75	63
Negligent money laundering	22	38	42	71	71
Money laundering violation	22	25	34	31	46
Total	183	270	404	463	470

According to FATF, it is impossible to give accurate estimates of how much money is laundered each year.[16] However, UNODC[17] has estimated that between two and five per cent of the world's GDP is laundered each year.[18] If it assumed that the phenomenon is as widespread in Finland as in the rest of the world, the amount of money laundered in our country would total between EUR 5 and 12 billion each year.

Self-laundering

In self-laundering, the person who commits the offence also launders the proceeds of their crime. The established practice is that a money launderer who is involved in the predicate offence is not separately punished for money laundering. Thus, money laundering is an unpunished offence following a predicate offence as the view is that it is already adequately reviewed when a sentence for the predicate offence is determined.[19]

In December 2020, the amendments required by the anti-money laundering directive of the EU were incorporated into the Criminal Code. Under the amendments, the scope of punishment for self-laundering (money laundering in which the perpetrator also launders the proceeds of their crime) and for concealing criminal proceeds was extended. If a person that has committed a predicate offence takes measures to conceal the proceeds of their crime, they may also be punished for money laundering.[20] According to preliminary

16 FATF: 'What is Money Laundering?', referred to on 5 August 2020.

17 The United Nations Office of Drugs and Crime, UNODC.

18 UNODC: Money-Laundering and Globalization, referred to on 4 August 2020.

19 Government Proposal No.183/2020, p. 5.

20 Rahanpesu.fi: Rahanpesusäännöksiä täydennetään rikoslaissa [*Provisions on money laundering will be supplemented in the Criminal Code of Finland*], referred to on 5 January 2021

estimates, extending the scope of punishment for self-laundering will increase the number of money laundering sentences by between 100 and 200 each year.[21]

1.3.2 Terrorist financing

Terrorist financing means the provision or collecting of funds from legal or illegal sources directly or indirectly or with the awareness that the funds will be used for terrorist purposes. Terrorist financing is defined in chapter 34(a) section 5 of the Criminal Code[22] and it comprises financing of terrorist acts or preparation of terrorist acts, financial support for other terrorist activities or terrorist groups and promotion of terrorist activities.

Terrorist financing has three stages: collecting/raising funds, moving funds and using funds.[23] It has been noticed in Finland that terrorism is primarily financed with funds obtained from legal sources and the transactions are by means of account transfers, cash or money remittance services. Transactions take place between a large number of different countries.[24]

To combat terrorism and to prevent terrorist financing, funds of natural or legal persons can be frozen as provided in the Act on the Freezing of Funds with a View to Combating Terrorism (325/2013). In Finland, the freezing decisions are made by the National Bureau of Investigation, which also keeps a publicly accessible list of the decisions. The freezing decisions are implemented by the enforcement authorities. According to the statistics on special collection by the enforcement service, nearly EUR 1,000 in funds were frozen in 2019. In 2018, the figure had been slightly more than EUR 10,000 whereas no funds were frozen in 2017.

Sanctions are also imposed to combat terrorism and prevent terrorist financing and in practice they mean restrictions on economic or other cooperation targeting specific parties. The purpose of the sanctions is to impact activities that are considered a security or other threat. In the combating of terrorism, sanctions may take the form of financial sanctions involving the freezing of funds. The sanctions[25] against terrorism are listed on the website of the Ministry for Foreign Affairs.

21 Government Proposal No. 183/2020, p. 33.

22 For changes to chapter 34(a) of the Criminal Code contained in Government Proposal No. 135/2020, see section 1.5.2 'National legislation'.

23 FATF 2019, pp. 3 and 29.

24 Financial Intelligence Unit 2020b.

25 Ministry for Foreign Affairs: Sanctions against terrorism, referred to on 4 August 2020.

As a rule, launching a criminal investigation of terrorist financing is at the discretion of the Prosecutor General. The Prosecutor General must issue an order for prosecution if the offence has been committed outside Finland. If the suspected offence has been committed in Finland, the police will decide on the launching of the criminal investigation. After 2015, one criminal investigation of terrorist financing has been launched in Finland. A total of three criminal investigations of terrorist financing have been launched in Finland. One case of terrorist financing has been considered by a court but the charges were rejected by a Court of Appeal in March 2016.[26] No final court decisions on terrorist financing had been given in Finland by the end of 2020.

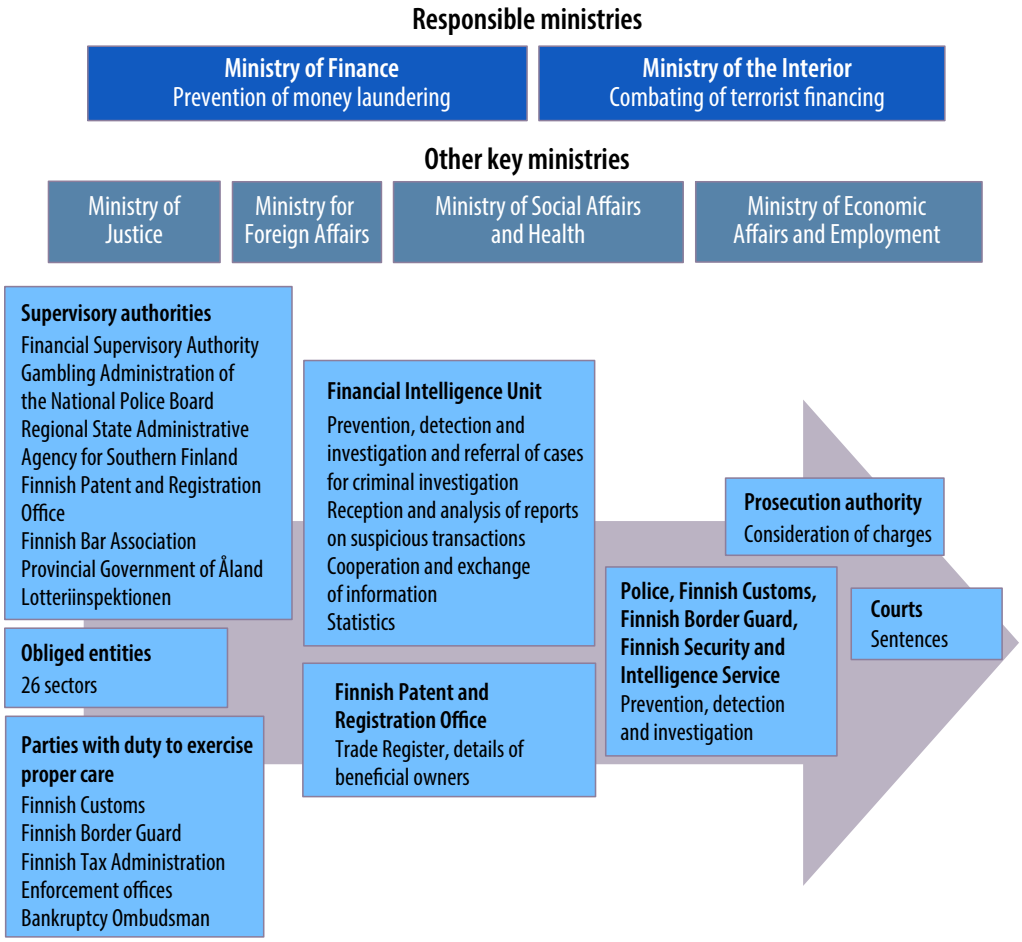
1.4 Combating money laundering and terrorist financing in Finland

1.4.1 Structure of the preventive work

The Ministry of Finance is responsible for enacting legislation on preventing money laundering and terrorist financing and provisions issued under it, national coordination of FATF matters and the preparation of the national risk assessment of money laundering. The Ministry of the Interior is responsible for enacting legislation on the Financial Intelligence Unit and the provisions issued under it, preparation of the national risk assessment of terrorist financing and the action plan based on the strategy on the combating of the shadow economy and economic crime. Other key ministries involved in the work are the Ministry of Justice, the Ministry for Foreign Affairs, Ministry of Social Affairs and Health and the Ministry of Economic Affairs and Employment.

26 Sentence of the Court of Appeal of Helsinki, 23 March 2016 No. 16/111925.

Figure 2. Key actors in the activities to prevent money laundering and terrorist financing.



1.4.2 Supervisory authorities and the registers maintained by supervisory authorities

Under the Anti-Money Laundering Act, government agencies and the Finnish Bar Association are tasked with overseeing that the obliged entities comply with their obligations laid down in the Anti-Money Laundering Act. Oversight of the obliged entities in the financial sector is the responsibility of the Financial Supervisory Authority,[27] while auditors are supervised by the Finnish Patent and Registration Office and attorneys-at-law by the Finnish Bar Association. Supervision of the gambling operator referred to in section 11 of the Lotteries Act (1047/2011) is the responsibility of the Gambling Administration of the National Police Board.[28] The Regional State Administrative Agency for Southern Finland is tasked with overseeing the other obliged entities referred to in the Anti-Money Laundering Act. The Provincial Government of Åland supervises real estate brokerage and letting agencies operating in Åland, while Lotteriinspektionen supervises the gambling operator of Åland.

27 The Regional State Administrative Agency for Southern Finland also supervises financial sector actors that do not come under the oversight of the Financial Supervisory Authority.

28 Under the Anti-Money Laundering Act, the National Police Board also supervises the business operators referred to in chapter 1(2)(2) that supply participation fees and registrations for participation for gambling provided by the gambling operator referred to in chapter 1(2)(1)(9). The powers to supervise the gambling operator referred to in the provincial legislation of Åland in Åland have been transferred to Lotteriinspektionen under the Decree of the President of the Republic on the carrying out of certain tasks laid down in the Act on Preventing Money Laundering and Terrorist Financing in Åland (500/2018).

Table 3. Supervisory authorities under the Anti-Money Laundering Act and the obliged entities supervised by them.

Supervisory authorities	Obliged entities
Financial Supervisory Authority	Deposit banks and other credit institutions, payment service providers, providers of virtual currency services, providers of investment services, fund management companies, crowdfunding companies, alternative investment fund managers, life insurance and non-life insurance companies, earnings-related pension insurance companies, insurance agents, central securities depository, account operators and custodians, housing loan intermediaries
Gambling Administration of the National Police Board	Gambling operator of Mainland Finland
Finnish Patent and Registration Office	Auditors
Finnish Bar Association	Attorneys-at-law
Regional State Administrative Agency for Southern Finland	Currency exchange offices, providers of asset management and business services, financial service providers that do not come under the oversight of the Financial Supervisory Authority (such as providers of consumer credit), debt collectors, peer-to- peer lenders, providers of business consulting and investment ancillary services, pawnbrokers, real estate agencies and apartment rental services, providers of tax advisory services or parties providing tax-related support directly or indirectly, par- ties executing accounting services, parties selling or brokering goods (combined value of cash transactions at least EUR 10,000), art dealers, (combined payment transactions at least EUR 10,000), and providers of legal services (excluding attorneys-at-law)
Provincial Government of Åland	Real estate agencies and apartment rental services operating in Åland
Lotteriinspektionen	Gambling operator of Åland

Supervisory authorities may impose administrative sanctions for non-compliance with the obligations laid down in the Anti-Money Laundering Act.[29] The purpose of the system of administrative sanctions is to prevent illegal activities and to ensure that it is not repeated or continued. Public warning, administrative fine and penalty payment are used

29 The Finnish Bar Association may not impose administrative sanctions on attorneys-at-law. It must submit a proposal for imposing administrative sanctions to the Regional State Administrative Agency for Southern Finland.

as administrative sanctions. A supervisory authority may issue an obliged entity with a public warning when the party in question, intentionally or negligently, fails to comply with the provisions of the Anti-Money Laundering Act or provisions or orders issued under it or the payer information regulation other than those referred to in chapter 7(1)(1) or chapter 7(1)(2) or section 3(1)(2). An administrative fine may be imposed on an obliged entity that intentionally or negligently fails to comply with its obligations. Under the Anti-Money Laundering Act, the penalty payment may only be imposed for a serious, repeated or systematic breach of obligations. The amount of the administrative fine and the penalty payment are based on an overall assessment.[30] Under the Anti- Money Laundering Act, the supervisory authority must publish its decision to impose an administrative fine or penalty payment or issue a public warning without delay after the person subject to the decision has been notified of the decision.

The Regional State Administrative Agency for Southern Finland has maintained a money laundering supervision register since 1 July 2019. Under the Anti-Money Laundering Act, obliged entities that are supervised by the Regional State Administrative Agency must be registered in the supervision register if they are not supervised as licence holders or obliged to be registered in other registers maintained by a supervisory authority. The supervision register has been established to ensure that the Regional State Administrative Agency is better placed to perform its supervisory duties and to maintain contacts with the obliged entities.[31]

The Finnish Patent and Registration Office registers companies, associations, foundations and other organisations and collects the details of the beneficial owners of registered legal persons, foreign express trusts or legal arrangements with similar legal form. The Finnish Patent and Registration Office also collects financial statements information of companies and other organisations and checks that foundations comply with the Foundations Act and their own rules.

30 Financial Supervisory Authority 2019, pp. 1 and 6. In December 2019, the Financial Supervisory Authority issued two operators with administrative sanctions (public warning and penalty payment). The sanctions were prompted by negligence on the part of the operators in such matters as customer due diligence. It should be noted, however, that the public warning received by one of the operators was based on the Act on the Financial Supervisory Authority (878/2008) because there were no provisions on public warning in the Anti-Money Laundering Act in effect at the time. The penalty payment imposed on the other operator was based on the Act on the Financial Supervisory Authority and it was for a failure to comply with the provisions of the Act on Credit Institutions (610/2014) and the Anti-Money Laundering Act.

31 Regional State Administrative Agency for Southern Finland: Money laundering supervision register, referred to on 29 July 2020.

1.4.3 Resources allocated to the prevention of money laundering and terrorist financing

Under the Anti-Money Laundering Act, one purpose of the risk assessment is to describe the structures of the combating of money laundering and terrorist financing, general measures taken to tackle the problem and the resources allocated to the efforts. In a survey carried out among the key government agencies[32] and supervisory authorities involved in the work, the respondents were asked about the resources for combating money laundering and terrorist financing available to them and their adequacy.

According to the survey findings, the supervisory authorities referred to in the Anti-Money Laundering Act allocate about 26 person-years to the combating of money laundering and terrorist financing. The figure covers staff members working to combat money laundering and terrorist financing on a full-time basis. The organisations may also employ persons whose tasks include the combating of money laundering and terrorist financing. It is difficult to use person-years to measure the resources of the actors referred to in the Anti-Money Laundering Act to which the duty of care applies. This is because the combating of money laundering and terrorist financing is only one of the duties of these actors. Depending on the organisation, the work tasks of between 50 and 300 people also include the combating of money laundering and terrorist financing. The Financial Intelligence Unit of the National Bureau of Investigation has a capacity of about 40 person-years.

The ministries playing a key role in the prevention of money laundering and terrorist financing allocate between six and eight person-years to the work. This figure includes persons who also perform tasks other than combating money laundering and terrorist financing.

Generally speaking, the bodies participating in the survey consider their resources inadequate. Changes in anti-money laundering legislation, increase in the number of obligations and (in the case of supervisory authorities) the large number of supervised parties are the main reasons why resources are seen as insufficient.[33]

32 The survey questionnaire was sent to the organisations represented in the risk assessment working group, the Finnish Border Guard and the National Enforcement Authority Finland.

33 In its Mutual Evaluation Report on Finland, FATF also highlighted the modest resources, which affects the supervision of AML and CFT work. See for example FATF MER 2019, p. 13.

1.4.4 Financial Intelligence Unit

Obliged entities must meet the customer due diligence obligation, detect and investigate suspicious transactions and report on suspicious transactions and suspected terrorist financing without delay. The task of the Financial Intelligence Unit is to:

- prevent, detect and investigate cases of money laundering and terrorist financing and refer the cases for criminal investigation
- receive reports on suspicious transactions and analyse them and give feedback on their impacts
- cooperate with other authorities in the prevention of money laundering and terrorist financing
- cooperate and share information with the authorities of foreign countries and international organisations tasked with the prevention and investigation of money laundering and terrorist financing
- cooperate with the obliged entities
- keep statistics on the number of reports on suspicious transactions and freezing of transactions, number of reports on suspicious transactions referred to investigation and on received and rejected information requests and information requests to which answers have been given, and
- receive and process the reports referred to in section 3(2) of the Act on the Freezing of Funds with a View to Combating Terrorism (325/2013), review the prerequisites for the freezing decisions referred to in section 4 of the same act and submit proposals for freezing decisions.

The Financial Intelligence Unit has a staff of about 40.[34] In 2019, the Financial Intelligence Unit received more money laundering reports, launched more investigations and issued more orders to freeze transactions than ever before.[35] In 2019, a total of 64,403 money laundering reports were submitted, which was about 64 per cent more than in 2018. In 2018, a total of 39,220 reports were submitted, which was about 19 per cent below the figure for 2017 (48,318 money laundering reports).[36] For comparison: in Sweden, just over 20,000 money laundering reports were submitted in 2019.[37] The number of manual reports[38] has increased over a period of several years. At the same time, the number

34 Financial Intelligence Unit 2019, p.10.

35 Financial Intelligence Unit 2019, p. 3.

36 Financial Intelligence Unit 2019, p.15.

37 Forsman 2020, p. 49.

38 Money laundering reports submitted by parties other than gambling companies and payment gateway providers. Reports are received on the basis of individual risk assessments and sum limits. All reports are processed and reviewed on a case-by-case basis.

of high volume reports[39] increased by 82 per cent between 2018 and 2019, which was partially a result of a substantial increase in the sum limit-based reports by payment gateway providers.[40]

In 2019, a total of 25 separate terrorist financing reports were submitted.[41] However, some of the money laundering reports may also include observations on terrorist financing. In 2019, the Financial Intelligence Unit launched a total of 1,515 investigations and 1,425 of them concerned money laundering and 90 terrorist financing.[42]

Under section 6 of the Act on the Financial Intelligence Unit (445/2017), the Financial Intelligence Unit has the right to issue an order to freeze transactions for a maximum of ten working days. Like the number of money laundering reports, the number of freezing orders has increased in Finland each year. In 2019, a total of 73 freezing orders were issued, which was a new record. In 2019, a total of EUR 9.8 million in funds was frozen and more than EUR 4.9 million of this remained in the possession of the authorities.[43]

1.4.5 Other authorities

The police, Finnish Customs and the Finnish Border Guard participate in the prevention, detection and investigation of money laundering and terrorist financing as part of their own activities. These authorities also act as criminal investigation authorities in money laundering offences within scope of their powers. The duty of the Finnish Security and Intelligence Service is to prevent and combat the most serious threats to national security, such as terrorism.

Under the Anti-Money Laundering Act, certain authorities must also exercise proper care. Finnish Customs, the Finnish Border Guard, tax and enforcement authorities and the Bankruptcy Ombudsman must ensure that as part of their work, they pay attention to the prevention and detection of money laundering and terrorist financing. They must also report suspicious transactions and suspected cases of terrorist financing detected as part of their duties to the Financial Intelligence Unit.

39 High volume reports are money laundering reports submitted by gambling companies and payment gateway providers. The reports are not processed on a case-by-case basis.

40 Financial Intelligence Unit 2019, p. 13.

41 Terrorist Financing Report, TFR.

42 Financial Intelligence Unit 2019, pp. 3 and 19.

43 Financial Intelligence Unit 2019, p. 23.

1.4.6 National FATF steering group and FATF group

The Ministry of Finance appointed the national FATF steering group in October 2019. The FATF steering group is a national body appointed until further notice and its task is to steer and coordinate the implementation of the obligations arising from Finland's FATF membership on a national basis. The FATF steering group appointed by the Ministry of Finance continues the work of the FATF steering group appointed by the Ministry of the Interior on 26 January 2015 in accordance with the memorandum of understanding between the Ministry of the Interior and the Ministry of Finance in December 2018. The chairmanship of the FATF steering group is held by the Ministry of Finance and its membership comprises representatives of the key authorities and other actors responsible for preventing money laundering and terrorist financing.

In accordance with the FATF Recommendation 2, the FATF steering group deals with the following national matters pertaining to the prevention of money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction: cooperation between relevant authorities, development of action plans and deciding on their implementation, coordination of relevant issues and discussions on them, and determining of Finland's standpoints for FATF working group meetings and Plenary. The FATF steering group is also tasked with ensuring that appropriate preparations are made for the Mutual Evaluation of Finland and that the recommendations made in the evaluation are properly implemented.

The national FATF group works under the auspices of the FATF steering group and its work is monitored and if necessary steered by the FATF steering group. The FATF group prepares the Finnish standpoints for decision by the steering group and collects information for responses to the requests for comments and information received from FATF. The FATF group is chaired by the Ministry of Finance. The competent national authorities represented in the FATF steering group are also represented in the FATF group.

1.4.7 National cooperation group for preventing money laundering and terrorist financing

The national cooperation group for preventing money laundering and terrorist financing was originally appointed by the Ministry of the Interior for the term 4 May 2018 – 31 December 2020. In December 2018, the Ministry of the Interior and the Ministry of Finance prepared a memorandum of understanding in which they agreed on the reallocation of their official responsibilities for preventing money laundering and terrorist financing as from 1 March 2019. As a result, the Ministry of Finance and the Ministry of the Interior appointed a new national cooperation group for preventing money laundering and terrorist financing on 18 December 2019. In the same connection, the working group

was enlarged. The working group is jointly chaired by the Ministry of Finance and the Ministry of the Interior. The new working group was appointed until further notice. The task of the working group is to develop national measures to prevent money laundering and terrorist financing and to make the work more effective. Its tasks include improving the flow of information between supervisory bodies, the authorities and prosecution authorities, ensuring closer cooperation between the authorities and obliged entities and harmonising the operating models used in the supervision of the prevention of money laundering and terrorist financing. The working group may establish sub-working groups, which report to the working group. A sub-working group of the supervisory authorities has already been established and it organises its meetings independently.

1.4.8 Public private partnership (PPP) – expert work- ing group comprising the authorities and private sector and dealing with the prevention of money laundering and terrorist financing

An expert working group comprising representatives of the authorities and private sector and dealing with the prevention of money laundering and terrorist financing (Public private partnership, PPP) was established in 2020. Its purpose is to ensure closer cooperation between and among the authorities[44] and private sector actors.[45] The working group is chaired by the Financial Intelligence Unit. The working group focuses on the promotion of crime prevention objectives, or effective prevention, detection and investigation of money laundering offences, their predicate offences and terrorist financing offences and referral of the cases to criminal investigation.

Concrete operational cooperation and cooperation aimed at developing processes to prevent money laundering and terrorist financing are the two key goals of the expert working group. In the field of developing preventive processes, the aim is to identify and remove obstacles to exchange of information and to share topical information on the methods of money laundering and terrorist financing and money laundering risks. The parties represented in the working group were selected by the Financial Intelligence Unit. In the selection of the parties, consideration was given to national money laundering risks and the size of the obliged entities and their role in the financial sector and the prevention of money laundering.

44 The authorities: Financial Intelligence Unit, police, ministries and supervisory authorities.

45 Private sector actors: obliged entities and the organisations supervising their interests.

1.5 Regulation of preventing money laundering and terrorist financing

1.5.1 Supranational actors and regulation

The work against money laundering and terrorist financing is partially guided by international recommendations and guidelines. In addition to its own national legislation and European Union legislation, Finland is also bound by the supranational risk assessment prepared by the European Commission. At the same time, even though the guidelines and recommendations issued by FATF are not binding on its member countries under international law, FATF members are politically committed to implementing them on a national basis. Other parties relevant to the prevention of money laundering and terrorist financing are the United Nations and the UN Security Council, Council of Europe, Egmont Group of financial intelligence units, and (in terms of law enforcement) Europol and Interpol.

The United Nations Office on Drugs and Crime (UNODC) combats illegal drugs and international crime and the global programme against money laundering also operates under its auspices.[46] In many of its resolutions, the UN Security Council has imposed sanctions on terrorist organisations and individuals and groups connected with them and it maintains a publicly accessible list of such actors.

FATF

FATF is an inter-governmental task force coordinated by the OECD (Organisation for Economic Co-operation and Development) working to prevent money laundering and terrorist financing. It is engaged in international cooperation against money laundering and terrorist financing, it prepares and issues recommendations on the combating of money laundering and terrorist financing and monitors their implementation in FATF member countries. FATF promotes the effective implementation of regulation-based operational measures to combat money laundering, terrorist financing, proliferation of weapons of mass destruction and other activities threating international financial markets.

The 40 recommendations issued by FATF serve as guidelines helping countries to develop their own activities to combat money laundering, terrorist financing and proliferation of weapons of mass destruction by applying the guidelines to the countries' own legal and administrative frameworks and financial systems. The purpose of the recommendations is

46 The Global Programme against Money Laundering, UNGPML.

to set international standards and improve the effectiveness of the systems designed to prevent money laundering and terrorist financing.[47]

FATF expects its members to apply a risk-based approach to the combating of money laundering and terrorist financing, and this approach is defined in Recommendation 1 ('Assessing risks and applying a risk-based approach'). Under the recommendation, to mitigate the risks, member countries are required to carry out national risk assessments and apply a risk-based approach based on the risk assessment results. Under Recommendation 1, national actors, such as financial institutions, are also required to carry out their own risk assessments.[48]

Supranational risk assessment of the European Commission

EU Member States must take into account the supranational risk assessment of the European Commission when preparing their own national risk assessments. The second supranational risk assessment was published in 2019. It specifies products and services that can provide a basis for money laundering and terrorist financing and recommends that Member States should identify high-risk and low-risk sectors and areas in their national risk assessments. The supranational risk assessment contains recommendations for Member States on how to mitigate money laundering and terrorist financing risks and its results must be considered in the drafting of national risk assessments.

Supranational regulation

The EU-level provisions on the prevention of money laundering and terrorist financing are contained in the two anti-money laundering directives. The purpose of the fourth anti-money laundering directive[49] is to prevent the use of the Union's financial system for money laundering and terrorist financing. The key regulatory components of the directive are as follows: risk-based approach, customer due diligence, verification and registration of the information on the beneficial owners, and the reporting obligations. In addition to a small number of amendments to the fourth anti-money laundering directive, the fifth anti-money laundering directive[50] also introduced new regulation extending the scope of the

47 FATF 2012–2020, p. 7.

48 FATF 2012–2020, p. 10.

49 Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Di- rective 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

50 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

two directives to the providers of virtual currencies, and it also obliged the Member States to establish a bank and payment accounts control system.

Provisions on the prevention of money laundering are also contained in the second payer information regulation (2015/847).[51] The regulation applies to the information on payers and payees that must be provided with transfers of funds in any currency for the purpose of preventing, detecting and investigating money laundering and terrorist financing. The regulation can be applied to a transfer of funds if at least one of the payment service providers involved in the transfer is established in the Union.

The national regulation on preventing terrorist financing is also based on international obligations, the most important of which is the International Convention for the Suppression of the Financing of Terrorism (Finnish Treaty Series 74/2002). The UN Security Council Resolution 1373 (2001) on the measures to prevent terrorism and terrorist financing has also influenced national regulation on terrorist financing. Finland has also acceded to the 2005 Council of Europe Convention on the Prevention of Terrorism (Finnish Treaty Series 49/2008).

1.5.2 National legislation

National legislation on the prevention of money laundering and terrorist financing is based on EU directives and FATF recommendations. From the administrative perspective, the Anti-Money Laundering Act and the Act on the Financial Intelligence Unit can be seen as preventive legislation, whereas the essential elements of money laundering and terrorist financing contained in the Criminal Code concern the retroactive assessment of the activities.

The Anti-Money Laundering Act that entered into force in 2017 repealed the Anti-Money Laundering Act of 2008. The purpose of the Anti-Money Laundering Act is to prevent money laundering and terrorist financing, to help to detect and investigate such activities and to ensure more effective tracing and recovery of the criminal proceeds. With the Anti-Money Laundering Act of 2017, Finland incorporated the fourth anti-money laundering directive and the second payer information regulation into its national legislation. Finland has incorporated the fifth anti-money laundering directive into its national legislation with the Act on the Bank and Payment Accounts Control System (571/2019), the Act on Virtual Currency Providers (572/2019) and amendments to the Anti-Money Laundering Act.[52]

51 Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

52 Government Proposal No. 167/2018, p. 1.

Compared with the old act, the regulatory focus in the current Anti-Money Laundering Act is on risk assessments, register of beneficial owners, official supervision and cooperation between the authorities. It also contains provisions on the money laundering supervision register. The Anti-Money Laundering Act of 2017 has a stronger focus on risk assessment than the old act.[53]

The Act on the Financial Intelligence Unit contains provisions on the Financial Intelligence Unit, and the register on the prevention, detection and investigation of money laundering and terrorist financing. Before the overhaul of the anti-money laundering legislation in 2017, the provisions on the Financial Intelligence Unit were contained in the Anti-Money Laundering Act. The existence of a separate piece of legislation can be justified by the fact that the Financial Intelligence Unit is a police unit to which police legislation partially applies. The data protection provisions applying to FIU also differ from those observed by the supervisory authorities.[54]

The Mutual Evaluation Report on Finland prepared by FATF between 2018 and 2019 highlighted inadequacies in the national anti-money laundering legislation. On 25 January 2019, the European Commission also issued a reasoned opinion stating that Finland has not fully aligned its national legislation with the provisions of the fourth antimoney laundering directive. After the European Commission had drawn particular attention to a number of provisions of the directive, it was determined that there is a need to make certain parts of the national legislation more specific. In spring and summer 2020, the Ministry of Finance also asked key actors involved in the prevention of money laundering and terrorist financing to submit proposals for changes in the legislation on the prevention of money laundering and terrorist financing. The purpose of the legislative projects under way is to change the Anti-Money Laundering Act and the Act on the Financial Intelligence Unit so that the national legislation can be aligned with the FATF recommendations and the anti-money laundering directive. The projects concern the need for technical and more fundamental changes to the legislation.[55]

Most of the legal provisions on terrorist financing are contained in chapter 34(a) of the Criminal Code. Moreover, to meet the obligations set out in the UN Security Council Resolution 1373 (2001), Finland has also enacted the Act on the Freezing of Funds with a View to Combating Terrorism (325/2013). The act contains provisions on the administrative freezing of funds and it applies to the funds of a natural or legal person that is reasonably

53 Government Proposal No. 228/2016, p. 1.

54 Government Proposal No. 228/2016, p. 1.

55 Ministry of Finance project: Government proposal on amending the Act on Preventing Money Laundering and Terrorist Financing, referred to on 5 August 2020. Of the changes concerning customer due diligence under preparation in the project, see section 2.2.3 'Customer due diligence'.

suspected of, charged with or convicted of a terrorist offence criminalised under chapter 34(a) of the Criminal Code.

The Ministry of Justice is currently drafting a Government proposal[56] under which changes will be made to the provisions on terrorist financing. The changes have been prompted by the assessment of FATF and the Counter-Terrorism Committee of the UN Security Council (CTED) concerning Finland's terrorist financing legislation. *Under terrorist financing*, a new penal provision proposed to be added to the Criminal Code, it would be punishable to finance persons who on the basis of the opinions or threats that they have expressed or the information otherwise received on their activities are acting to commit offences with terrorist intent referred to in chapter 34(a). There would also be technical changes to the provision on the financing of a terrorist group and the requirement that the parties providing or collecting the funds must act with a specific intent or be aware of their activities would be added to the essential elements of the offence. In addition to these changes, it is also proposed that the type of crime describing terrorist financing would be changed into *financing of a terrorist offence*.[57]

56 Government Proposal No. 135/2020 was under review by Parliamentary Committees in February 2021.

57 Ministry of Justice 2020a, pp. 6-7.

2 Money laundering

2.1 Key observations

Excessive trust in the customer due diligence of credit institutions is seen as the key money laundering risk in all sectors of obliged entities. These measures primarily refer to the continuous monitoring of customer relationships by credit institutions and the measures to establish the source of the funds. As a result, the measures to establish the source of funds originating from the customer's account may remain insufficient if it assumed that the credit institution has already adequately established the origin of the funds.

International connections are also seen as a risk in all sectors. For example, in the case of credit institutions and payment service providers this primarily means international transactions. However, in many sectors, the international dimension relates to the customers and their domicile. As a rule, customers from outside the EEA are seen as a high risk because establishing the beneficial owners of such customers and determining the sources of their funds is difficult.

New products, services and actors made possible by technological development are seen as a high risk and the risk can be examined in terms of the obliged entities, supervisory bodies and other authorities. For example, from the actor's perspective, the operating principles of the new payment service providers and technologies are so new that there are still no well-established practices for identifying suspicious transactions carried out as part of ordinary business operations. The key challenge facing supervisory bodies and other authorities is to keep pace with the changes and to adjust the supervisory and other activities accordingly.

Even though in overall terms, national anti-money laundering expertise can be considered good, training is nevertheless needed in nearly every sector of obliged entities. It emerged from the interviews with experts that there is a particular need for actor-internal training but it is also felt that supervisory authorities should issue general guidelines on such matters as continuous customer monitoring. Uniform and explicit sector-specific guidelines and clarifying the legislation to narrow the scope for interpretation would also help to focus risk-based assessment.

The risk levels of the sectors examined in the national risk assessment[58] are described below (on a scale of 1 to 4).[59] Formation of the risk levels is described in more detail in the appendix on the risk assessment methodology.

Table 4. Risk levels of the sectors examined in the national risk assessment.

Sector	Risk level
Hawalas	4
Providers of virtual currency services	4
Payment service providers	3
Credit institutions	3
Currency exchange	2
Gambling operators	2
Other providers of financial services	2
Financial institutions	2
Cash-based reporting obligation based (sales of goods)	2
Providers of tax advisory services or parties providing tax-re- lated support directly or indirectly	2
Other providers of legal services	2
Bookkeepers	2
Providers of asset management and business services	2
Art dealers	2
Attorneys-at-law	2
Real estate agents	2
Debt collectors	2
Auditors	2
Insurance companies	2
Pawnbrokers	2
Apartment rental services	1

58 The sectoral division is based on the groups of obliged entities defined in the scope of application of the Anti-Money Laundering Act. The formation of the sectors is described in more detail in the appendix on the risk assessment methodology.

59 The scale is applied as follows: 1=less significant risk, 2=moderately significant risk, 3=significant risk and 4=very significant risk.

2.2 General factors impacting money laundering risk

Before sector-specific risks are examined, general factors concerning the operating environment impacting the assessment of money laundering risk are highlighted. According to FATF, 'environmental' factors include political, economic, social, technological and legislative aspects.[60] In this national risk assessment, money laundering predicate offences, geographical location of Finland, customer due diligence and technological development are highlighted as general factors contributing to the money laundering risk. Under the Anti-Money Laundering Act, obliged entities and supervisory authorities must also take these factors into account when assessing the money laundering risks arising from customer relationships.

2.2.1 Money laundering predicate offences

Money laundering predicate offences can be considered as money laundering risks and any offence generating economic benefits may constitute a money laundering predicate offence. Identifying and preventing predicate offences is also important in terms of preventing money laundering. The focus in the examination of money laundering predicate offences is on identified and the most important predicate offences. Annual crime statistics, a report on the predicate offences behind money laundering sentences and data disclosures by the Financial Intelligence Unit have been considered in the assessment. Offences that may have generated substantial criminal proceeds have also been considered.

In 2020, more than 537,000 offences under the Criminal Code were reported to the police, an increase of more than 80,000 compared with the previous year. More than 252,000 of this total were property offences. In fact, property offences account for about half of all offences under the Criminal Code reported to the police. Offences involving fraud are included in the category of property crime and they totalled more than 33,000 in 2020. This means that they were the second most common type of property offence after burglaries. According to annual crime statistics, there has been an increase in property offences, which can be considered to have impacts on possible money laundering predicate offences.[61]

60 FATF 2013, p. 25.

61 Statistics Finland: The use of coercive means increased by 3 per cent, referred to on 23 March 2021.

The number of money laundering offences reported to the police has been more than 400 over the past four years.[62] Even though no direct conclusions can be drawn from the statistics, moderate growth in fraud until 2019 (compared with the trend in money laundering offences) may give some idea of how many offences involving fraud are committed as money laundering predicate offences.

There are no up-to-date figures or analyses of the ratio between money laundering predicate offences and sentence for money laundering. The latest report on sentences for aggravated money laundering offences compiled by the Financial Intelligence Unit covers the sentences given 2015 and 2016. The report shows that different types of fraud[63] constitute a substantial proportion of predicate offences. In addition to fraud, embezzlement, theft, narcotics offences, and offences by a debtor are also typical money laundering predicate offences.[64] In a fraud, the perpetrator of a predicate offence may have sold non-existent assets or may obtain online banking codes through phishing allowing a direct transfer of funds from the victims' accounts to the accounts of the money launderer (third person). There have also been cases involving the increasingly common fake police phenomenon in which the injured parties are deceived to disclose their online banking codes by phone to persons posing as police officers.

Most of the information disclosed by the Financial Intelligence Unit for criminal investigations between 2015 and 2020 has involved aggravated fraud. This is also in line with the report based on the sentences.

62 PolStat.

63 Fraud comprise basic fraud, aggravated fraud and means of payment fraud.

64 Financial Intelligence Unit 2018a, p. 14.

Table 5. Most common types of crime for which the Financial Intelligence Unit disclosed information between 2015 and 2020.

Type of crime
Aggravated fraud
Fraud
Aggravated money laundering
Aggravated accounting offence
Investigation to impose a ban on business operations
Aggravated tax fraud
Money laundering
Aggravated dishonesty by a debtor
Registration offence
Aggravated embezzlement
Aggravated narcotics offence
Aggravated means of payment fraud
Identity theft
Forgery
Other types of crime (194)

The most common money laundering predicate offences are not specified in the information on different types of crime disclosed by the Financial Intelligence Unit. It should also be noted that the disclosures include such types of crime as aggravated money laundering and money laundering because information is disclosed for both predicate offences and money laundering offences. In terms of data disclosures, there are substantial differences between fraud and other predicate offences as more than a third of all data disclosures have been made for criminal investigations of fraud or aggravated fraud.

In Finland, money laundering is typically connected with fraud, theft, narcotics offences, offences by a debtor, tax offences and other economic crime.[65] When comparisons are made between predicate offences listed in the report on case law and the types of crime disclosed by the Financial Intelligence Unit, it can be noted that there are differences concerning narcotics offences and theft. According to the case law report, narcotics

65 Government Proposal No. 183/2020, p. 9.

offences and theft are common money laundering predicate offences, whereas they constitute a lower proportion of the offences on which information is disclosed for criminal investigations. However, it was noted in the case law report that narcotics offences now constitute a lower proportion of money laundering predicate offences.[66]

Organised criminal groups have been identified as one threat in money laundering. In addition to traditional organised criminal groups wearing special insignia, groups committing property offences across national boundaries and defined in the Criminal Code are also considered as organised criminal groups in case law. Such groups may only exist for the duration of a single offence or a series of offences after which they are dissolved. According to the observations made by the police, international organised crime in particular is making increasing use of data networks in its criminal activities. The offences include fraud and hoaxes used to deceive individuals or company employees to transfer sums to criminals' accounts. In data networks, the activities can be carried out on a large scale, which means that small sums may also generate substantial proceeds of crime.[67]

International comparisons concerning predicate offences were produced so that unifying and distinguishing features of predicate offences could be illustrated.[68] It was noted in the comparison that the money laundering predicate offences identified at national level and considered as the most common such offences (fraud, tax fraud, economic crime and narcotics offences) were also considered as common money laundering predicate offences and major risks. No notable distinctive national features were found in the comparison. However, in the risk assessment conducted in Luxembourg, corruption and bribery were identified as particularly high-risk predicate offences. This can be considered a substantial deviation from national findings because giving and aggravated giving of bribes in business were not seen as high-risk predicate offences in the assessment.

Fraud

In a fraud, a person who, in order to obtain unlawful financial benefit for themselves or other persons or in order to harm another, deceives another or takes advantage of an error of another so as to have this person do something or refrain from doing something and in this way causes economic loss to the deceived person or to the person over whose benefits this person is able to dispose. Provisions on fraud are contained in chapter 36 and on means of payment fraud in chapter 37(8-11) of the Criminal Code. In addition,

66 Government Proposal No. 183/2020, p. 9.

67 Police: Organised crime, referred to on 21 January 2021.

68 It was noted that not all countries have specified money laundering predicate offences in their risk assessments. For this reason, only the risk assessments of the United Kingdom (2017) and Luxembourg (2018) were included.

provisions on tax fraud are contained in chapter 29 of the Criminal Code (Offences against public finances).

Fraud is a multi-faceted offence because it covers a wide range of different ways of committing crime, victims and perpetrators. Fraud may target the public or private sector or charity operators and the offences may be committed online or in everyday life.

Most of the money laundering predicate offences committed in Finland are different types of fraud. Fraud is on the increase again after a decline over a period of two years. According to the preliminary figures compiled by Statistics Finland, a total of 33,300 cases of fraud were reported to the police, Finnish Customs and the Finnish Border Guard in 2020.[69] This was 16.1 per cent more than in 2019. A total of 2,000 cases of aggravated fraud were reported, a decrease of 2.4 per cent compared with 2019. An increase of 16.5 per cent in means of payment fraud was also recorded.[70] According to a press release by the National Police Board, an increase in petty fraud has been the biggest factor contributing to the increase in fraud. There has also been concern over elderly people becoming victims of online fraud.

Economic crime

Economic crime involves the operations of companies and other organisations and in them the aim is to obtain financial advantage by criminal means. Other offences committed with the intention of obtaining advantage and that are connected with business operations are also considered as economic crime.[71] Tax fraud is the most common type of economic crime. Other typical economic offences include accounting offences and offences by a debtor.

Between 1,800 and 2,000 economic offences are reported to the police every year. Between 700 and 800 of them are tax offences, and between 400 and 500 offences by a debtor. Even though there was a decrease in the overall crime rate in 2019, a substantial increase in economic crime was reported. There was a particularly strong increase in aggravated tax offences, aggravated dishonesty by a debtor and aggravated accounting offences during 2019.[72] The overall economic situation has an impact on the amount of economic crime each year. When the economy is doing well, there is also a decrease in economic crime reported to the police. The impacts of the COVID-19 pandemic on the

69 The types of fraud referred to above are offences listed in chapter 36(1-3) of the Criminal Code (fraud, petty fraud and aggravated fraud).

70 Statistics Finland: Property crime increased by 16.9 per cent, referred to on 21 January 2021.

71 Police: Economic crime, referred to on 21 January 2021.

72 Grey economy & economic crime: Crime prevention, referred to on 22 January 2021.

economy and consequently on economic crime will probably be visible with a slight delay.[73]

Shadow economy can also be a feature of legal business operations, if the operators neglect the payment of taxes and other statutory contributions. It is estimated that the shadow economy accounts for between one billion and 14 billion euros of Finland's GDP. Shadow economy is hidden crime, which means that not all offences are reported to the police.[74]

The damage caused by economic crime and the shadow economy and the proceeds generated by them are also substantial and the damage caused by economic crime also has significant societal impacts. The damage caused by the economic offences investigated in 2019 totalled more than EUR 320 million and nearly EUR 32 million in criminal proceeds were seized by the authorities. All types of economic crime (such as tax fraud, fraud, money laundering offences and embezzlement) are included in the statistics on criminal proceeds.[75]

Narcotics offences

In a narcotics offence, a person unlawfully produces, possesses, obtains, uses, con- veys or sells narcotic substances or attempts to do any of the above. Provisions on narcotics offences are laid down in chapter 50 of the Criminal Code. Narcotics crime is often hidden crime, which may have an impact on the number of narcotics offences (and thus also the number of money laundering predicate offences) reported to the police. Narcotics offences are often uncovered by the police in connection with other activities.[76]

Even though it was noted in the case law study prepared by the Financial Intelligence Unit that narcotics crime now constitutes a lower proportion of money laundering predicate offences, overall narcotics crime has increased. In 2020, a total of nearly 37,000 narcotics offences were reported to the police, which was 14.4 per cent more than in the year before. However, there was a decrease of 9.9 per cent in aggravated narcotics crime. Nearly two thirds of all narcotics offences involve unlawful use of narcotics, and the number of such offences reported to the police increased by 12.4 per cent compared with 2019.[77] In

73 Ministry of the Interior: Tax fraud is the most common type of economic crime, referred to on 22 January 2021.

74 Ministry of the Interior: Tax fraud is the most common type of economic crime, referred to on 22 January 2021.

75 Grey economy & economic crime: Crime prevention, referred to on 22 January 2021.

76 Police: Narcotics offences, referred to on 21 January 2021.

77 Statistics Finland: Property crime increased by 16.9 per cent, referred to on 21 January 2021.

unlawful use of narcotics, a person only possesses small amounts of narcotics for their own use.[78]

Cannabis, amphetamine and derivatives of amphetamine are the most common narcotic substances used in Finland. The use of cocaine has also increased in recent years and according to a wastewater study, the combined use of amphetamine, methamphetamine, MDMA and cocaine has tripled since 2012. According to the study, the COVID-19 pandemic has had an impact on the use of narcotic substances as after the introduction of the state of emergency, the amounts of amphetamine have reached record levels. At the same time, the rising trend in cocaine use has levelled off during the pandemic.[79]

Illegal trade in narcotics is often cross-border crime carried out by professionals on an organised basis. Over the past ten years, illegal trade in narcotics has moved from the streets to the internet and it often takes place in the dark web to ensure maximum anonymity of the activities.[80] It has been noted that in the virtual currency sector, narcotics offences are fairly common predicate offences of money laundering. Narcotics offences involve anonymous online trade in narcotics in which the dealers are paid in virtual currencies.[81]

Proceeds of crime

Forfeiture or confiscation is a criminal law sanction imposed by a court. Provisions on the general prerequisites of forfeiture and forfeiture of the proceeds of crime are contained in chapter 10(1–2) of the Criminal Code. Under the Criminal Code, proceeds of crime mean the proceeds of criminal activities. Thus, an act punishable under the law is a prerequisite for a forfeiture order. The proceeds of crime ordered forfeit to the State may include property directly obtained by criminal means, property replaced by property, return on property, value of the property and the returns, or the value of the savings generated by criminal means.

There is substantial annual variation in money laundering confiscation statistics.

78 Police: Narcotics offences, referred to on 21 January 2021.

79 Finnish Institute for Health and Welfare (THL): Wastewater study – narcotics use among the population, referred to on 22 January 2021.

80 Police: Narcotics offences, referred to on 21 January 2021.

81 Financial Intelligence Unit 2018b, pp. 21–22.

Table 6. Forfeiture orders issues by district courts, in euros.

Type of crime	2015	2016	2017	2018	2019	Total
Money laundering	27,022	78,463	78,463	341,627	15,485	531,185
Aggravated money laundering	105,208	189,901	99,782	896,788	35,150	1,326,829
All money laundering offences[82]	132,475	268,365	175,170	1,414,615	52,645	2,043,270

The proceeds of economic crime totalled EUR 32 million in 2019. The proceeds of crime presented in the money laundering confiscation statistics are included in the proceeds of economic crime.[83] Despite annual variation, the conclusion is that money laundering has generated substantial criminal proceeds over the past five years.

2.2.2 Geographical location

When the money laundering risk is assessed, the impact of the geographical location must also be considered. This means the impact of Finland's geographical location on money laundering risks and their levels, and the impact of factors outside Finland (such as foreign customers and the risks they bring) on the national money laundering risk. Transactions and goods traffic between Finland and other countries may involve geographical risks. Finland may be used as a country of origin or destination but also as a country of transit.

According to the Mutual Evaluation Report on Finland prepared by FATF, Finland can be seen as a gateway between EU countries and countries outside the EU. According to the Mutual Evaluation Report, Finland's geographical closeness to Russia and the impacts of the trade relations between the two countries should be taken into account.[84] Tax audits of companies doing business in Russia have frequently revealed extensive use of tax havens and cash. In such cases, the sales and purchase receipts entered in the accounts do not always tally with the actual transactions. There are often indications of money laundering in the suspicious transfers of funds carried out as part of business operations with Russian

82 Contains details of the following types of crime: money laundering, money laundering violation, negligent money laundering and aggravated money laundering.

83 Grey economy & economic crime: Crime prevention, referred to on 22 January 2021.

84 FATF MER 2019, p. 7.

partners, and Finnish companies may have been used as intermediaries in the transfer of funds and in transactions between companies established in other countries.[85] It has also been determined that most of the criminal funds flowing from Russia to European banks originate from the shadow economy. Criminal actors in Russia use shell companies, making it difficult for Russian supervisory authorities to detect the recycling of funds through foreign bank accounts and companies.[86]

Russia's impact is also reflected in real estate transactions concluded in Finland. According to the statistics compiled by the National Land Survey of Finland, Russians made a total of 266 real estate transactions in Finland in 2018 and 2019. The total value of these transactions was about EUR 30 million.

In addition to Russia, Finland also has close trade links with the Baltic states and Nordic countries. Measured on the basis of total trade figures, Germany, Sweden, Russia, China and the Netherlands were Finland's largest trading partners in 2020.[87] Trade routes that are geographically close also increase illegal flows of goods and money. [88] Through Helsinki Airport, Finland also serves as an international air traffic hub, especially for Asian passengers.[89] In 2019, international transit passengers accounted for 38.6 per cent of all passengers.[90]

It was highlighted in the interviews with experts that many of the risks associated with customers are also connected with geographical risks. In this connection, the geographical aspect refers to the lists of high-risk countries compiled by FATF and the European Commission,[91] and as a rule, no transactions are conducted with customers from these countries.

85 Grey economy & economic crime: Shadow economy in east-west trade, referred to on 1 December 2020.

86 Financial Intelligence Unit 2018b, p. 23.

87 Finnish Customs: Graphs of Finland's foreign trade 2020, referred to on 23 November 2020.

88 FATF MER 2019, p. 18.

89 Kauppalehti 3 April 2019: Three new airlines start flying to Helsinki Airport – Two of them are Chinese, referred to on 23 November 2020.

90 Finavia: A total of 26 million passengers passed through Finavia's airports in 2019 – year of moderate growth in air traffic, referred to on 23 November 2020.

91 FATF keeps two separate lists of high-risk countries. The list 'High-Risk Jurisdictions subject to a Call for Action" ('blacklist') comprises the countries that have major inadequacies in their AML/CFT systems. The list 'Jurisdictions under Increased Monitoring' ('grey list') comprises the countries that have inadequacies in their AML/CFT systems but that are cooperating with FATF to improve the situation.

2.2.3 Customer due diligence

Customer due diligence referred to in chapter 3 of the Anti-Money Laundering Act is one of the key obligations laid down in the act. *Customer due diligence* comprises all the measures and obligations specified in the chapter that must be observed throughout the customer relationship using a risk-based assessment as a basis. In accordance with the risk-based assessment, when assessing risks arising from customer relationships, obliged entities must consider the money laundering and terrorist financing risks arising from customers, countries, geographical regions, products, services, transactions, distribution channels and technologies. It should be noted that even though customer due diligence is a key obligation under the Anti-Money Laundering Act, the concept 'customer' is not defined in the Anti-Money Laundering Act or the anti-money laundering directive. This can also be considered to have an impact on the formation and assessment of risks.

Identifying the customer and verifying its identity is part of customer due diligence. The obliged entities must identify their customers and verify their identity when establishing a permanent customer relationship. The customer must also be identified and their identity verified when:

1. the amount of the transaction or the total amount of linked transactions is at least EUR 10,000 and the customer relation is on an occasional basis or it is a question of a transfer of funds referred to in Article 3, point 9 of the payer information regulation amounting to more than EUR 1,000;
2. the transaction involving the sales of goods or the amount of linked transaction in cash totals at least EUR 10,000 and the customer relationship is on an occasional basis;
3. it is a question of a suspicious transaction and if the obliged entity suspects that the assets included in the transaction are used to finance terrorism or a punishable attempt to finance terrorism; or
4. the obliged entity suspects that the verification information on a customer whose identity has already been verified is not reliable or adequate.

By way of derogation from paragraphs 1 and 2 above, in gambling operations, the customer must be identified and their identity verified when the stake is wagered or the winnings collected or in both situations if the stake wagered or the winnings collected by the gambler totals at least EUR 2,000 as a single transaction or as linked transactions.

There is often heavy reliance on strong electronic identification in the identification of the customer and the verification of their identity. In that case, in terms of preventing money laundering, it is also essential for the parties issuing electronic identifiers and the parties brokering identification events to take the necessary measures to identify the customers and to verify their identity.

In a permanent customer relationship, customer due diligence is a continuous process. In addition to identifying the customer and verifying their identity, obliged entities must also have adequate monitoring arrangements in place concerning the type and extent of the customer's activities, duration of the customer relationship and the risks involved. Continuous monitoring helps to ensure that the customer's activities are in accordance with the information on the customer and their activities possessed by the obliged entity and the experience it has accumulated. It has been noted in a number of risk assessment sectors that continuous monitoring of customers is difficult and that sectoral actors are not sure which procedures they should apply to the customer relationship after they have identified the customers and verified their identity. Thus, continuous monitoring of customers involves vulnerabilities.

In the legislative project to overhaul the Anti-Money Laundering Act now under way,[92] changes will also be made to the provisions on customer due diligence. For example, in the future, obliged entities would no longer be able to apply simplified customer due diligence if the obliged entity detects unusual or suspicious transactions. It would also become illegal to establish and maintain anonymous customer relationships or customer relationships with fictitious names, while in occasional customer relationships, the lower limit for verifying customer identity would be set at EUR 1,000 when virtual currencies are transferred.

2.2.4 Technological development

Advances in technology expand the range of methods used and required in money laundering and in the prevention of this activity. Different types of electronic services and products provide new ways and channels for money laundering and may be attractive to criminals by offering anonymity and ways to obliterate funds. Considering new technologies in national risk assessments and in the risk assessments produced by obliged entities and supervisory authorities is based on FATF Recommendation 15 that concerns new technologies.[93]

FinTech or financial technology is a rapidly growing sector. It includes the information technology used to provide banking, insurance, financial, investment and payment services. Financial technologies include payment services, mobile wallets, virtual currencies and different types of electronic customer service.[94] RegTech means the use

92 Ministry of Finance project: Government proposal on amending the Act on Preventing Money Laundering and Terrorist Financing (in Finnish).

93 FATF 2012-2020 p. 17 and HE 38/2018, p. 21.

94 Financial Supervisory Authority: FinTech – financial sector innovations, referred to on 31 July 2020.

of new technologies for regulatory and supervisory purposes.[95] In terms of anti-money laundering activities, technologies can be used by introducing more effective procedures for supervising customer profiles and for submitting money laundering reports and by developing more effective cooperation between the authorities.[96] In March 2020, FATF issued guidelines on how Digital ID systems can be used to meet the customer due diligence requirement.[97]

Bank and payment accounts control system

The Act on the Bank and Payment Accounts Control System (571/2019) entered into force in 2019. The purpose of the act is to provide the authorities with better electronic access to information on the bank and payment accounts of citizens, companies and organisations. The users of the information collected using the control system are specified in the act. The purpose of the control system is to create a secure channel to obtain information from credit institutions, payment institutions, electronic money institutions and virtual currency providers. No new additional powers to access information are provided under the act as the control system offers new ways to retrieve information using electronic means.[98]

Under the existing national legislation, the bank and payment accounts control system comprises two parts: 1) bank and payment accounts register established by Finnish Customs; and 2) information retrieval systems maintained by credit institutions, payment institutions, electronic money institutions and virtual currency operators. As the implementation of the Act on the Bank and Payment Accounts Control System is making progress, it has become clear that the decentralised model set out in the act is both expensive and complex for competent authorities, credit institutions, payment institutions, electronic money institutions and virtual currency operators. Because of the limited powers and decentralisation set out in the existing legislation, the bank and payment accounts control system will probably be little used and it will not help to achieve the objectives of ensuring more effective combating of money laundering, terrorist financing and shadow economy envisaged when the system was designed. The challenges arising from the current situation have been recognised in connection with the national implementation of the financial information directive ((EU) 2019/1153). Because of this, in connection with the directive implementation project, it has been decided to draft changes to the Act on the Bank and Payment Accounts Control System to ensure

95 EU SNRA 2019, p. 3.

96 Europol 2017, p. 36.

97 FATF 2020b.

98 Finnish Customs: Bank and Payment Accounts Control System, referred to on 2 December 2020.

more effective use of the system and thus also more effective combating of money laundering and terrorist financing.[99]

2.3 Insurance companies

2.3.1 Operating environment

Oversight of the organisations operating in the Finnish insurance market is the responsibility of the Financial Supervisory Authority. Under the Anti-Money Laundering Act,[100] the following organisations operating in the sector are subject to supervision:

- insurance companies and special purpose entities referred to in the Insurance Companies Act (521/2008)
- earnings-related pension insurance companies referred to in the Act on Earnings-Related Pension Insurance Companies (354/1997)
- branches of insurance companies from third countries referred to in the Act on Foreign Insurance Companies (398/1995)
- local mutual insurance associations referred to in the Local Mutual Insurance Associations Act (1250/1987)
- insurance intermediaries, ancillary insurance intermediaries, and branches of foreign insurance intermediaries and ancillary insurance intermediaries operating in Finland and referred to in the Act on Insurance Distribution (234/2018).

According to Finance Finland, at the end of 2019, there were 47 Finnish insurance companies operating in Finland employing a total of about 10,000 persons. At the end of 2019, there were also 20 branches of foreign insurance companies operating in Finland. Registered insurance broker companies totalled 90.[101] In 2019, insurance companies operating in Finland accumulated about EUR 26 billion in premium income and paid a total of almost EUR 27 billion in insurance payments. Most of the premium income and insurance payments were related to pension insurance policies.[102]

99 It is also proposed in the financial information directive project to expand the group of authorities that in addition to having the right to use the bank and payment accounts control system to prevent money laundering and terrorist financing are also authorised to use it to prevent, detect and inves- tigate serious crime.

100 Non-life insurance companies also fall within the scope of the Anti-Money Laundering Act even though this is not a requirement under the EU directives or FATF recommendations.

101 Finance Finland 2019b, p. 7.

102 Finance Finland 2019b, p. 6.

Finnish insurance companies typically offer insurance policies tailored to the needs of specific groups, such as consumers, companies, and agricultural and forestry customers.[103] Moreover, there is often a division into statutory[104] and voluntary insurance policies.

Insurance companies and earnings-related pension insurance companies submitted a total of 134 money laundering reports to the Financial Intelligence Unit in 2019.[105]

2.3.2 Money laundering risks

The overall risk facing the insurance sector is at level two (**moderately significant**). A total of 28 experts from the public and private sector took part in the assessment.

Inadequacies in the exchange of information (especially between sectoral actors and credit institutions) are seen as a significant risk in the insurance sector in terms of vulnerability. For example, actors in the insurance sector are unable to verify the actual holders of the bank accounts given by their customers and they must pay the insurance payments to the accounts given by the customers without receiving any verification from the bank.

Some of the most significant risks facing the sector are also deemed to be associated with insurance broker activities. Insurance brokers are focused on sales and financial operations and in such activities **AML measures can be seen as a negative factor or an additional burden**. Insurance brokers report on their financial activities to the Financial Supervisory Authority, but the reports do not include any information on AML matters. Money laundering risks associated with the processing of funds are also identified as a moderately significant risk in insurance broker activities. They may manifest themselves in **excessive trust in the customer relationship monitoring by banks, verification of the source of customers' funds, customer due diligence or identification of beneficial owners**. In such cases, the obliged entities may not strive to determine whether any unusual transactions have taken place.

Complex business and ownership arrangements by the customer and new corporate customers are seen as a moderately significant risk in life and non-life insurance operations as they make the identification of beneficial owners more difficult. The

103 Interview with an expert.

104 Motor liability insurance, insurance against treatment injury and environmental impairment liability insurance are statutory non-life insurance policies, see Ministry of Social Affairs and Health: Statutory insurances against loss of damage, referred to on 8 October 2020.

105 Financial Intelligence Unit 2020a, p. 9.

customer's business sector is a key factor in this respect because the complex ownership arrangements are considered risky, especially in the construction sector. Construction sector actors must take out specific insurance policies before they can start working on a contract, which adds to the challenging nature of the sector.

Paying insurance premiums from accounts not belonging to the customer is considered risk if there is no logical explanation for the practice. The risk is considered to apply to all insurance products.

Insurance products in which it is easy to transfer assets and convert them into cash are also seen as a moderately significant risk. Such products include flexible endowment assurance policies and capital redemption policies. In such products, funds can be withdrawn in full or in part and the one-off agreement payments can be substantial.

2.4 Payment service providers (incl. currency exchange and hawalas)

2.4.1 Operating environment

Payment service providers comprise a wide range of different services and products related to the execution of payments and transfer and conversion of funds. Oversight of the payment service providers is the responsibility of the Financial Supervisory Authority and currency exchange offices are supervised by the Regional State Administrative Agency for Southern Finland. Under the Anti-Money Laundering Act, the following organisations operating in the sector are subject to supervision:

- payment institutions and electronic money institutions referred to in the Act on Payment Institutions (297/2010)
- natural persons and legal persons referred to in sections 7 and 7a of the Act on Payment Institutions
- branches of foreign payment institutions and electronic money institutions op- erating in Finland
- foreign payment institutions and electronic money institutions if the payment institution offers services in Finland through an intermediary without establishing a branch in Finland.

A payment service provider wishing to offer its services in Finland must be granted an authorisation by the Financial Supervisory Authority. Alternatively, the Financial Supervisory Authority may decide that in activities meeting specific requirements,

payment services may be provided without an authorisation.[106] Moreover, an actor authorised to operate as a payment service provider in an EEA country may offer payment services in Finland under the passporting system. A total of 76 payment service providers overseen by the Financial Supervisory Authority have been registered in Finland. A total of 264 agents appointed by foreign payment service providers authorised to offer payment services in Finland also operate in Finland.

Between 1 March 2019 and 28 February 2021, the financial intelligence units of Finland and Sweden carried out the Black Wallet project in which money laundering and terrorist financing risks in the field of financial technology were identified.[107] The project was funded by the EU (ISF). In addition to identifying risks, the project also described the FinTech sector as a whole, with emphasis on products and services used in the transfer of funds.[108]

Hawalas[109] meet the criteria for the provision of payment services and for this reason, the authorisation for providing payment services is, as a rule, also required for hawalas. The hawala system is used to transfer funds from Finland to such regions as North and Northeast Africa as well as the Middle East.[110] A total of 12 hawalas operating in Finland have been granted the authorisation to provide payment services. These actors are registered providers of payment services, as referred to in section 7 of the Act on Payment Services.

In addition to payment services, payment service providers may also offer currency exchange services. According to the Regional State Administrative Agency for Southern Finland, there were a total of 15 currency exchange offices operating in Finland in 2019.

Payment service providers (including those offering currency exchange services) submitted a total of 32,790 money laundering reports in 2019.[111] It should be noted that there were no hawalas among these actors.

106 Financial Supervisory Authority: Payment service providers, referred to on 22 July 2020.

107 The Risk Indicators report and Risk Indicators, the first products of the Black Wallet project have now been published, see Black Wallet 2020a and Black Wallet 2020b.

108 National Bureau of Investigation: Black Wallet, referred to on 22 July 2020.

109 Hawala is a non-registered and unregulated system for transferring funds or an unofficial value transfer system (see PRIO 2007), in which members of a diaspora send money to support their families or local businesses and their development in their home countries. The hawala system is mainly used to transfer funds to regions where bank services are only available on a limited scale.

110 Financial Supervisory Authority 2020b, p. 8.

111 Financial Intelligence Unit 2020a, p. 9.

2.4.2 Money laundering risks

Payment service providers

The overall risk facing payment service providers is at level three (**significant**). A total of 20 experts from the public and private sector took part in the assessment.

New payment service providers entering the sector and new technologies with functionalities that are difficult to understand and supervise are seen as the most significant vulnerabilities and thus also major risks in the sector. It may be difficult to understand the operating principles of the new services and technologies and the transactions carried out using them. The difficulty of understanding the services also impacts the supervision, which should, however, apply to all areas of the sector on a uniform basis. The fact that the authorities do not fully understand the functioning of the services and transactions and their inability to keep pace with technological development was also identified as a threat in the Black Wallet project.[112]

The view is that **small actors in the sector are not adequately familiar with anti-money laundering procedures**, which also manifests itself in a vulnerability for money laundering. Compliance functions[113] of small actors may be inadequate or non-existent, which means that there are no clear procedures for identifying suspicious transactions. Inadequate customer due diligence procedures and in particular deficient procedures for identifying beneficial owners and money remitters give rise to specific threats, such as the use of **intermediaries**[114] **and money mules**[115] **in payment services**.

Retroactive monitoring of the payments is also a very significant risk, and it can be considered a vulnerability. International payment transfers are also quick, which means that at the time of the monitoring, the funds have already been transferred and can no longer be stopped. **Limitations on the exchange of information** between banks and other actors in the sector significantly contribute to the risk. As a result of the limitations, there is no common channel for information sharing between the parties. Data protection and other secrecy provisions also make it more difficult for the authorities to exchange information. The view is that more open exchange of information between supervisory

112 Black Wallet 2020a, p. 14 and Black Wallet 2020b, p. 3.

113 The term 'compliance' refers to the procedures used by a company to ensure that its internal processes are in accordance with the law and required standards (see Hoppu – Hoppu – Hoppu 2020, p. 407).

114 In this context, 'intermediary' refers to persons that act in their own name on behalf of other persons.

115 The Financial Intelligence Unit has highlighted the increasing use of professional money mules in Finland. In the mule activities detected by the agency, individuals arriving from other countries open bank accounts using false personal data. Proceeds of crime are transferred to these accounts from which they are quickly transferred to other accounts or withdrawn in cash. See Financial Intelligence Unit 2018b, p. 24.

authorities and actors would also mitigate the risk concerning the **challenges arising from the identification of money laundering scenarios**. This risk is currently seen as significant. Inadequate understanding of risk scenarios also leads to inadequate monitoring procedures.

The **ease of converting types of money into other types in payment services** is seen as a significant risk, which mainly concerns cash and electronic money. A criminal actor may take out a loan and use it to buy valuable items that can be converted into cash (such as electronical equipment).

Using a false identity with criminal intent is also seen as a significant risk in payment services. A criminal actor (threat factor) may pose as a company representative and the electronic methods used by payment service providers to verify identities cannot prevent such activities.

Verifying the source of funds is difficult mainly because money can be quickly transferred across national boundaries. This is a significant risk, and it is also associated with the retroactive nature of the payment monitoring procedures referred to above.

Hawalas

The overall risk facing hawalas is at level four (**very significant**). A total of 16 experts from the public and private sector took part in the assessment. In its risk assessment published in 2020, the Financial Supervisory Authority also concluded that the risk facing money remittance services is significant.[116]

There are a number of vulnerabilities with regard to hawalas that concern supervision. There are indications that **some of the hawalas use their own systems in which tracing money transfers is more difficult than in the transfers carried out using banks**. It is difficult to obtain information about the sector, which also makes the targeting of supervision difficult. The fact that hawalas are often unable to establish and verify the sources of the funds is also seen as a very significant risk. What are called 'money collectors' are also a feature of the hawala activities. They collect large amounts of cash from customers and then forward the money for transfer. In such cases, it is impossible to establish the owner of the sent funds or the actual origin of the funds.

In hawala activities, **the funds are often transferred to high-risk regions or to coun- tries or persons subject to sanctions**. These are also potential threat factors, which constitutes

116 Financial Supervisory Authority 2020a, p. 4.

a very significant money laundering risk from the geographical perspective. The Financial Supervisory Authority has made similar observations in its own risk assessment concluding that the risk is increased by a poor supervisory regime and inadequate AML procedures in the countries to which the money is sent.[117]

Use of intermediaries and money mules are also seen as a risk from the threat perspective in the hawala activities. The inadequate AML procedures used by hawalas allow criminal actors to operate behind the transactions.

Non-registered hawalas are seen as a very significant risk and their exact number or extent is not known. Even though hawalas are required to apply for authorisation as payment service providers, there are indications that activities are also carried out without appropriate authorisation. Non-registered hawalas are not actively monitored by the Financial Supervisory Authority. Due to the nature of the activities, persons using nonregistered hawalas and suffering losses as a result do not necessarily notify the Financial Supervisory Authority.

Currency exchange

The overall risk facing currency exchange services is at level two (**moderately significant**). A total of 19 experts from the public and private sector took part in the assessment.

The most significant risks primarily manifest themselves in vulnerabilities. **Inadequate knowledge of AML methods among small actors** is seen as the most significant risk as it is one factor allowing money laundering to take place. There is a wide range of actors of different sizes operating in the sector and this is also reflected in anti-money laundering capabilities. **Small currency exchange operators in particular can be exploited in the efforts to obliterate the origin of the funds**, which is seen as a significant risk.

Cash is extensively used in currency exchange activities, which highlights the risk arising from the **difficulty of establishing the source of the funds**. The one-off nature of the customer relationships often adds to the difficulty of establishing the origin of the money.

117 Financial Supervisory Authority 2020b, p. 8.

2.5 Gambling operators

2.5.1 Operating environment

There are two gambling operators in Finland: one with exclusive rights to organise gam- bling in Mainland Finland and the other one with similar exclusive rights in Åland. The Mainland Finland operator may only organise gambling in Mainland Finland, and the operator in Åland may not organise gambling in Mainland Finland. Under the Anti-Money Laundering Act, the National Police Board supervises the activities of the exclusive operator operating in Mainland Finland and (to a limited extent) the activities of its agents.[118] In practice, the supervision is the responsibility of the Gambling Administration of the National Police Board. Gambling operations in Åland are supervised by Lotteriinspektionen (established in 2017), which comes under the auspices of the Provin- cial Government. The anti-money laundering legislation is applied as follows:

- All operations of the exclusive operators
- provisions of chapters 3 and 4 of the Anti-Money Laundering Act are applied to business operators and organisations that supply participation fees and registrations for participation for gambling provided by the exclusive operators referred to above if the exclusive operator has tasked other business operators or organisations with the identification and registration ('agents')
- chapters 7 and 8 of the Anti-Money Laundering Act are applied to the supervision of the business operators and organisations ('agent') in the manner laid down in the chapters in question.

Finns are among Europe's top gamblers in terms of money spent on the games.[119] In a survey carried out by the Finnish Institute for Health and Welfare, some 78 per cent of the respondents aged between 15 and 74 said that they had spent money on gambling during the preceding 12 months.[120]

Mainland Finland

Provisions on running gambling operations in Mainland Finland are contained in the Lotteries Act (1047/2001).[121] Provisions on the manner in which the Mainland Finland

118 According to information provided by the Mainland Finland gambling operator (Veikkaus), it has about 6,300 gambling locations, see Veikkaus Ltd: Pelipaikat ja pelit [*Gaming locations and games*]., referred to on 2 November 2020.

119 Finnish Institute for Health and Welfare: Gambling, referred to on 7 January 2021.

120 Finnish Institute for Health and Welfare 2019, p. 5.

121 The Ministry of the Interior is currently overhauling the Lotteries Act. The draft Government proposals was being circulated for comments in early 2021. See Ministry of the Interior project: Overhaul of the Lotteries Act, referred to on 25 February 2021.

exclusive operator can run gambling operations are also contained in the Government decree (1414/2016)[122], and provisions on gambling rules in the Ministry of the Interior decree (2719/2020).[123] Purpose of the supervision of lotteries (and thus also gambling, which is a form of lotteries) is to ensure the legal rights of the lottery participants and prevent misuse and crime. Under the Lotteries Act, the general minimum age for gambling is 18 years. Games offered by the Mainland Finland exclusive operator can be played online and in sales outlets. The games offered by the exclusive operator include pools, betting, slot machine games and casino games. Many of the games can also be played in the agents' sales outlets. In addition to its own specific game rooms and gambling locations, the operator also has a casino in Helsinki. The operator also plans to open a casino in Tampere in December 2021.[124]

The profit for the gambling games offered by the Mainland Finland exclusive operator amounted to EUR 1,690.7 million in 2019. Online games accounted for 31.8 per cent of this total. According to the Gambling Administration of the National Police Board, the profits generated by foreign online gambling games played in Finland are currently estimated at about EUR 200 million. The profits generated by online gambling games outside the Mainland Finland exclusive system and the self-governing Province of Åland amounted to less than EUR 300 million.[125]

Åland

Provisions on the running of lotteries in Åland are contained in the provincial lotteries act 1966:10 (Landskapslag om lotterier). The exclusive operator of Åland offers online games in the form of betting and casino games, and online games are its largest business segment. In addition to online games, the exclusive operator also has game machines and game desks in Åland and on cruise ships operating in the Baltic Sea and a casino in Mariehamn.[126] In 2019, the operator had a turnover of EUR 114.2 million and online games accounted for EUR 84.5 million of this total.[127]

122 The Government decree in question also contains provisions on participation in gambling, rounding up of the winnings, distribution of unclaimed winnings, and the maximum number of slot machines, specific game rooms, and the number of casinos. Under section 11 of the decree, the gambling company may run casino operations in one casino in Helsinki and in one casino in Tampere.

123 The Ministry of the Interior decree contains detailed rules of all gambling games offered in Mainland Finland. The rules of the games contain a number of elements that impact the attractiveness of gambling in terms of money laundering. The rules impose restrictions on such matters as the level of stakes and the payment of winnings. The Ministry of the Interior decree is frequently amended.

124 Veikkaus Ltd: Press release 28 August 2020, referred to on 2 November 2020.

125 Police: Manner-Suomen rahapelimarkkinoiden kehitys [*Development of Mainland Finland's gambling market*], referred to on 19 January 2021.

126 Lotteriinspektionen: Åland och spel, referred to on 2 November 2020.

127 PAF 2019, p. 55.

Provincial acts 2016:10 and 2016:11 contain provisions on the supervision of lotteries and the last-mentioned also amended the provincial lotteries act.

A total of 11,901 money laundering reports concerning gambling were submitted to the Financial Intelligence Unit in 2019.[128] There has been a decline in the number of reports in recent years.

2.5.2 Money laundering risks

The overall risk associated with gambling operations in Mainland Finland and Åland is at level two (**moderately significant**). A total of 20 experts from the public and private sector took part in the assessment.

Overall risks facing the sector

The use of foreign gambling companies and the vulnerability associated with it, which arises from fragmented supervision and challenges involving access to information, are seen as the most significant money laundering risk. This has been identified as a significant risk in Mainland Finland and Åland. The games offered by foreign gambling companies are all played online.[129] Spending the winnings won in the games offered by foreign gambling companies in Finnish games is seen as a challenge by domestic exclusive operators. There may be situations in which Finnish citizens play games offered by foreign gambling companies, transfer the winnings to their own accounts and use them to play games offered by Finnish exclusive operators. When measures are taken to establish the source of the funds, the individuals concerned may claim that they are winnings won outside Finland even though the funds have actually been obtained by other means (such as fraud). In such situations, it is difficult to verify whether the funds actually are winnings won in the games offered outside Finland. Foreign gambling companies may have an effective supervisory regime but in addition to supervised gambling companies, there may also actors that are entirely outside supervision.[130]

Betting in which the winnings are paid immediately after the end result is clear and in which measures are taken to ensure that a certain percentage of the winnings is returned is also seen as a significant risk. Betting constitutes a major risk in situations in which the player places bets on the same object on different options offered by different

128 Financial Intelligence Unit 2020a, p. 9.

129 Playing online games offered by operators outside Finland has not been criminalised.

130 The observation is based on expert assessments.

gambling companies or operators. In such cases a gambling company or operator is unable to check whether the player bets on a win of the home team and the visiting team simultaneously. **A situation in which a player plays games offered in Mainland Finland and Åland** is seen as a problem. In such situations, neither of the operators knows the volume of the player's gambling activities, which also makes it more difficult to detect suspicious transactions.

A significant money laundering risk also arises when **funds are transferred to the player account and from there to the destination account but the source account and the destination account are different**. From the perspective of the gambling company or operator, this is a question of an obstacle to information exchange between obliged entities and the bank account ownership details cannot be checked with the other obliged entity. The gambling company or operator subject to the reporting obligation may, under the existing anti-money laundering legislation, notify the bank if the money laundering report has been prompted by the funds transferred between the source and/or the destination account.[131] A situation in which the **money is circulated via the player** account back to the same account from which the original transfer was made is seen as a moderately significant money laundering risk.

The **use of remote identification** in connection with gambling is seen as a moderately significant risk. In such situations, the person to be identified is not present at the identification. Remote identification is connected with enhanced customer due diligence, which does not, however, prevent misuse. The means of identification required for strong electronic identification may have been stolen or given to another person. The purpose of such action has been to conceal the real identity of the individual laundering money through gambling. **Anonymous gambling in which the players are not identified, or their identity is not verified or it cannot be done retroactively** are also seen as high-risk situations.[132]

Inadequate capacity of gambling providers to detect suspicious transactions constitutes a risk for example when the players are not identified, or their identity is not verified in practice in the required manner. The ability of the gambling providers to develop their customer due diligence and continuous customer monitoring processes helps to mitigate the risk because it also increases the capacity to identify suspicious transactions.

131 See chapter 4, section 4(3) of the Anti-Money Laundering Act on other situations in which information can be disclosed.

132 See Ministry of the Interior project: Overhaul of the Lotteries Act. Obligator identification in all gambling in Mainland Finland would be a requirement under the new act.

Mainland Finland

Gambling in casinos is seen as a significant risk in Mainland Finland. Gambling in casinos may involve high stakes and thus also substantial sums of money. Money launderers consider small or occasional losses acceptable as the purpose of money laundering is not to generate profits but the obliterate the source of funds. In terms of risk, the key issue in gambling in casinos is the verification of the source of the funds used for gambling and the risk is mitigated if this can be carried out as required. Illegal casinos that do not comply with the requirements laid down in the Anti-Money Laundering Act are also seen as a risk.

The **use of ticket vending machines** has also been identified as a risk. In that case, the personnel do not have contacts with the customers, making customer identification more difficult. Tickets are primarily used to pay for games and to claim winnings in foreign game machines.

Åland

Casinos on cruise ships are seen as a moderately significant risk with regard to Åland. The risk primarily arises from inadequacies in customer due diligence and the inability to properly establish the source of the funds. The fact that most of the customers are from outside Finland is the main challenge in this respect.

2.6 Credit institutions

2.6.1 Operating environment

Credit institutions are supervised by the Financial Supervisory Authority. Under the AntiMoney Laundering Act, the following organisations operating in the sector are subject to supervision:

- credit institutions and branches of third-country credit institutions referred to in the Act on Credit Institutions (610/2014)
- with regard to the actors referred to above, also the branches of similar foreign organisations and foreign organisations that offer services in Finland through an agent without establishing a branch in Finland.

Credit institutions accept deposits or other funds repayable on demand from the public and offer credit or other funding on their own account. The activities of credit institutions partially overlap with other sectors reviewed in the risk assessment as credit institutions

can offer payment services and investment services within the framework of their authorisation.[133]

There were a total of 246 credit institutions and 790 bank branches in Finland at the end of 2019.[134] In recent years, banking sector operators have increasingly developed into financial groups that, in addition to credit institutions, also include fund management companies and insurance companies.[135] Most of the credit institutions operating in Finland belong to a banking group or conglomerate and in 2019, the Finnish banking sector comprised a total of 12 banks (when consideration is given to the group structure).[136] In 2019, the operating profit of the Finnish banking sector totalled EUR 3.4 billion. The two largest banking groups had a combined market share of 60 per cent.[137]

Finnish credit and financial institutions (banks) submitted a total of 10,024 money laundering reports in 2019.[138]

2.6.2 Money laundering risks

The overall risk facing credit institutions is at level three (**significant**). A total of 35 experts from the public and private sector took part in the assessment. Good understanding and competence among the actors concerning the money laundering risks facing the sector are seen as a factor mitigating the risk.

The sentence given by the Helsinki District Court on 13 April 2018[139] is an example of the money laundering scenarios facing credit institutions.

133 Financial Supervisory Authority: Payment service providers, referred to on 3 November 2020.

134 Finance Finland 2019a, p. 7.

135 Finance Finland: Pankit merkittäviä kansantaloudelle [*Banks play a vital role in the national economy*], referred to on 2 November 2020.

136 Finance Finland 2019a, p. 7.

137 Finance Finland 2019a, pp. 8-9.

138 Financial Intelligence Unit 2020a, p. 9.

139 Sentence of the Court of Appeal of Helsinki, 13 April 2018 No. 18/116182.

Case involving a mule

Person A had received in their bank account a total of EUR 17,000, which had been transferred from a foreign bank account by means of fraud. Immediately after re- ceiving the money, Person A had transferred EUR 7,000 to the bank account of Person B and EUR 9,000 to the bank account of Person C. Person A had kept and spent the rest of the money. According to the court, Person A was guilty of aggra- vated money laundering because the laundered property had to be considered of extremely high value. The conduct was also considered systematic and thus the act had to be considered of aggravated nature when assessed as a whole. The sentence is legally valid.

International connections are considered as the most significant risks facing credit institutions. **International payment traffic, its speed and use for money laundering, and large transaction volumes with non-EEA countries**, in which legislation, the supervisory regime and level of corruption may differ from the situation in Finland, are seen as particularly high risks. Funds transferred between Finland and non-EEA countries are seen as a risk. Establishing the sources of the funds transferred to Finland from non-EEA countries is particularly difficult.

It has been noted that **payment service providers outside credit institutions pose challenges to the monitoring of transactions**. Payment information may be concealed by using payment service providers outside credit institutions. In that case, credit institutions do not necessarily see the payee details but can only determine that a transaction has been carried out using the services of a specific payment service provider. Moreover, the **large number of transactions** makes monitoring and the detection of suspicious transactions more difficult. It has been noted that ensuring effective monitoring allowing the detection of unusual transactions and finding a balance between wrong and right hits requires continuous efforts.

Cash and establishing the source of cash funds are also seen as a significant risk. Cash is associated with significant money laundering risks because determining and tracing the origin of the funds is practically impossible. FATF is also of the view that transporting cash across national boundaries and using it in money laundering is one of the oldest and most typical forms of money laundering.[140] The **wide variety of products and services** offered

140 FATF 2015a, p. 3.

by credit institutions also impacts the identification, prevention and supervision of money laundering scenarios, especially in connection with products and services that have been introduced recently.

It has also been noted that credit institutions face **money laundering risks associated with their customers' customers and customers' partners**. These risks mainly depend on the due diligence practices that credit institutions are expected to apply to their customers' customers and customers' partners.

As digital banking services are become more widespread, **technological development** is also seen as a significant risk. This also has an impact on customer due diligence and customer identification procedures. The new technologies used by credit institution customers in customer due diligence and customer identification are also seen as a money laundering risk.

Exploiting **correspondent banking** for money laundering purposes is also seen as a significant risk. A correspondent bank is a bank that has concluded an agreement with a bank in another country (such as Finland) on carrying out assignments involving liabilities.[141] The country of location of the correspondent bank and the level of supervision are two factors impacting the risk. Payment chains, a typical feature of correspondent banking, increases the risks arising from this type of activity. The ability of a Finnish credit institution to determine[142] whether the other party is sufficiently familiar with the risks also impacts the risk level. For this reason, the risk arising from a correspondent banking relationship should be reviewed on a regular basis.

2.7 Financial institutions, other providers of financial services and debt collectors

2.7.1 Operating environment

Financial institutions, other providers of financial services and debt collectors comprise a large number of financial sector actors. Under the Anti-Money Laundering Act, the

141 The number of obliged entities registered by the Financial Supervisory Authority is based on the figures given by the Financial Supervisory Authority on 26 January 2021. The number of obliged entities registered by the Regional State Administrative Agency for Southern Finland has been retrieved from the registers maintained by the Regional State Administrative Agency on the following dates: debt collectors on 6 November 2020; peer-to-peer lenders on 30 October 2020; providers of financial and investment services on 11 November 2020; and companies providing financial services on 22 February 2021.

142 A credit institution must, using enhanced customer due diligence methods, determine the ability of a credit or financial institution established in a non-EEA country to act as a counterparty. The same applies to dealing with counterparties operating in an EEA country.

Financial Supervisory Authority[143] and the Regional State Administrative Agency for Southern Finland are tasked with overseeing the sector. The following actors in the sector are subject to oversight:

Table 7. Financial institutions, other providers of financial services and debt collectors, number of actors and supervisory authorities.

Actor	Number of obliged entities[144]	Supervisory authority
Custodians[145]	Seven actors	Financial Supervisory Authority
Providers of investment services[146]	54 actors	Financial Supervisory Authority
Central securities depositories[147]	1 actor	Financial Supervisory Authority
Fund management companies[148]	29 actors	Financial Supervisory Authority
Alternative investment fund managers [149]	128 actors	Financial Supervisory Authority

143 The Financial Supervisory Authority also maintains a register of warnings concerning unauthorised service providers. The register is regularly updated and it lists all service providers whose activities are not in compliance with the legislation or the supervisory authority suspects that the operations are unauthorised. In August 2020, the register contained the names of 154 actors and most of them are suspected of providing investment services in Finland without a proper authorisation. See Financial Supervisory Authority: Warnings concerning unauthorised service providers, referred to on 4 August 2020.

144 The number of obliged entities registered by the Financial Supervisory Authority is based on the figures given by the Financial Supervisory Authority on 26 January 2021. The number of obliged entities registered by the Regional State Administrative Agency for Southern Finland has been retrieved from the registers maintained by the Regional State Administrative Agency on the following dates: debt collectors on 6 November 2020; peer-to-peer lenders on 30 October 2020; providers of financial and investment services on 11 November 2020; and companies providing financial services on 22 February 2021.

145 Custodians authorised under the Act on Common Funds (213/2019) and authorised deposit banks referred to in the Act on Credit Institutions (610/2014).

146 Investment service companies referred to in the Act on Investment Services (747/2012). Deposit banks are not included in the figure.

147 Central securities depository referred to in the Act on the Book-Entry System and Settlement Activities (348/2017), including the registration fund and settlement fund established by it.

148 Fund management companies referred to in the Act on Common Funds (213/2019).

149 Alternative investment fund managers that have been authorised to act as alternative investment fund managers under the Act on Alternative Investment Funds Managers (162/2014), and alternative investment fund managers subject to registration obligation and referred to in the same act. The figure also includes fund management companies authorised to act as alternative investment fund managers.

Actor	Number of obliged entities	Supervisory authority
Crowdfunding intermediaries[150]	13 actors	Financial Supervisory Authority
Account operators[151]	Nine actors	Financial Supervisory Authority
Housing loan intermediaries[152]	Four actors	Financial Supervisory Authority
Companies providing financial services (other than those supervised by the Financial Supervisory Authority), such as providers of consumer credit, providers of financial leasing, and parties engaged in other types of financial and guarantee operations.	96 actors	Regional State Administrative Agency for Southern Finland
Peer-to-peer lenders[153]	Five actors	Regional State Administrative Agency for Southern Finland
Providers of investment services (other than those supervised by the Financial Supervisory Authority)[154]	Seven actors	Regional State Administrative Agency for Southern Finland
Debt collectors[155]	78 actors	Regional State Administrative Agency for Southern Finland

Alternative investment fund managers are the largest group of actors in the sector. Many fund management companies are also licensed to act as alternative investment fund managers. An alternative investment fund is an entity or other type of collective investing where funds are raised from a number of investors with a view to investing them

150 Crowdfunding intermediaries referred to in the Crowdfunding Act (734/2016) and other actors licensed as crowdfunding intermediaries.

151 Account operators and Finnish offices of foreign organisations authorised to act as account operators referred to in the Act on the Book Entry System and Clearing Operations (749/2012). The figure includes Finnish bank groups and branches of foreign banks that are authorised to make entries in the book entry system.

152 Finnish credit intermediaries and Finnish branches of foreign credit intermediaries referred to in the Act on Intermediaries of Consumer Credit related to Residential Property (852/2016).

153 Business operators falling within the scope of the Act on the Registration of Certain Credit Providers and Credit Intermediaries (853/2016) when they act as intermediaries of peer-to-peer loans.

154 Actors providing the service referred to in chapter 2, section 3(1) (1-8) of the Act on Investment Services (747/2012) as part of their business operations or on a professional basis.

155 Debt collectors referred to in the Act on the Registration of Debt Collectors (411/2018).

in accordance with a defined investment policy. Management of alternative investment funds comprises both portfolio management and risk management.[156] Providers of investment services are the second major category of actors in the sector. Investment service companies provide investment-related services, such as asset management, investment advice and carrying out of assignments relating to financial instruments.[157]

Debt collection can also be considered an important part of the sector in relation to the number of actors. Debt collection means the recovery of claims on behalf of someone else or the recovery of one's own claims when the claims have been received for the purpose of recovery.[158] Debt collection consists of measures aimed at persuading the debtor to voluntary repay overdue debts. Debt collectors must be entered in the register of debt collectors maintained by the Regional State Administrative Agency for Southern Finland.

In the 2015 national risk assessment, the supervision of peer-to-peer lenders operating online was seen as inadequate as the supervision was not the responsibility of the Financial Supervisory Authority or the Regional State Administrative Agency for Southern Finland. Transactions in the lenders' segregated accounts were not subject to external supervision either.[159] Peer-to-peer lenders are now obliged entities supervised by the Regional State Administrative Agency for Southern Finland and they are obliged to submit their details to the register of lenders and peer-to-peer lenders.

Credit and financial institutions (other than banks) submitted a total of 9,247 money laundering reports in 2019. It should be noted, however, that one major actor accounted for 99.2 per cent of all reports. In 2019, investment service companies submitted nine money laundering reports, debt collectors eight reports and peer-to-peer lenders three reports.[160]

2.7.2 Money laundering risks

The overall risk facing the sector is at level two (**moderately significant**). A total of 34 experts from the public and private sector took part in the assessment. The money laundering risk facing debt collectors is estimated to be lower than that associated with financial institutions and other providers of financial services.

156 Financial Supervisory Authority: Alternative investment fund managers (AIFMs), referred to on 11 November 2020.

157 Financial Supervisory Authority: Investment firms, referred to on 11 November 2020.

158 Regional State Administrative Agency for Southern Finland: Debt collection, referred to on 22 July 2020.

159 National risk assessment of money laundering and terrorist financing 2015, p. 107

160 Financial Intelligence Unit 2020a, p. 9.

Remote identification is seen as a moderately significant risk in the sector. In many of the services provided in the sector, there are no face-to-face customer contacts, which means that any vulnerabilities arising from remote identification increase the risk even more. Remote identification is seen as particularly risky in connection with **foreign customers** as in their case, the identification of the persons behind the customer relationship and thus also the identification of beneficial owners is seen as problematic.

One-off assignments are also seen as risky because it is difficult to relate them to the ordinary transactions of the actors in the absence of a permanent customer relationship. Identifying potential suspicions arising from one-off assignments is made more difficult because financial institutions do not offer monitored accounts as a service. At the same time, the fact that such accounts are not offered can be seen as a factor mitigating the overall sectoral risk.

Supervision of the companies operating in the sector comes within the purview of two supervisory authorities, depending on the products and services that they offer. This is seen as a moderately significant risk because in the absence of centralised sector-specific supervision, it is difficult to form an overall picture of the sector and the risks facing it.

Financial institutions and other providers of financial services

A total of 33 experts from the public and private sector took part in the assessment.

Peer-to-peer loans are seen as the most significant risk. Peer-to-peer loans are connected with inadequate understanding of the products and services contained in them, which means that potential misuse and criminal operating models associated with the loans are not identified. Threat factors (criminals) may try to exploit these gaps **by using intermediaries**. Inadequate customer due diligence and ease of obtaining credit facilitate the use of intermediaries in the sector.

Supervision-related problems arising from the undefined nature of financial services also constitute a significant risk. Providers of financing services have been obliged to enter their details in the money laundering supervision register since 1 July 2019. However, it is unlikely that all actors subject to the registration obligation have submitted their details. This makes it more difficult for the supervisory authorities to get an overview of the total number of actors in the sector and supervise their operations.

Unnecessary borrowing and quickly repayable transactions are also seen as risks associated with financial services as establishing the sources of the repaid funds is critical from the risk perspective.

Challenges arising from the verification of the sources of foreign funds are seen as the most significant risk facing investment services. To a great extent, the risk also depends on geographical factors, which means that if the funds originate from a country with a high money laundering risk, the certificate of origin or the information contained in the document may be of limited value.

Investment services often include **complex ancillary services and products**, the supervision of which is on a fragmented basis. As with general risks facing the sector, work of the supervisory authorities is hampered by the absence of a unified overall picture of the risks associated with investment service products. The risk can only be mitigated by ensuring a more centralised or a more coordinated supervisory regime.

Wealthy domestic customers and potential irregularities concerning the sources of their funds are also seen as a risk. Establishing the origin of domestic customers' funds is considered easier than determining the sources of foreign funds, which may mitigate the risk. At the same time, however, the assumption that the funds of wealthy domestic customers only come from legal sources may lead to inadequate certificates or origin.

Sales of fund units relatively soon after they have been acquired is seen as a moderately significant risk. The aim of such activities is to quickly obliterate the origin of the proceeds of crime by selling and buying fund units.

Debt collectors

A total of 17 experts from the public and private sector took part in the assessment.

Making overpayments in the hope of refunds is seen as a significant risk. **Bogus transactions** are also seen as a risk and judgements by default in particular make such operating models economically attractive.

Unawareness of money laundering risks among the actors is also a significant risk. The risk greatly depends on the size of actor, which is reflected in risk awareness. At general level, actors may be aware of the money laundering risks facing their sector, but they are unable to identify risks associated with their own activities.

2.8 Virtual currency providers

2.8.1 Operating environment

The virtual currency providers referred to in the Act on Virtual Currency Providers (572/2019) fall within the scope of the Anti-Money Laundering Act. Oversight of the virtual currency providers is the responsibility of the Financial Supervisory Authority. Virtual currency is defined in the fifth anti-money laundering directive, according to which it can be characterised as follows:

- it means a digital representation of value that is not issued or guaranteed by a central bank or a public authority
- it is not necessarily attached to a legally established currency
- it does not possess a legal status of currency or money
- it is accepted by natural or legal persons as a means of exchange and
- it can be transferred, stored and traded electronically.

Providing virtual currency means the issuing of virtual currency, and the provision of exchange services, marketplace or custodian wallet services.[161] In Finland, virtual currency providers are entered in a register maintained by the Financial Supervisory Authority, and by September 2020, six providers of virtual currency had been entered in the registry. In connection with the registration process, the Financial Supervisory Authority checks that the virtual currency provider has taken adequate measures to combat money laundering and terrorist financing. New virtual currency providers can only launch operations in Finland after their registration application has been approved.[162] The reporting obligation of virtual currency providers laid down in the Anti-Money Laundering Act entered into force in December 2019.

The Finnish virtual currency sector comprises operators of different sizes and in 2019, they had a combined turnover of about EUR 27 million.[163] It should be noted, however, that one operator accounts for a major proportion of this total. Virtual currency operators established in Finland mainly provide exchange services based on the purchases and sales of virtual currencies. These services also include exchange platforms. They have a highly international clientele.[164]

Virtual currency providers submitted a total of 75 money laundering reports in December 2019. By the end of June 2020, virtual currency providers had submitted a total of 1,735

161 Financial Supervisory Authority: Virtual currency providers, referred to on 11 November 2020.

162 Financial Supervisory Authority: Press release 1 November 2019, referred to on 11 November 2020.

163 The turnover figures were provided by Suomen Asiakastieto Oy. For one operator, no turnover figures were available.

164 Interviews with experts.

money laundering reports, or an average of 289 reports each month.[165] It should be noted that in addition to virtual currency providers, such bodies as credit institutions may also submit money laundering reports connected with virtual currencies.

2.8.2 Money laundering risks

The overall risk facing the virtual currency sector is at level four (**very significant**). In its risk assessment published in 2020, the Financial Supervisory Authority also classified virtual currency services and e-money as significant risk products and services.[166] A total of 19 experts from the public and private sector took part in the overall national risk assessment.

The use of virtual currencies by **organised criminal groups** in money laundering is seen as a very significant risk and threat. The risk level is increased by the potential **anonymity or pseudo-anonymous character** of virtual currencies, which makes it more difficult to trace funds and determine their sources. The risk scenarios also include a situation in which **criminals develop a block chain project or a new virtual currency for fraudulent purposes** that can also be used in money laundering. As there are thousands of international operators in the sector, identifying fraudulent block chain projects is difficult.

Inadequate establishment of the source of funds is considered a very significant risk. The view is that virtual currency providers are less well-placed to determine the origins of the customers' funds than traditional financial sector operators. Anti-money laundering regulation started to apply to these actors in December 2019, which has an impact on the development of the operating models.

Geographical risks are also seen as very significant risks to virtual currency providers. **Global customers, the mainstream character of remote identification solutions and challenges arising from their usability in different countries, lack of interna- tional standards and differences in operating practices** significantly increase the operators' money laundering risk.

Virtual currency funds can be placed in a large number of different exchange services. There is a large number of international exchange services available, and the sources of the funds can thus be effectively obliterated by using a variety of different exchange

165 Financial Intelligence Unit 2020a, p. 9.

166 Financial Supervisory Authority 2020a, p. 4.

services. **Mixer services** have also been seen as a risk as they are used to break the traceability of virtual currencies.

The **real-time nature of the transactions** is also seen as a significant risk as it means that the currency disappears quickly beyond the reach of the authorities. Moreover, the **transactions are irreversible**, which means that the request for returning funds cannot be applied to virtual currency transactions. Virtual currency providers deal with a **large number of transactions**, which increases the money laundering risk. The obligations laid down in the Anti-Money Laundering Act have only applied to the sector for a short time and thus there is still room for improvement in the monitoring of the transactions.

Virtual currency services are the result of technological development, which also has an impact on the **rapid pace of change in the sector**. The rapid pace of change also requires resources, which means that the resulting **lack of resources in anti-money laundering work** in the private and public sectors impacts the money laundering risk of the virtual currency service sector.

Virtual currency dispensers are vulnerable to misuse. Using virtual currency dispensers, criminals can withdraw the proceeds of crime in cash or the proceeds received in cash can be converted into virtual currency.

Sharing of information between the operators is seen as a significant risk if there is no sharing of information between operators. Lack of access to information may lead to significant gaps because by sharing information operators are also well-placed to identify and combat the money laundering risks facing the sector.

2.9 Expert services

Expert services comprise sectors and organisations outside the financial sector designated in anti-money laundering and counter-terrorist financing regulation ('designated non-financial businesses and professions', DNFBP[167]). Expert services are divided into six sub-groups in the risk assessment. The nature and typical features of the activities have been considered in the division so that the risk assessment can be more effectively focused.

167 For more details of the definition, see FATF 2012-2020, p. 120.

2.9.1 Real estate brokerage agencies and letting agencies

2.9.1.1 Operating environment

Under the Anti-Money Laundering Act, the following actors in the sector are subject to oversight:

- Real estate brokerage agencies and letting agencies referred to in the Act on Real Estate Brokerage and Letting Agencies (1075/2000)
- Real estate brokerage agencies and letting agencies referred to in the provincial legislation of Åland.

Real estate brokerage agencies and letting agencies are supervised by the Regional State Administrative Agency for Southern Finland, which also maintains a register of real estate brokerage agencies and letting agencies. On 1 September 2020, the register contained the details of 1,590 active real estate brokerage agencies and 102 letting agencies. The real estate brokerage agencies and letting agencies operating in Åland are supervised by the Provincial Government of Åland.

In 2019, turnover of the real estate brokerage sector totalled about EUR 610 million.[168] According to the information provided by the Central Federation of Finnish Real Estate Agencies (KVKL), about 62,000 old dwellings and about 10,500 new dwellings were sold in 2019.[169]

The 2015 national risk assessment highlighted the absence of external supervision of the segregated accounts of the real estate brokerage agencies and the difficulty in establishing the sources of funds of foreigners purchasing real estate in Finland. It was also seen as problematic that the identity of the real estate brokerage agent submitting a money laundering report may be disclosed to the suspect. In the view of the experts, investments in real estate are an important and increasingly popular means of money laundering.[170] This was also stated in the 2019 supranational risk assessment.[171]

168 Statistics Finland: Structural business and financial statement statistics, class 68310 'Real estate agencies' referred to on 12 November 2020. See also Federation of Real Estate Agency: Kiinteistönvälitysalan liikevaihto nousi 7,7 % vuonna 2019 – toimiala kasvanut yhtäjaksoisesti viimeiset viisi vuotta [*Federation of Real Estate Agency's revenue increased 7.7% in 2019 – sector grown continuously over the past five years*], referred to on 12 November 2020.

169 Federation of Real Estate Agency: Vanhojen asuntojen kauppa loikkasi vuonna 2019 – joulun alla vauhti vain kiihtyi [*Sharp rise in sales of old apartments in 2019 – rate increased leading up to Christmas*], referred to on 12 November 2020. The statistics compiled by the Central Federation of Finnish Real Estate Agencies cover about 80% of the sales of old dwellings and less than 50% of the sales of new dwellings.

170 National risk assessment of money laundering and terrorist financing 2015, p. 105.

171 EU SNRA 2019 – Commission Staff Working Document, p. 170.

In 2019, real estate brokerage agencies submitted ten money laundering reports to the Financial Intelligence Unit.[172]

2.9.1.2 Money laundering risks

The overall risk facing real estate brokerage agencies is at level two (**moderately significant**) and the risk facing letting agencies at level one (**less significant**). A total of 28 experts from the public and private sector took part in the assessment. In overall terms, the risk facing real estate brokerage agencies is higher than the risk facing letting agencies, but the letting agencies are less familiar with the anti-money laundering process. In Åland, the risk is mitigated by the right of domicile, which gives a person the right to own real property in Åland. Persons without the right of domicile must apply for a permit for real estate transactions from the Provincial Government.

One of the key risks facing the sector is **excessive trust in the customer due diligence, customer monitoring, verification of the source of funds and identification of the customer or beneficial owners by the credit institution**. Actors in the sector often assume that the credit institution has already adequately checked the origin of the customer's funds and do not question the checks or carry out any verification themselves.

Reluctance to submit money laundering reports or investigate potentially suspicious transactions as the actors are anxious not to lose customers is also seen as a risk facing the sector. The fees received by the agents are often based on sales, which means that in their determination to complete contracts, the agents often ignore the suspicions concerning the customers.

Influence of Russian customers on the sector is also seen as a risk. Even though there has been a decline in real estate purchases by Russians, they can still be considered a risk. Even though the use of cash in the sector is now less widespread, it is still a common practice among Russians. Furthermore, establishing the source of Russian funds may be difficult due to the use of tax haven companies and complex corporate arrangements.[173]

The use of segregated accounts is seen as a moderately significant risk facing the sector. Segregated accounts are still used in the sector, for example for the down payment paid to the customer purchasing a dwelling. The risk is that the proceeds of crime are circulated through the accounts in order to obliterate their origins. The actors may also assume that the bank has already checked the source of the funds paid to the account.

172 Financial Intelligence Unit 2020a, p. 9.

173 Financial Intelligence Unit 2018b, p. 23.

Agents in the sector may also be exploited so that the assignment would look credible. The sales or purchasing assignment may be based on an arrangement simply aimed at circulating the funds through a real estate brokerage agency considered a reliable partner.

The **use of intermediaries** in real estate brokerage and letting activities is also seen as a risk. The intermediary (an individual or a company) may attempt to purchase or rent a property, which is ultimately intended for the use of a criminal actor. The funds used in the transaction may have been obtained by criminal means.

2.9.2 Attorneys-at-law and other providers of legal services and tax advisory services or parties providing tax-related support directly or indirectly

2.9.2.1 Operating environment

The Anti-Money Laundering Act is applied to the following actors in the sector:

- attorneys-at-law[174] referred to in the Advocates Act (496/1958) and their assistants and other parties providing legal services as part of their business opera- tions or on a professional basis to the extent that they act on behalf of or in the name of the customer in transactions related to economic activities or real estate or when they take part on behalf of the customer in the planning or execution of the following transactions:
  - purchases or sales of real estate or business units
  - management of customer's funds, securities or other assets
  - opening or management of bank, savings or book-entry accounts
  - establishment or management of companies, or arrangement of funds needed to administer companies, or
  - establishment or management of foundations, companies or similar organisations or management of their operations.

- providing tax advisory services or tax-related support as their main business or professional activity, directly or indirectly.

174 Only persons approved by the Finnish Bar Association and entered in its membership register may act as attorneys-at-law.

The Finnish Bar Association supervises compliance with the provisions of the Anti-Money Laundering Act among attorneys-at-law to the extent that the services provided by attorneys-at-law fall within the scope of the Anti-Money Laundering Act. At the end of 2019, the Finnish Bar Association had 2,177 attorneys-at-law and 770 law offices as its members. Just over one third of all attorneys-at-law worked in law offices with one or two lawyers.[175] In 2019, the turnover of the sector totalled nearly EUR 700 million.[176]

Providers of legal services other than attorneys-at-law and tax advisory services and parties providing tax-related support are supervised by the Regional State Administrative Agency for Southern Finland. By November 2020, a total of 430 providers of tax advisory services[177] and 78 providers of legal services had submitted their details to the money laundering supervision register.

Segregated accounts were highlighted as a significant money laundering risk in the 2015 national risk assessment. The absence of explicit legal provisions on the bookkeeping of segregated accounts was seen as a problem.[178]

Attorneys-at-law and other providers of legal services submitted a total of 13 money laundering reports in 2019.[179]

2.9.2.2 Money laundering risks

The overall risk facing attorneys-at-law and other providers of legal services was put at level two (**moderately significant**). A total of 36 experts from the public and private sector took part in the assessment. One reason why providers of legal services face a slightly higher money laundering risk than attorneys-at-law is because attorneys-at-law must be members of the Finnish Bar Association and the association's board assesses the meeting of the membership criteria when reviewing the membership applications. At the same time, providers of tax advisory services face a higher risk than providers of legal services.

Foreign customers, especially **parties operating in non-EEA countries**, are seen as a significant risk in the sector. Customers engaged in business activities in high-risk countries or in activities associated with high-risk countries or that have partners associated with high-risk countries are particularly risky. Remote identification may

175 Finnish Bar Association 2019, p. 2.

176 Statistics Finland: Structural business and financial statement statistics, class 69101 'Legal representation activities' referred to on 12 November 2020.

177 Most of the actors provide tax advice as an ancillary activity.

178 National risk assessment of money laundering and terrorist financing 2015, p. 107.

179 Financial Intelligence Unit 2020a, p. 9.

involve challenges, especially in connection with large foreign companies or long ownership chains when remote identification is used to determine the beneficial owners of such actors. **Complex business structures and the associated difficulty of identifying beneficial owners** are also widely seen as a significant risk in the sector. This is because determining the structures of a company and obtaining the details of beneficial owners may be time-consuming and require substantial efforts.

Vagueness of the legislation is seen as a moderately significant risk. In this sector, it mainly concerns certain transactions listed in connection with attorneys-at-law and other providers of legal services in the scope of application of the Anti-Money Laundering Act. For this reason, it may be difficult for actors to determine whether the act can be applied to a specific assignment. This particular section of the Anti-Money Laundering Act is given a wide interpretation, which is also seen as a challenge facing the sector. As a result, transactions that are not intended to be covered by the act can also be included in its scope of application. Resources may also be erroneously channelled to transactions falling outside the scope of the act. In such situations, actors may also take measures that are in violation of the General Data Protection Regulation of the EU because there may not be any legal grounds for collecting customer data. Situations in which the nature of the assignment changes during the customer relationship or in which activities not included in the original assignment take place.

Occasional transactions and one-off customer relationships constitute a moderately significant risk when they cannot be justified in terms of business operations. The challenge in one-off customer relationships is to define such actor or activities because customer or customer relationship is not defined in the Anti-Money Laundering Act. A risk may also arise if the actor and the customer are located geographically far apart, and this situation cannot be justified.

Situations in which the **payment for the assignment comes from a third party or is based on a complex financing arrangement** are also seen as moderately significant risks. Even though the payment may come from the customer, the funds may actually originate from several different sources.

There is excessive trust in the sector in the customer due diligence, customer relationship monitoring, verification of the source of funds and identification of beneficial owners by the credit institution. This is a moderately significant risk, and it mainly concerns small actors and situations in which the actor's own compliance functions are inadequate or non-existent. In such cases, the actor may rely on the bank's expertise in customer due diligence and verification of the origin of its funds and neglects its own customer due diligence obligations.

There may be reluctance to submit money laundering reports or investigate potentially suspicious transactions as the actors are anxious not to lose customers. This is seen as a moderately significant risk in small law offices without centralised procedures for money laundering reports. Another reason why the risk is smaller in large offices is because they are anxious to avoid any reputational risks even if it means the end of a customer relationship or the failure to establish one. The reluctance to submit money laundering reports may also be prompted by the fear that the suspect will learn about it.

Segregated accounts have traditionally been seen as a high risk in the sector and they are still identified as a potential money laundering channel and a moderately significant risk. However, the view is that the risk has substantially decreased over the past few years as actors now make less use of segregated accounts an any fund transfers made to such accounts are usually known in advance and thus expected.

Bogus transactions, which may involve mediated agreements concerning bogus disputes, are also a potential risk associated with segregated accounts. In such situations, bogus disputes are used as a basis for circulating funds through segregated accounts. In such cases, law offices are used to lend credibility to shady arrangements.

The risks facing the providers of tax advisory services are often similar to those associated with attorneys-at-law and providers of legal services. With regard to tax advisory services, **customers operating in specific high-risk sectors**, such as the construction industry or sectors in which cash is used, are also considered risky. However, the risk depends on whether the customer is a small company owned by a small number of individuals or a large actor whose beneficial owners are difficult to establish. The risk is also associated with **foreign customers or customers that have undergone complex corporate arrangements without acceptable commercial reasons.**

2.9.3 Bookkeepers and auditors

2.9.3.1 Operating environment

Under the Anti-Money Laundering Act, the following actors operating in the sector are subject to supervision:

- auditors referred to in the Auditing Act (1141/2015) when they are carrying out statutory audits referred to in chapter 1, section 1(1) of the act
- parties carrying out accounting assignments as part of their business operations or on a professional basis.

Accounting offices provide accounting and financial statement services, which include bookkeeping and payroll services. The statutory audit conducted by auditors and audit firms comprises the accounts of the financial year, financial statements and the management audit. At the conclusion of this process, the auditor issues the audit report. Auditors and audit firms may also provide other services that fall within the scope of the Anti-Money Laundering Act, such as tax advice. Under the Anti-Money Laundering Act, bookkeepers are supervised by the Regional State Administrative Agency for Southern Finland, while auditors are supervised by the Finnish Patent and Registration Office. Auditing is an activity subject to authorisation and the Finnish Patent and Registration Office is also responsible for ensuring that auditors comply with obligations other than those concerning anti-money laundering.

There was a total of 4,106 accounting firms in Finland in 2019 with a combined turnover of about EUR 1.1 billion.[180] A total of 1,293 bookkeepers had submitted their details to the money laundering supervision register by November 2020. There was a total of 1,317 auditors and 73 audit firms in Finland at the end of 2019.[181] Auditors conducted more than 124,000 statutory audits in 2019.

Bookkeepers submitted 21 and auditors 13 money laundering reports in 2019.[182]

2.9.3.2 Money laundering risks

The overall risk facing bookkeepers and auditors is at level two (**moderately significant**). A total of 30 experts from the public and private sector took part in the assessment. Bookkeepers face a higher money laundering risk than auditors but at the same time, bookkeepers are better placed to detect money laundering than auditors.

It is difficult for bookkeepers and auditors to detect suspicious transactions among the large amount of data they process, and this is also seen as the most significant risk in the sector. As the amount of data involved is large, only the most blatant cases of misuse are detected. In fact, suspicious transactions are usually only detected at a later stage, for example in connection with tax audits. The use of **bogus receipts** and adding them to bookkeeping documents is also seen as a significant risk because they make it more difficult to detect suspicious transactions. Criminal actors may try to exploit newly started bookkeepers who have not yet built any long-standing customer relationships based on

180 Statistics Finland: Structural business and financial statement statistics, class 69201 'Bookkeeping and closing-of-accounts activities' referred to on 12 November 2020.

181 Finnish Patent and Registration Office: Registration of auditors, referred to on 7 January 2021

182 Financial Intelligence Unit 2020a, p. 9.

mutual trust. Carrying out **bogus transactions** to mislead bookkeepers and auditors is relatively easy and such transactions are also difficult to detect.

Actors associated with **complex business structures that are not commercially justified** are seen as moderately risky customers from the perspective of bookkeepers and auditors. They often involve activities in which the organisation providers services in a wide variety of different sectors. Complex business structures make it more difficult to identify beneficial owners.

Reluctance to submit money laundering reports or investigate potentially suspicious transactions as the actors are anxious not to lose customers is also seen as a moderately significant risk facing bookkeepers. A bookkeeper may in practice detect suspicious transactions but may aim to ostensibly remain unaware of them. Auditors are more likely to take action when detecting suspicious customer transactions but do not necessarily submit any statutory money laundering reports on them.

There is **excessive trust in the sector in the customer due diligence, customer monitoring, verification of the source of funds and identification of beneficial owners by banks**. The bookkeeper or auditor may assume that the bank has already established the source of the funds received by customer companies and therefore does not adequately question the bank's judgement. In fact, transactions are more closely monitored from the customer company onwards.

2.9.4 Providers of business services

2.9.4.1 Operating environment

Under the Anti-Money Laundering Act, providers of business services are organisations or business operators that provide any of the following services to third parties on a commercial basis:

- establishment of a business entity
- acting as a person with liability under company law, as a partner or in a similar position in another legal person
- providing a registered office, business or postal address or other similar services
- acting as a trustee of a foreign express trust or a similar legal arrangement referred to in Article 3(7)(d) of the anti-money laundering directive in Finland
- acting as an authorised nominee when the authorised nominee has been entered in the register of shareholders of a non-listed company.

Provision of business services in Finland often involves the establishment of companies or provision of addresses for administrative purposes. Under the existing Anti-Money Laundering Act, business services do not include selling of shelf companies.[183]

Trusts or their structures do not exist under the Finnish legal system and for this reason, references to asset management services in the Anti-Money Laundering Act explicitly concern foreign trusts and acting as their trustees. In accordance with the fourth anti-money laundering directive, this also applies to acting as a trustee of a similar legal arrangement.[184]

Providers of business services are obliged entities supervised by the Regional State Administrative Agency for Southern Finland. The business service register maintained by the Regional State Administrative Agency for Southern Finland under the old antimoney laundering act has been replaced with the money laundering supervision register. A total of 284 providers of business services had submitted their details to the register by November 2020.

Business service providers did not submit any money laundering reports in 2019.

2.9.4.2 Money laundering risks

The overall risk facing business service providers is at level two (**moderately significant**). A total of 18 experts from the public and private sector took part in the assessment.

Occasional transactions that do not involve long-standing customer relationships are seen as a risk in the sector. Situations involving **customer assignments that are also unusual in other respects** can also been considered risky. In such situations, the customer and the actor carrying out the assignment may be located geographically far apart. The assignment may also differ significantly from typical lines of business of the customer's sector.

The use of tax havens and tax haven companies makes it substantially more difficult to identify the real actors behind the customer company and establish the source of funds. Such companies often involve complex business arrangements. Customers' **links with risk zones and cultural differences** between the countries of the customer company and the service provider are also seen as risks. In particular, the differences between these countries in legal compliance and AML legislation increase the risk.

183 Regional State Administrative Agency for Southern Finland: Valuutanvaihto ja yrityspalvelut [*Currency exchange and business services*.], referred to on 5 November 2020.

184 Government Proposal No. 228/2016, p. 91.

Reluctance to submit money laundering reports or investigate transactions as the actors are anxious not to lose customers is also seen as a risk in the sector. The fact that in 2019, providers of business services did not submit a single money laundering report lends support to this. At the same time, it has also been recognised that actors in the sector are not necessarily aware that they are obliged entities. Actors in the sector may offer business services as an ancillary activity and are unaware that the Anti-Money Laundering Act also applies to this line of business.

2.9.5 Pawnbrokers

2.9.5.1 Operating environment

Pawnbrokers referred to in the Pawnshops Act (1353/1992) fall within the scope of the Anti-Money Laundering Act and they are supervised by the Regional State Administrative Agency for Southern Finland. Pawnbrokers grant cash credit to natural persons against items that are pawned. Pawnbrokers may not accept deposits or other funds repayable on demand.

Pawnshops are supervised by the Regional State Administrative Agency for Southern Finland, which also grants licences for pawnbroker activities. When applying for a licence, a pawnbroker must provide the required details of the owners of the pawnbroker business, their shares, company management and the persons responsible for the management. There are 11 licenced pawnbrokers in Finland.[185] Turnover of Finnish pawnbrokers totalled about EUR 18.7 million in 2019 and one actor accounted for a significant proportion of this sum.[186]

Pawnbrokers submitted one money laundering report in 2019.

2.9.5.2 Money laundering risks

The overall risk facing pawnbrokers is at level two (**moderately significant**). A total of 17 experts from the public and private sector took part in the assessment.

One-off customer relationships are seen as a risk in the sector, which is characterised by long-standing customer relationships. Establishing the origin of the items that are pawned by one-time customers may be particularly difficult. Stolen goods can be offered as pawns if the origin of the items is not adequately verified. Challenges of determining the origin

185 Regional State Administrative Agency for Southern Finland: Panttilainauslupaluettelo 13.11.2020 [*List of licensed pawnbrokers*], referred to on 17 November 2020.

186 The turnover figures were provided by Suomen Asiakastieto Oy.

of the funds also have an impact on the risk arising from **the use of cash**. The risk may materialise when a pawned item is redeemed and at this stage, the pawnbroker should check that the item is not redeemed using proceeds of crime.

Gold objects are the highest-risk category of pawned items. For example, gold jewellery is valuable in money terms and establishing the origin and actual owners of such items is difficult because they are not registered.

The sentence given by the Helsinki District Court on 21 March 2018[187] is an example of money laundering carried out in conjunction with pawnbroker business.

Case involving the pawning of guitars

Persons A and B had received and kept in their possession electric guitars. At the request of an unknown person, Persons A and B had taken the guitars to a pawnshop with the intention of pawning them, each on different days. Persons A and B had handed nearly all of the cash received from the pawnshop to the un- known person. Persons A and B had told in the criminal investigation that they had slight doubts about the origin of the electric guitars. According to the court, both persons were guilty of money laundering. The sentence is legally valid.

2.9.6 Art dealers

2.9.6.1 Operating environment

Parties selling or brokering art as part of their business operations or on a professional basis fall within the scope of the Anti-Money Laundering Act when at least EUR 10,000 is paid or received in a single transaction or as linked transactions.

Art galleries, auction houses and other parties selling and brokering art as part of their business operations or on a professional basis fall within the scope of the Anti-Money

187 Sentence of the Court of Appeal of Helsinki, 23 March 2018 No. 18/112809.

Laundering Act. The works of art falling withing the scope of the act have not been specified as they are considered to include both items and immaterial art.[188]

There were a total of 259 art and antiques shops and auction houses in Finland in 2019 with a combined turnover of about EUR 35 million.[189] The art dealers referred to in the Anti-Money Laundering Act are supervised by the Regional State Administrative Agency for Southern Finland. Art dealers must submit their details to the money laundering supervision register maintained by the Regional State Administrative Agency. A total of 44 art dealers had submitted their details to the register by November 2020.

2.9.6.2 Money laundering risks

The overall risk facing art dealers is at level two (**moderately significant**). A total of 17 experts from the public and private sector took part in the assessment.

Art purchases by Russian customers are seen as the main risk facing the sector. This manifests itself in trade practices in which cash payments are combined with bank giro payments and large sums are spent on art purchases. There may also be efforts to offer Russian art forgeries for sale in Finland and they may also be distributed more widely using Finland as a country of transit.

Art forgeries in general are also one of the main risks facing the sector. Customers are not necessarily able to identify art forgeries, which means that art dealers have a particular responsibility in this respect. The money laundering risk arising from forgeries also depends on the type of the item (is the product unique or a valuable object that is more difficult to specify).

Determining the value of the works created by new artists is seen as difficult and the risk is that **criminals may try to influence the process**. Criminal actors are not considered to play a major role in the process of determining the value of well-known works of art as such pieces usually have a well-established market value. Neither is overpricing a problem at auctions as the attempts by criminals to influence the value of the works are more likely to occur when art galleries sell items.

188 Government Proposal No. 167/2018, p. 92.

189 Statistics Finland: Structural business and financial statement statistics, classes 47781 'Retail sale of art; art gallery activities', 47791 'Antiques shops' ja 47793 'Auction houses', referred to on 12 November 2020.

2.9.7 Goods retailers

2.9.7.1 Operating environment

Parties selling or brokering goods as part of their business operations or on a professional basis fall withing the scope of the Anti-Money Laundering Act when at least EUR 10,000 is paid or received in a single cash transaction or as linked cash transactions.

Parties selling goods as part of their business operations or on a professional basis referred to in the Anti-Money Laundering Act are supervised by the Regional State Administrative Agency for Southern Finland. Such actors must submit their details to the money laundering supervision register and by November 2020, 13 sellers of goods had been entered in the register.

Even though the number of the goods retailers entered in the money laundering supervision register is small, the total number of the actors in the sector and the turnover generated by them is considered substantial. For example, large sums may be paid in the purchases of motor vehicles, watches and jewellery. There were about 2,000 motor vehicle dealers in Finland in 2019, with a combined turnover of about EUR 12 billion.[190] The same year, there were 331 watch and jewellery retailers, with a combined turnover of about EUR 229 million.[191]

Actors that had received more than EUR 10,000 in cash submitted 38 money laundering reports in 2019.[192]

2.9.7.2 Money laundering risks

The overall risk facing goods retailers is at level two (**moderately significant**). A total of 18 experts from the public and private sector took part in the assessment.

The **lack of knowledge of the cash-based reporting obligation among the actors** is seen as the most significant risk in the retail sales of goods. In other words, the actors do not necessary realise that they are obliged entities. This is underlined by the fact the even though Finland has a large number of goods retailers, only 13 of them have submitted their details to the money laundering supervision register. However, the cash limit of

190 Statistics Finland: Structural business and financial statement statistics, class 451 'Sale of motor vehicles', referred to on 12 November 2020.

191 Statistics Finland: Structural business and financial statement statistics, class 4777 'Retail sale of watches and jewellery in specialised stores' referred to on 12 November 2020

192 Financial Intelligence Unit 2020a, p. 9.

EUR 10,000 means that most of the actors are outside the scope of the Anti- Money Laundering Act and thus also outside the supervision register.

Sales of expensive cars, boats and machinery involve particularly high risks in the sector. However, the use of cash in the purchases of such items has become less common, which significantly mitigates the risk.

3 Terrorist financing

3.1 Key observations

No final court decisions on terrorist financing have been given in Finland and only one criminal investigation has been launched since 2015. The small number of cases and the absence of sentences make risk assessment particularly difficult in all sectors as there are no concrete cases to examine. Identifying the phenomenon and defining the risk scenarios are seen as a challenge in both private and public sectors. Moreover, in the private sector there is also less awareness and understanding of terrorist financing than of money laundering. In many risk assessments, money laundering and terrorist financing are placed in the same category, which means that they do not take into account the differences between the two phenomena. The absence of clear guidelines of such matters as assessment criteria and the extent of the assessment mean that actors in the sector may not possess adequate methods to combat terrorist financing.

According to the essential elements listed in the Criminal Code, providers of financing must be aware that their funds are used to finance specific types of terrorist acts, and experience has shown that proving such intent is difficult. This is one reason why there have been so few criminal investigations of terrorist financing. Most of the terrorist acts have taken place in crisis zones and carrying out criminal investigations in these parts of the world is all but impossible. However, a working group appointed by the Ministry of Justice concluded in its report that the difficulty of obtaining evidence of an offence and assessing it are not in themselves a justification for making another similar offence punishable on the grounds that in such cases the criminal intent is easier to prove.[193]

The funds used to finance terrorism may have been acquired from lawful sources. Individuals may use their earnings or savings for the purpose.[194] For this reason, the sums channelled to terrorist financing may be small,[195] which in turn makes it more difficult to detect suspicious transactions. The source of funds is also one feature distinguishing terrorist financing from money laundering because in money laundering, the laundered funds have been obtained by means of predicate offences. Investigating cases related

193 Ministry of Justice 2020b, p. 56.

194 Ministry of the Interior 2019, p. 91.

195 Interviews with experts.

to terrorist financing is also difficult because they involve cross-border activities, which complicates the process of obtaining information.

Challenges involving the identification of fund end users are a risk in many sectors, especially in terms of vulnerability. Actors may identify persons on sanctions lists[196] or, on the basis of indicators, identify other highly suspicious individuals and refuse to start customer relationships with them. In the absence of such indicators, actors are poorly placed to establish the actual recipient of the funds, if the customers do not otherwise arouse any suspicions. Furthermore, the view in many sectors is that remote identification involves uncertainties. From the perspective of risk mitigation, actors would benefit from recommendations on strong electronic identification listing the identification services that should be used.

The risk levels of the sectors examined in the national risk assessment are given below (on a scale of 1 to 4).[197] Formation of the risk levels is described in more detail in the appendix on the methodology used in the risk assessment. The most significant risks of each sector are examined.

196 Of the international sanctions in effect, see Ministry for Foreign Affairs: Sanctions, referred to on 2 March 2021.

197 The scale is applied as follows: 1=less significant risk, 2=moderately significant risk, 3=signifi- cant risk and 4=very significant risk.

Table 8. Risk levels of the sectors examined in the national risk assessment.

Sector	Risk level
Hawalas	4
Providers of virtual currency services	3
Credit institutions	3
Payment service providers	3
Other providers of financial services	2
Financial institutions	2
Currency exchange	2
Providers of tax advisory services or parties providing tax-related support directly or indirectly	2
Bookkeepers	2
Art dealers	2
Cash-based reporting obligation (sales of goods)	2
Gambling operators	2
Other providers of legal services	2
Attorneys-at-law	2
Auditors	2
Insurance companies	2
Real estate brokerage agencies	2
Debt collectors	2
Providers of business services	1
Pawnbrokers	1
Apartment rental services	1

3.2 General factors impacting terrorist financing risk

3.2.1 Terrorist financing in the Finnish context

Terrorist financing in the Finnish context can be examined from a variety of different perspectives. Money to finance terrorism collected in Finland may be sent to other countries (such as to individuals in conflict zones). The Financial Intelligence Unit has prepared a report on the typical features of terrorist financing,[198] and the cases examined in the document involve a large number of international connections. The report examined international links involving the use of the funds and means of transferring, collecting and recycling funds in cases with international connections. According to the report, actors in a total of 92 countries on all continents were involved in the use of funds. The most important country in this respect was Turkey, followed by Sweden, Germany and Russia. The most common means of transferring funds in cases involving international connections were account transfers, cash and money remittance services.[199]

In its report, the Financial Intelligence Unit identified three major ways to collect and recycle funds: non-profit associations, fundraising and gambling. According to the report, nearly 90 per cent of the cases involving non-profit associations and fundraising also involved cross-border use of the funds.[200]

Hawalas are probably also used to channel funds to terrorist activities. Hawalas play a particularly important role as a means of transferring funds to regions without workable banking systems or where people have no trust in traditional banks. In recent years, there have been indications that funds are also transferred by means of virtual currencies.[201]

Financing terrorism in Finland using funds collected in other countries may involve persons returning to Finland from conflict zones. According to the threat assessment prepared by the Finnish Security and Intelligence Service, individuals returning from conflict zones constitute both direct and indirect security threats.[202] Terrorist activities in Finland are mostly in the form of support activities involving funding and recruitment.[203]

198 The report examined cases under investigation that involved terrorist financing connections between January 2017 and June 2019.

199 Financial Intelligence Unit 2020b. The following 12 different means of transferring funds are listed in the report: hawala, card payment, consumer credit, courier, cash, loan, money remittance service, cheque, account transfer, insurance, currency order and virtual currency.

200 Financial Intelligence Unit 2020b.

201 Opinion of the Finnish Security and Intelligence Service for the national risk assessment of money laundering and terrorist financing, 15 January 2021.

202 Finnish Security and Intelligence Service: Terrorism threat assessment, referred to on 17 December 2020.

203 Ministry of the Interior 2019, p. 11.

Individuals returning from conflict zones may facilitate and accelerate terrorist support activities in Finland because such persons help Finnish-based actors to expand links with jihadist groups in conflict zones.[204] Financing (fundraising and channelling funds to support terrorist activities) may be intended to facilitate attack plans, and support com- batants and groupings. The money may also be used to pay salaries and to finance equipment purchases. Fundraising may also be disguised as charity, in which cases individuals may not be aware of the actual destination and purpose of their donations. People may also be pressured or coerced to give money.[205]

The increasing threat of extreme right-wing terrorism should also be highlighted in the Finnish context. According to the Finnish Security and Intelligence Service, there are also persons in Finland that support far-right terrorist activities or sympathise with them. Individuals and small groups supporting radical Islamist or extreme right-wing ideology constitute the most serious threat of terrorism in Finland. The cross-border nature of the extreme right-wing activities is reinforced by international far-right groups and the use of social media as a communication platform.[206]

According to international estimates, extreme right-wing groups and individuals communicate and cooperate in the internet and these activities also include financial support across national boundaries.[207] According to Europol, far-right and far-left groups receive funding from their supporters in the form of contributions and donations. Europol adds that collecting contributions from supporters and sympathisers in the form of account transfers or in cash during concerts or other similar events is a highly popular fundraising method among extreme right-wing groups. Far-right actors may also raise funds by marketing and selling different types of promotional items, such as products displaying logos.[208] Raising funds for extreme right-wing terrorism is also a possibility in Finland as far-right terrorism is becoming an increasingly serious threat in our country.

3.2.2 Geographical location

The geographical dimension is a key factor in terrorist financing as international connections are highly important in such activities. Even though the remote location of Finland may partially explain the low level of terrorist activities in our country, social media

204 Ministry of the Interior 2019, p. 12.

205 Opinion of the Finnish Security and Intelligence Service for the national risk assessment of money laundering and terrorist financing, 15 January 2021.

206 Finnish Security and Intelligence Service 2020, p. 3.

207 CTED 2020, p. 5.

208 Europol 2020c, pp. 22-23.

in particular has transformed the way in which Finland is viewed in the jihadist movement. For example, it has become easier to establish personal ties across geographical boundaries.[209]

It was pointed out in the interviews with private-sector representatives that the lists of high-risk countries compiled by FATF and the European Commission are regularly used as a basis for assessing geographical risks. In the view of actors in different sectors, most customers from these countries as well as links between customers and these countries involve risks. Furthermore, actors in specific sectors may refuse to conduct transactions with individuals, companies and other organisations from such countries.

According to the European Commission, strategic deficiencies in the systems to combat money laundering and terrorist financing in high-risk third countries are a major threat to the financing system of the European Union. The following countries are listed as high-risk third countries in a European Commission Delegated Regulation:[210] Afghanistan, Barbados, Botswana, Cambodia, Ghana, Iraq, Jamaica, Mauritius, Mongolia, Myanmar/Burma, Nicaragua, Pakistan, Panama, Syria, Trinidad and Tobago, Uganda, Vanuatu, Yemen and Zimbabwe. With a few exceptions, all these countries are also listed by FATF as Jurisdictions under Increased Monitoring (grey list).[211] Iran and North Korea are the countries on the FATF list of High-Risk Jurisdictions subject to a Call for Action (blacklist).[212] According to the Financial Intelligence Unit, Somalia and Turkey should also be treated as high-risk countries in respect of terrorist financing.[213]

3.2.3 Technological development

Technological development and, in particular, internet-based means of communication are seen as significantly facilitating communication between terrorists, recruitment and fundraising for terrorist activities.[214] The growth of social media has allowed terrorist activities to expand and helped organisations to build networks. The ability to wield

209 Ministry of the Interior 2019, pp. 108 and 111.

210 Commission Delegated Regulation C(2020) 2801 final, adopted 7 May 2020.

211 Afghanistan, Iraq, Mongolia, Trinidad and Tobago and Vanuatu are listed as high-risk countries by the European Commission, but they are not included on the FATF grey list. Albania is also included on the FATF list updated in October 2020.

212 Countries blacklisted by FATF have significant strategic deficiencies in their regimes to counter money laundering and terrorist financing. FATF urges all its members to apply enhanced customer due diligence in respect of the blacklisted countries.

213 Financial Intelligence Unit 2020b.

214 Palonen – Laitinen 2011, p. 81.

influence through social media and the rapid spread of material online partially explain why many young individuals have travelled to the conflict zones of Syria and Iraq.[215]

Social media platforms, such as Twitter, Facebook and YouTube, allow actors to spread propaganda and raise funds. Moreover, in a number of social media services, messages can be encrypted (WhatsApp) or the information can only be viewed for a limited period (Snapchat). However, the view is that social media or other new technological solutions (such as virtual currencies and crowdfunding) will not replace the traditional fundraising methods used by jihadist groups. At the same time, the impact of technological development, new payment methods and virtual currencies should be taken into account in situations in which groups are transferring funds to their core regions.[216]

Extreme right-wing groups are also making effective use of technological advances and social media. They have rapidly embraced the latest information technology, adapted it to their own needs and are using a variety of different platforms (such as websites and discussion forums) to spread their ideology.[217] Facebook, Twitter and YouTube also remain important communication and propaganda channels[218] and in this role, they also help groups to raise funds. Left-wing extremists also favour internet-based platforms when disseminating propaganda. According to Europol, left-wing extremist groups use encrypted applications and means of communication. such as Signal and Telegram.[219]

3.3 Terrorist financing risk associated with the insurance sector

The overall risk of terrorist financing facing the insurance sector is at level two (**moderately significant**). A total of 21 experts from the public and private sector took part in the assessment. For a definition of the operating environment of the sector, see section 2.3.1.

Terrorist financing may be a multi-faceted activity and thus difficult to detect, and for this reason **identifying the phenomena and risks associated with it is seen as a challenge**. This is the most significant risk facing the sector, especially in terms of vulnerability. Actors in the sector are able to identify risk scenarios associated with specific insurance products

215 Pohjonen 2020, p. 53.
216 Tuomaala-Järvinen 2020, p. 103.
217 Europol 2020c, p. 24.
218 Europol 2020c, p. 73.
219 Europol 2020c, p. 62.

but terrorist financing scenarios that may be associated with nonlife insurance operations are more difficult to understand and thus often remain unidentified.

Situations in which **insurance payments are channelled to foreign accounts** and the insurance company is unable to establish the actual account holders are seen as risky.

Taking out life insurance before travelling to conflict zones or high-risk regions has been identified as a risk. In such situations, the beneficiary may be a person acting with terrorist intent to whom any insurance payments are directed. However, the process of granting a life insurance policy contains procedures to control such activities and exploiting life insurance policies would require knowledge and understanding of different types of life insurance products. This is a factor significantly mitigating the risk.

Situations in which associations take out insurance are also seen as a terrorist financing risk. This is mainly connected with associations applying for insurance that collect money and send it to conflict zones.

3.4 Terrorist financing risks associated with payment service providers (incl. currency exchange and hawala systems)

Difficulty of identifying phenomena and risks associated with terrorist financing is seen as a risk concerning the sector as a whole. This is because such activities are multi-faceted and difficult to detect. This can partially be explained by a lack of understanding of terrorist financing among the actors, which means that they are unable to identify any suspicious indicators in their own activities. Understanding of the risk essentially depends on the size of the actor. Situations associated with the lack of knowledge have also been identified as risks with regard to payment service providers in the Black Wallet project. One example is a situation in which the actor's employees fail to identify risk indicators because of inadequate CFT training.[220]

Payment service providers

The overall risk facing payment service providers is at level three (**significant**). A total of 19 experts from the public and private sector took part in the assessment. For a definition of the operating environment of the sector, see section 2.4.1.

220 Black Wallet 2020a, p. 13.

Quick transactions make the freezing of funds impossible, which is seen as a very significant risk in terms of vulnerability. The number of transactions is huge and the fund transfers take place immediately. If the customer is not on a sanctions list and the authorities are unable to interfere with the transaction in this way, the transaction quickly passes through the system after which the funds are beyond the reach of the authorities.

The **willingness of the criminals to exploit the systems of payment service providers** is also a very significant risk. Quick transactions, easy-to-use services and the option of concealing the identity of the actual payee make payment services an attractive fund transfer channel for actors financing terrorism.

Supervisory challenges arising from the international nature of the payment services are seen as a significant risk in terms of vulnerability. New actors are continuously entering the sector and maintaining a unified picture of the activities is difficult. There are also differences between national legislations, which makes it more difficult for the authorities to exchange information. Rapid advances in technology also mean that regulation cannot fully keep pace with the advances and this inevitably leads to gaps in regulation.

Challenges concerning the monitoring of the vast number of transactions and detection of suspicious transactions are seen as risks, especially in terms of vulnerability. As mentioned above, the level of transaction monitoring partly depends on the size and resources of the actor. The actors may be familiar with general CFT methods but have not examined how they could be applied to their own activities and identification of their own risks at practical level.

The terrorist financing risk increases if the **actors are unable to form an overall picture of the customer or the customer's activities**. Many actors obtain the basic customer details required under the law but such matters as continuous customer monitoring or more extensive customer due diligence are inadequately organised. Customers are primarily identified by means of remote identification and in the absence of personal contacts, this may make the identification process insufficient. There are particularly significant challenges regarding the identification of beneficial owners, which substantially impacts the formation of the overall picture of the customer relationships and thus also increases the risk.

Hawalas

The overall terrorist financing risk facing hawalas[221] is at level four (**very significant**). A total of 15 experts from the public and private sector took part in the assessment.

The **willingness of criminals to exploit the system** is also seen as a very significant risk facing hawalas. The fact that hawalas **can be easily used in terrorist financing** is a particular problem in this respect. Transferring money through them is easy and inexpensive and they can also be used to forward payments to conflict zones. The activities are also fairly 'invisible' as cash is widely used.

Challenges arising from the supervision of hawalas are seen as a very significant risk in terms of vulnerabilities. Hawalas operating in Finland base their activities on international systems, which means that effective supervision requires understanding of the functioning of the hawala system and the risks associated with it. **The difficulty of establishing the ultimate destination and use of the money transport** is also a supervision-related challenge. The use of cash in hawalas makes it practically impossible to determine the ultimate destination of the funds. **In general, cash has moved from banking to unofficial money transfer systems**, which increases the risk.

Non-registered hawalas are seen as a very significant risk in both money laundering and terrorist financing, and their exact numbers or extent are not known. Such actors are unlikely to comply with the legislation and regulation on the prevention of terrorist financing, which means that they do not necessarily use any means to identify their customers.

Currency exchange

The overall risk facing the currency exchange sector is at level two (**moderately significant**). A total of 15 experts from the public and private sector took part in the assessment.

Use of cash and the large number of transactions may make it more difficult to detect terrorist financing, which is seen as a significant risk. Customer identification and establishing the source of the cash play a particularly important role in the prevention of terrorist financing in currency exchange.

221 For more details of the definition of hawala, see section 2.4.1 of the risk assessment.

The **use of intermediaries in the exchange of cash** is also seen as a significant risk. This allows the exchange of large sums, and the suspicious nature of the activities is concealed by using a large number of recruits.

3.5 Terrorist financing risks associated with gambling operations

The overall risk associated with gambling operations in Mainland Finland and Åland is at level two (**moderately significant**). A total of 15 experts from the public and private sector took part in the assessment. For a definition of the operating environment of the sector, see section 2.5.1. The terrorist financing risks in Mainland Finland and Åland are similar in nature and for this reason, the risks are not presented separately in the same manner as money laundering risks.

Playing games offered by foreign gambling companies and the fragmented nature of the supervision, a vulnerability associated with this situation, are a significant risk. Supervision is the responsibility of a large number of authorities in a large number of countries, which may create blind spots in the supervision. This also impacts the chances of national gambling operators to understand the gambling operating environment because it is difficult to produce an overview of the amount of money spent on gambling and its sources. In connection with this, **gambling outside the exclusive system** (especially online) is considered a moderately significant risk.

In the gambling sector, terrorist financing is also seen as a multi-faceted activity that is not easy to understand, which makes it **difficult to identify the phenomena and risks** associated with it. Detecting the phenomenon is hampered by the lack of concrete action as no final court decisions on terrorist financing have been given in Finland.

Repatriation of casino winnings is also seen as a moderately significant risk because it may be difficult to establish the account holder and/or user given in connection with the process. In such cases, the player and the account holder may be two different people. However, the winnings are mostly paid in cash. In Åland, this risk also relates to casino games offered on cruise ships.

3.6 Terrorist financing risks associated with credit institutions

The overall risk facing credit institutions is at level three (**significant**). A total of 30 experts from the public and private sector took part in the assessment. For a definition of the operating environment of the sector, see section 2.6.1.

The **challenges concerning the monitoring of the transactions caused by payment service providers** are seen as a very significant risk. This risk is similar to the risk discussed in the money laundering section and it usually manifests itself as a vulnerability. Payment details may be hidden when payment services are used and in such cases, the credit institution is unable to verify the actual payee. **Account transfers to conflict zones or high-risk countries** are also seen as a general risk.

Terrorist financing is an activity that is difficult to detect also from the perspective of credit institutions, **which means that identifying the phenomena and risks associated with it is challenging**. The absence of practical examples and concrete cases adds to the difficulty of identifying the phenomenon. There are also differences in the AML and compliance functions between credit institutions of different sizes. Some of them have been able to invest more in such areas as training. Level of customer due diligence and monitoring may also vary, depending on the number of customers and customer types.

The fact that terrorist acts can be committed at relatively low cost also makes it harder to identify the phenomenon. **The difficulty of detecting suspicious activities in connection with small transactions** is a significant vulnerability-related risk in this connection. The detection of suspicious account transfers is also particularly challenging when there is nothing else in the transaction arousing suspicions (such as high-risk country or suspicious payee or payer). This risk has also been identified as a challenge in other sectors.

Exploiting payment systems is a potential means of financing terrorism, and it has been identified as a significant risk. **The difficulty of identifying fund end users** is a major vulnerability in this connection. It may be extremely difficult to establish the ultimate purpose of the cash funds and the cash may also be moved anonymously outside the system. The purpose for which unsecured credit is taken out is not usually verified. Long payment chains may also make it difficult to detect the end user. **Taking out consumer credit and transferring it to other accounts to finance terrorism** are also seen as a moderately significant risk. If the granting of the consumer credit proceeds quickly and the money is transferred immediately, it is impossible to block the transfer by means of retroactive monitoring. Here, too, it is difficult to prove that such activities are carried out with the specific intent of financing terrorism.

Processes and supervision carried out as part of international activities are fragmented, and as a result, the supervision does not cover the entire transaction chain. Actors that forward funds to crisis zones as part of their business operations are also high-risk parties.

Inadequate customer due diligence is a significant risk in terms of vulnerability. This is a particularly high risk in the case of foreign fighters whose identity is not known to credit institutions. The problem is connected with the challenges arising from the flow of information. At the moment, credit institutions must rely on public sources (such as the list of administrative freezes) when making assessments.

3.7 Terrorist financing risks associated with financial institutions, other providers of financial services and debt collectors

The overall risk facing the sector is at level two (**moderately significant**). A total of 25 experts from the public and private sector took part in the assessment. For a definition of the operating environment of the sector, see section 2.7.1. Debt collectors face a lower terrorist financing risk than financial institutions and other providers of financial services.

Vulnerabilities are the most significant risks associated with the sector. **Difficulty of identifying the phenomena and risks associated with terrorist financing** are seen as the most significant risk. When the risks remain unknown, terrorist financing is not considered a risk affecting one's own operations. The absence of clear indicators is seen as impacting the process of understanding risk scenarios. Terrorist financing is a low-cost activity and transactions carried out to finance it may be small. This makes it harder for actors to link specific transactions to terrorist financing.

The sector comprises actors of different sizes, which impacts the adequacy of the monitoring activities carried out in the sector. Small-size actors do not possess the resources and capacity to detect terrorist financing, which impacts the **organisation and level of monitoring**. Automated monitoring systems are expensive, but at the same time, manual monitoring has limited effectiveness.

The challenges related to identifying fund end users is also seen as a significant risk affecting the sector as a whole. Even if an actor does have all the required customer due diligence procedures in place, it is extremely difficult to establish a connection between the end user and terrorism and to identify the destination of the funds.

Financial institutions and other providers of financial services

Taking out consumer credit and transferring the money to conflict zones or high-risk regions is seen as a significant risk. Consumer credit is an easy way of collecting reasonable sums and it is not possible to monitor the purpose for which the money is used. Intermediaries can be used to take out consumer credit, in which case the true recipient remains unknown. Funds can also be withdrawn by means of identity theft.

Using crowdfunding to finance terrorism is seen as a risk. For example, in **peer-to-peer loans**, the lender may not be able the establish the real identity of the recipient and how the money would be used. The real purpose of crowdfunding campaigns organised in social media may be to collect money for such parties as terrorist organisations. Such collections may also be disguised as charity drives, in which case the donors are unaware of the real destination of the funds.[222]

The powers of national and home state supervisory authorities to oversee **foreign actors offering cross-border services from a foreign country without establishing a branch** are seen as a moderately significant risk from the vulnerability perspective for investment service providers. An actor in an EEA country wishing to provide services in Finland without establishing a branch in Finland must notify the supervisory authorities of its home state and the national supervisory authority must maintain a list of these notifications. Actors providing services in Finland without establishing a branch in Finland do not come under the oversight of the national supervisory authorities. Thus, the national supervisory authorities cannot take any direct action if there are irregularities in the activities of a service provider from another EEA country, as the matter is the responsibility of the supervisory authorities in the service provider's home state.

Situations in which **specific investment schemes offered outside Finland can be considered complicated and thus suspicious** are also seen as risky. The scheme may actually be a fundraising drive disguised as an investment opportunity. They may also involve charity schemes in which some of the proceeds are channelled to high-risk regions instead of being used for the declared purpose. However, such scenarios are relatively complicated, which reduces the likelihood of the risk.

Debt collectors

Bogus transactions carried out to direct funds to other countries have been identified as a significant risk facing debt collectors. For example, a fake invoice is taken to debt collection and the payment is intended for a party acting with terrorist intent. Debt

222 FATF 2015b, p. 31 and Tuomaala-Järvinen 2020, p. 104.

collection measures may be launched automatically, especially if the claims are not contested.

3.8 Terrorist financing risks related to virtual currency providers

The overall risk facing virtual currency providers is at level three (**significant**). The assessment was produced by 20 experts from the public and private sector. For a definition of the operating environment of the sector, see section 2.8.1.

Identifying phenomena and risks related to terrorist financing is also seen as a challenge in the virtual currency sector. The sector is relatively new and its actors do not yet have a clear picture of the risk scenarios associated with terrorist financing. Virtual currency providers are also a relatively new group of obliged entities under the Anti-Money Laundering Act, and for this reason, their own internal processes in this area may not yet be fully in place.

Challenges concerning the monitoring of transactions arising from the large number of transactions and cross-border activities are also seen as a very significant risk in terms of vulnerability. Business activities in the sector have developed in an unregulated environment and the changeover to a regulated regime has been relative rapid. For this reason, the monitoring systems are not yet fully operational. Differences in the level of monitoring may also encourage potential providers of terrorist financing **to use virtual currency providers instead of banking systems**, which might lower the risk of being caught. However, virtual currencies are not widely accepted as means of payment in the purchases of goods and services, which reduces the likelihood of such scenarios.

Customers from outside the EEA are seen as a very significant geographical risk in the sector. Remote identification of such customers is particularly difficult if strong electronic identification cannot be used. Verifying the authenticity of the identification documents supplied by the customers may be problematic. Transfers of funds to non-EEA countries are also seen as risky because it is difficult for the virtual currency providers to give the reasons for the transfer to third parties.

The anonymous or pseudo-anonymous character of virtual currencies is identified as a very significant risk. Even though funds can be traced using blockchain analytics, many of the virtual currencies have been designed to support anonymity. Few publicly accessible virtual currency wallets offer anonymity but private wallets are usually anonymous.

Raising funds in virtual currencies or using virtual currencies is also a risk. In such cases, the fundraiser, which may act with the intent of financing terrorism, is the high-risk actor from the perspective of preventing terrorist financing. The raising of funds may be disguised as a charity drive. However, the view is that jihadist organisations will prefer more traditional methods to virtual currencies in their fundraising in the 2020s.[223]

As virtual currency technologies are advancing, **loopholes and deficiencies in the legislation** are also seen as a significant risk. At the same time, it was highlighted in the interviews with experts that constant changes in legislation prompted by technological advances is making it more difficult for actors to keep up with the requirements.

Virtual currency dispensers located in high-risk countries are also seen as a potential risk. Such dispensers can be used to transfer funds to terrorists as the funds deposited in the virtual currency wallet can be withdrawn in cash from a dispenser.

3.9 Terrorist financing risks associated with expert services

As in the sectors discussed above, identifying terrorist financing phenomena and risks is also considered to be challenging in connection with expert services. Terrorist financing risks are not adequately identified and as a result, potential risk scenarios are not given a high priority.

3.9.1 Terrorist financing risks associated with real estate brokerage agencies and letting agencies

The overall risk facing real estate brokerage agencies is at level two (**moderately significant**) and the risk facing letting agencies at level one (**less significant**). A total of 22 experts from the public and private sector took part in the assessment. For a definition of the operating environment of the sector, see section 2.9.1.1.

The **use of intermediaries** is seen as a moderately significant risk. Even though the risk is recognised, investing in real estate and housing is considered substantially more complicated than other means of terrorist financing. The complexity may make the scenario less attractive to criminals.

223 Tuomaala-Järvinen 2020, pp. 106–107.

Buying and renting property and channelling the rental income to terrorist financing are also seen as a moderately significant risk. A property purchase may serve as an interim investment for parties financing terrorism. By selling the property at a later date, the parties are able to release funds for the activities. At the same time, rental income guarantees a steady flow of funds that can be forwarded to support terrorist activities.

3.9.2 Terrorist financing risks associated with attorneys-at-law, other providers of legal services and tax advisory services

The overall risk facing attorneys-at-law, other providers of legal services and tax advisory services is at level two (**moderately significant**). A total of 32 experts from the public and private sector took part in the assessment. For a definition of the operating environment of the sector, see section 2.9.2.1.

Limited access to information is considered a significant risk in terms of vulnerability. The actors have only limited chances to check the backgrounds of individuals or companies from different countries and the information rarely contains any hints of terrorist connections. Customers' connections with high-risk regions serve as a risk indicator but the other information available to the actors is rarely adequate to confirm that the person in question is acting with the intention of financing terrorism.

Inadequacy and vagueness of the legislation in matters concerning terrorist financing is also seen as a risk from the perspective of vulnerability. One example is the absence of decree-level regulation that would provide more detailed guidelines on preventing terrorist financing. It has also been noted that obliged entities are insufficiently familiar with legislative provisions concerning such matters as sanctions and freezing lists. Limitations imposed by data protection legislation are also seen as a vulnerability as data protection legislation limits access to and exchange of information.

The fact that the prevention of money laundering and terrorist financing is often considered as a single set of measures is seen as a moderately significant risk facing the sector. In such cases, the emphasis is often on establishing the source of funds rather than on checking the purpose of use of the money. When preparing their own risk assessments, sectoral actors do not necessarily pay sufficient attention to differences between money laundering and terrorist financing, as they are of the view that many of the risk scenarios apply to both phenomena. More effective action to prevent terrorist financing would require practical examples from the sector and organisationinternal training.

Assignments involving the **establishment of operating structures or functions** that are associated with a terrorist financing risk are also seen as a moderate risk. These include

the establishment of an association or foundation or the preparation of a last will and testament. For example, the origin of the funds donated to a foundation can be verified but ascertaining the real purpose of a money collection may be difficult, especially if the customer relationship does not continue after the establishment of the foundation.

Remote identification is considered a normal means of identification in the sector, even though it is recognised that it involves uncertainties from the perspective of terrorist financing. Detecting terrorist connections through remote identification is all but impossible.

3.9.3 Terrorist financing risks associated with bookkeepers and auditors

The overall risk facing bookkeepers and auditors is at level two (**moderately significant**). A total of 27 experts from the public and private sector took part in the assessment. For a definition of the operating environment of the sector, see section 2.9.3.1.

Difficulty of detecting suspicious transactions due to a high workload is seen as a significant risk in terms of vulnerability. A large number of customers and the pace of work are factors contributing to the risk. Bookkeepers, who are more closely involved in the processing of the customers' accounting material, are considered a particularly risk-affected group, whereas auditors review the material retroactively using a risk-based approach.

The use of bogus receipts has also been identified as a risk in the sector from the perspective of terrorist financing. Criminal actors may try to include seemingly correct receipts in the accounting material to mislead bookkeepers and auditors. Customers may disguise terrorist financing activities in the receipts to make them look legal, concerning consultancy fees, for example. Again, bookkeepers (especially newly established accounting firms) are particularly vulnerable in this respect.

Reluctance to question customer activities arising from the fear of losing business is seen as a moderately significant risk. The obliged entity may suspect fraud or misconduct but, being anxious not to lose a customer, may decide against investigating the matter any further. As a result, the terrorist financing will remain undetected. However, this risk is more likely to be present in money laundering than terrorist financing.

3.9.4 Terrorist financing risks associated with providers of business services

The overall risk facing providers of business services is at level one (**less significant**). A total of 10 experts from the public and private sector took part in the assessment. For a definition of the operating environment of the sector, see section 2.9.4.1.

A significant risk arises when **providers of business services are exploited in the process of establishing a company** the real purpose of which is to channel funds for terrorist financing. As in the case of attorneys-at-law and other providers of legal services, it is difficult to ascertain the real purpose of the funds of the new organisation if the monitoring does not continue beyond the establishment stage.

3.9.5 Terrorist financing risks associated with pawnbrokers

The overall risk facing pawnbrokers is at level one (**less significant**). A total of 10 experts from the public and private sector took part in the assessment. For a definition of the operating environment of the sector, see section 2.9.5.1.

Using pawning for the purpose of raising funds is seen as a significant risk facing pawnbrokers. Individuals (such as foreign fighters) may be under the impression that pawning is an easy way to obtain money and thus they may try to pawn all their belongings with monetary value before travelling to a conflict zone. Even though pawnbrokers make attempts to accurately establish the origin of the items, the loan granted by the pawnbroker may be used to finance terrorism. It is extremely difficult for a pawnshop to detect this.

3.9.6 Terrorist financing risks associated with art dealers

The overall risk facing art dealers is at level two (**moderately significant**). A total of 10 experts from the public and private sector took part in the assessment. For a definition of the operating environment of the sector, see section 2.9.6.1.

Situations in which the **proceeds of product sales are channelled to non-EEA countries** are considered a moderately significant risk. Even though this may involve any category of art objects, sales of oriental carpets and the ultimate destination of the proceeds of their sales are identified as a particular challenge.

3.9.7 Terrorist financing risks associated with goods retailers

The overall risk facing goods retailers is at level two (**moderately significant**). A total of 11 experts from the public and private sector took part in the assessment. For a definition of the operating environment of the sector, see section 2.9.7.1.

Situations in which **goods retailers use their own business to finance terrorism** are seen as significant risk in this sector. Few such cases have been reported but even if the practice were to become more common, it would be extremely difficult to supervise.

4 Phenomena

Topical issues concerning money laundering and terrorist financing were selected as subjects for the phenomenon section of the risk assessment. The phenomena exam- ined in the section are as follows:

- cash
- Covid-19 pandemic
- trafficking in human beings
- legal persons and
- weapons of mass destruction.

Cash was selected for examination because it remains a key means of money laundering. Even though digital means of transferring funds have assumed more importance, cash must be considered particularly attractive to criminals.

The Covid-19 pandemic was selected because of its topical nature and because it has had a particularly strong impact on the criminal operating environment by encouraging fraud. National-level observations related to the coronavirus pandemic that are relevant to the first risk assessment are discussed in the section from the perspective of money laundering and terrorist financing.

Trafficking in human beings is a global phenomenon and it is also connected with other serious crime. For this reason, it was considered appropriate to highlight the phenomenon in the risk assessment. Combating of human trafficking has been a focus area in Finland in recent years. In line with this, the police have been provided with additional resources to investigate human trafficking offences, and a separate police team tackling the problem is in the process of being established.[224] Trafficking in human beings may be a money laundering predicate offence and observations concerning this are discussed in the risk assessment.

224 Ministry of the Interior: Stepping up the fight against human trafficking through cooperation between authorities and organisations, referred to on 20 January 2021.

In its 2019 Mutual Evaluation Report on Finland, FATF noted that the potential misuse of legal persons should be considered in the risk assessment.[225] Risks facing non-profit legal persons are discussed in the NPO section of the risk assessment, and in the phenomenon section, the focus is on specific profit-driven legal persons.

Preventing funding of weapons of mass destruction is a topical issue for FATF as in October 2020, it adopted amendments to Recommendations 1 and 2. Under the amendments, FATF members and their obliged entities must identify the risks concerning operating models used to circumvent financial sanctions. Members and obliged entities must implement the amendments by a specific deadline and they will only become part of the mutual evaluation process in the fifth round of evaluations. Prompted by the changes, it has also been decided to highlight the phenomenon of weapons of mass destruction in the risk assessment and the section discussing them is intended as a theoretical overview of the subject. The topic should be discussed more extensively as FATF develops its guidelines.

The new risk sectors highlighted in the supranational risk assessment of the EU (professional football, free ports, and investor citizenship and residence schemes) are also discussed in the phenomenon section.

4.1 Cash

According to the Bank of Finland, use of cash has been on the decline in recent years, which is reflected in the number of cash withdrawals. Cash withdrawals totalling EUR 13.2 billion were made in Finland in 2019, compared with EUR 14.5 billion in the year before. Card purchases totalled EUR 54 billion in 2019.[226] The coronavirus pandemic caused a further decline in the use of cash during the early months of 2020.[227]

However, cash is still considered a key means of money laundering and terrorist financing as it offers anonymity and is difficult to trace. This makes cash-intensive sectors, such as restaurants, vulnerable to exploitation.[228] Customer identification and verification of identity are required when the value of the cash purchase exceeds EUR 10,000.[229] Identification and verification of identity are also required in suspicious transactions or if

225 FATF MER 2019, p. 12.

226 The Bank of Finland: Payments statistics 2019, referred to on 22 July 2020.

227 Europol 2020a, p. 18.

228 Europol 2015, p. 28.

229 By way of derogation from this rule, in gambling operations, a customer must be identified and their identity verified when a stake is wagered or winnings are collected or in both situations if the stake wagered or the winnings collected by the gambler totals at least EUR 2,000 as a single transaction or as linked transactions.

the obliged entity suspects that the funds involved in the transaction are used to finance terrorism or a punishable attempt of terrorist financing or the obliged entity has doubts about the adequacy or veracity of the verification information concerning an already identified customer. Under the Anti-Money Laundering Act, parties selling or brokering goods as part of their business activities or on a professional basis and that accept cash payments of at least EUR 10,000 must submit money laundering reports on their activities.

In 2019, the Grey Economy Information Unit carried out an extensive survey among government agencies in which the participants were asked which shadow economy phenomena they had encountered in their work and which of the phenomena had been particularly noticeable over the preceding three years. About 45 per cent of the respondents had noted that the use of cash is connected with the shadow economy.[230]

According to the 2015 national risk assessment, transport of cash is potentially a very significant money laundering and terrorist financing risk. According to the expert assessments contained in the risk assessment, cash couriers exploiting the free movement of people inside the EU are a common means of money laundering and terrorist financing.[231]

The Financial Intelligence Unit receives cash-related reports from obliged entities and reports on cross-border cash transports from the Finnish Customs.[232] An individual must submit a cash declaration to the Finnish Customs when leaving or entering the EU and carrying at least EUR 10,000 in cash. According to the Finnish Customs, individuals entering and leaving Finland in 2019 declared cash totalling about EUR 40 million. The sums have grown substantially over the past few years, as in 2016, the figure was about EUR 25 million. The Finnish Border Guard is also a competent authority in matters concerning cash transports when carrying out customs tasks.

4.1.1 Money laundering risks associated with cash

Cash is attractive to criminals because it is **an anonymous, untraceable, direct and irreversible means of transferring value**. For the same reasons, cash should also be considered a high-risk money laundering instrument. Cash may be connected with a wide range of different money laundering predicate offences, such as fraud, trafficking in human beings, theft and drugs trade. According to Europol, cash can be used as a means of money laundering in nearly all types of crime.[233]

230 Grey Economy Information Unit 2019, p. 25.

231 National risk assessment of money laundering and terrorist financing 2015, p. 106.

232 Financial Intelligence Unit 2019, p. 9.

233 Europol 2015, p. 10.

Cash is an instrument that allows the shadow economy to function. For example, in human trafficking offences, paying undeclared salaries in cash allows money laundering to take place. A company may also **claim that its business is cash-based** even though this is not the case.

Cash transports can be by means of couriers or money mules, allowing the source of the funds to be obliterated. Cash couriers are individuals recruited by criminals who carry criminally obtained cash between countries.[234] Cash couriers are not necessarily aware of the purpose of the cash they are carrying. Funds can also be transferred to other countries by means of **currency exchange**, in which the origin of the funds is obliterated by exchanging cash into other currencies. The sentence given by the Eastern Uusimaa District Court on 1 November 2019[235] is an example of the carrying of cash and the money laundering connected with it.

Case involving a cash courier

Person A had first travelled from Spain to Finland on 25 August 2019. He had then received a sum of EUR 14,000 from a Finnish individual in a hotel and, in accordance with his assignment, had taken the money to Spain on 26 August 2019 where he had handed over the amount to other persons. Person A had received EUR 1,000 for carrying out the task. Person A travelled from Spain to Finland for a second time on 13 September 2019 to take a sum of EUR 13,000 to Spain. During the visit, he had met with the Finnish person that he had already met during his first visit and received from him an amount of money in cash. Person A was allowed to use some of the money to pay for his travel expenses. Person A had tried to leave Finland on 15 September 2019 with the remaining EUR 12,500 in an envelope hidden in his luggage.

According to the prosecutor, the money can be considered to have originated from criminal activities, taking into account the nature of Person A's assignment (taking money from Finland to Spain), the fee of EUR 1,000 promised to Person A for both trips and the large amount of cash involved. Person A had also assumed that the money had originated from illegal activities. Person A admitted that he had acted in the manner described by the prosecutor and he received a sentence for aggravated money laundering. The sentence is legally valid.

234 FATF and MENAFATF 2015, p. 28.

235 Sentence the Eastern Uusimaa District Court, 1 November 2019 No. 19/148060, case R 19/4372.

Use of cash can be considered a culture-specific phenomenon as cash is more widely used in the areas adjacent to Finland than it is in Finland. For this reason, **extensive use of cash by foreigners** may create risks, as establishing the source of the funds is difficult, especially when the cash has originated from outside Finland.

The coronavirus pandemic has also impacted the use of cash and thus also the number of money laundering reports. According to the Financial Intelligence Unit, banks have been particularly alert with regard to large cash transactions during the coronavirus pandemic. Between March and October 2020, banks submitted more money laundering reports using the indicators 'several cash withdrawals' and 'several cash deposits' than in the same period in 2019. Cash-related money laundering reports accounted for 66 per cent of all money laundering reports submitted by Finnish banks between March and October 2020.[236]

4.1.2 Terrorist financing risks associated with cash

Cash-related risks associated with terrorist financing are fairly similar to those associated with money laundering. However, terrorist financing does not require a predicate offence and thus in the case of cash, the focus is on transferring the money to terrorist purposes. According to Europol, similar means of transferring and concealing cash funds can be used in both money laundering and terrorist financing.[237]

Many of the terrorist financing risks associated with cash are the same as those identified in connection with other sectors. For example, **converting consumer credit into cash** and forwarding the money to conflict zones or **converting cash into virtual currencies** and withdrawing it from virtual currency dispensers in a high-risk country are identified as risks.

In particular, it has been noted that actors **fail to understand** the existence of a link between cash and terrorist finance. As a result, they may not realise that one only needs very small amounts of cash when acting with the intention of financing terrorism. As the use of cash in banking systems has decreased, it has become an increasingly common means of transactions in sectors where large amounts of cash are still readily accepted.

In this respect, cash-related money transfers may in the future become a more widespread practice among hawalas and other money remittance services.

---

236 Helsingin Sanomat 20.10.2020: Koronapandemian aikana käteisen käyttö on vähentynyt: Suuntaus johtaa entistä helpommin rahanpesu-ilmoitukseen ja tietää vaikeuksia rikollisille, [*Use of cash has decreased during the coronavirus pandemic: This trend will lead to an increase in the filing of money laundering reports and will cause problems for criminals*], referred to on 22 December 2020.

237 Europol 2015, p. 45.

Different types of **cash-based money collections** also involve a terrorist financing risk. There may be efforts to exploit the organiser of the collection so that the activities would appear outwardly legitimate. Moreover, the party organising a seemingly legitimate money collection may also be involved in activities aimed at terrorist financing. Small sums can also be used for terrorist financing purposes, which makes identification of suspicious activities very difficult. This is because people normally donate small sums in cash-based fundraising drives.

4.2 Covid-19 pandemic

The novel Covid-19 virus started spreading from China at the end of 2019. According to the World Health Organization, the disease has developed into a pandemic because it has spread to all parts of the world. The first coronavirus vaccine received marketing authorisation in the EU on 21 December 2020. Finland is a participant in all purchases of coronavirus vaccines made by the EU.[238]

The Covid-19 pandemic has resulted in unprecedented global challenges, and economic disruptions and crises. The pandemic has prompted many countries to introduce emergency measures, which has also made criminals more active and led to new criminal phenomena. It has been noted that the fraud, cybercrime and misuse of international financial assistance resulting from the emergency-related vulnerabilities are creating new sources of proceeds for illicit actors and other criminals.[239] It has also been noted that the reduction in the use of cash prompted by the Covid-19 pandemic has also impacted money laundering methods. This is because money laundering in cashintensive sectors is now more difficult[240] and less cash is transported between countries. According to Europol, in the long term, the pandemic will have substantial impacts on economic crime. This means that criminal actors must find new money laundering methods to replace cash.[241]

There have been a large number of attempted hoaxes in conjunction with the Covid-19 pandemic and the first of them emerged in spring 2020 as the crisis came to a head. Consumers have been offered non-existent coronavirus test kits, face

238 Finnish Institute for Health and Welfare: Coronavirus COVID-19 – Latest Updates, referred to on 7 August 2020, World Health Organization: Coronavirus disease (COVID-19 pandemic), referred to on 7 August 2020; Finnish Institute for Health and Welfare: Arranging COVID-19 vaccinations in Finland, referred to on 14 January 2021.

239 FATF 2020a, pp. 2 and 4.

240 Europol 2020b, p. 7.

241 Europol 2020b, p. 12.

masks or pharmaceuticals.[242] The police have also warned the public of coronavirus scammers who have mainly targeted elderly people. Claiming to be coronavirus inspectors or health officials, these scammers have attempted to enter homes in order to steal cash or valuables.[243]

4.2.1 Impacts of the Covid-19 pandemic on money laundering

With the coronavirus pandemic, different types of **fraud** have become an increasingly common phenomenon in the criminal operating environment and they are also typical predicate offences of money laundering. The offences mainly involve online fraud in which criminals are selling products that do not exist or that are of poorer quality than what had been promised. These products include pharmaceuticals or protective equipment. In a case uncovered in Finland in spring 2020, a large number of face masks proved unsuitable, prompting a fraud investigation. FATF has identified a scenario in which criminals claiming to be employees of a company or a charity organisation sell face masks or coronavirus test kits. The actors request credit card details for payment but never deliver the goods.[244]

Fraud also involves different types of **cybercrime** in which criminal actors, citing the Covid-19 pandemic, try to obtain information by phone or by email. In a number of cases reported to the Finnish Institute for Health and Welfare, scammers have requested payment card details by phone, for reasons such as exposure to the coronavirus or a coronavirus test.[245] Scammers may also try to take advantage of the coronavirus situation by organising money collections in which they exploit people's willingness to help. Organisers claim that the purpose of the **money collections** is to help those suffering from the coronavirus crisis but in reality the proceeds may go to criminals. According to FATF, criminals claiming to represent charities circulate emails requesting donations.

Recipients of these emails are then directed to provide credit card information or make payments through the criminals' digital wallet.[246]

The coronavirus pandemic has led to a sharp fall in travel and as a result, fewer people now move across national boundaries. However, one can still enter Finland for valid

242 Yle News 5 April 2020, referred to on 9 November 2020.

243 Police: Poliisi varoittaa koronahuijareista – huijausten kohteina etenkin iäkkäät [*Police issues warning about coronavirus scammers – the elderly are the biggest target*], referred to on 9 November 2020.

244 FATF 2020a, p. 6.

245 Kauppalehti 16.8.2020: Saitko puhelun, jossa kyseltiin maksukortin tietoja koronatestauksen takia? – THL varoittaa huijaussoitoista [Have you had a phone call asking for payment card details for coronavirus testing? – Finnish Institute for Health and Welfare is warning people about scam phone calls], referred to on 21 December 2020.

246 FATF 2020a, p. 7.

reasons, such as work. Actors in specific high-risk sectors, such as construction workers, have been able to move across national boundaries almost as normal. Thus, such individuals can still be used as cash couriers. As mentioned above, Europol has noted that from the criminal perspective, the coronavirus pandemic has had a particularly strong impact on the transport of cash. As a result, money laundering is now carried out **by other means**. In fact, the assumption is that the operating environment is becoming increasingly digital and criminals will make more use of digital solutions when transferring funds.

Efforts have been made to assist companies and their business operations hit by the Covid-19 pandemic with different types of economic support. Even though in public, this support has been referred to as 'coronavirus subsidies', the support is also intended to boost business development and innovations. It has been suggested that recipients might be able to misuse the subsidies because the criteria for granting them may be flexible and the supervision is mostly on a retroactive basis. Criminal actors might circumvent the criteria by disguising their activities as legitimate and the funds granted as support could be channelled to criminal activities or obliterated by means of money laundering. In the survey carried out by the Grey Economy Information Unit of the Finnish Tax Administration, some 64 per cent of the authorities participating in the survey felt that there has been a slight or significant increase in the **misuse of public subsidies** as a result of the Covid-19 crisis.[247]

The financial distress facing companies may also make it more difficult for **actors in individual sectors to detect crime**. The problems in companies arising from the Covid-19 pandemic may blur the views on what can be considered as normal and what should be approached with suspicion. It emerged from the interviews with private sector actors that in some sectors, activities that would normally be deemed suspicious are now considered routine, and this has also made detecting suspicious transactions more difficult.

The Covid-19 pandemic has prompted many people to transfer to **remote work** and as a result, many services are now only available on a remote basis. Remote work may make it more difficult for actors to apply proper customer due diligence to their clientele. According to the survey conducted by the Grey Economy Information Unit in government agencies, remote work also impacts the supervision carried out by the authorities: 55 per cent of the respondents felt that the increase in remote work has made supervision less effective.[248]

247 The survey was carried out in September 2020 and it charted the views of government agencies on the impacts of the COVID-19 crisis on the combating of the shadow economy. For more details, see Grey economy & economic crime: Koronavirus lisännyt viranomaisten huolta tukipetosten kasvusta [*Coronavirus has increased the authorities' concerns of an increase in fraud associated with public aid.*], referred to on 21 December 2020.

248 Grey economy & economic crime: Koronavirus lisännyt viranomaisten huolta tukipetosten kasvusta [*Coronavirus has increased the authorities' concerns of an increase in fraud associated with public aid*], referred to on 21 December 2020.

4.2.2 Impacts of the Covid-19 pandemic on terrorist financing

Decrease in passenger traffic prompted by the Covid-19 pandemic and the fact that as a result, transporting cash has become more difficult may make hawalas a more popular means of terrorist financing. As cash couriers have been unable to carry cash intended for terrorist financing across national boundaries, cash may be transferred to hawala actors that forward the funds to the destination countries by electronic means. Traditional **payment gateway providers** are also increasingly used to forward cash to recipients.

The Covid-19 pandemic has also impacted the phenomenon of **foreign fighters**. Movements, funding trips and arranging travel have become more difficult during the Covid-19 crisis. As a result, individuals make increasing use of illegal routes not controlled by the authorities. The economic uncertainty caused by the Covid-19 pandemic and the resulting heavy psychological stress may lead to emotional instability, which **may radicalise** individuals, depending on their connections and sphere of life.

4.3 Trafficking in human beings

In the risk assessment, the term 'trafficking in human beings' refers to the definition contained in the Palermo Protocol, which is also used by FATF in its own publications.[249] Under the Criminal Code of Finland, trafficking in human beings, aggravated trafficking in human beings and their attempts are punishable acts. Offences resembling trafficking in human beings listed in the Criminal Code, such as aggravated pandering, aggravated arrangement of illegal immigration and extortionate work discrimination are also offences falling within the scope of the human trafficking definition used in the risk assessment. In legislation, trafficking in human beings may not be defined in the same manner in all countries, which makes it more difficult to investigate the cases. Trafficking in human beings differs from human smuggling (such as aggravated arrangement of illegal immigration) in that in human smuggling, the proceeds of crime are in the form of payments for the arrangement of illegal immigration whereas in trafficking in human beings, the aim is to achieve gains by exploiting the victims.

Trafficking in human beings is a growing phenomenon affecting all parts of the world. Trafficking in human beings is one of the most lucrative crimes when judged on the basis

249 The definition used by FATF is based on the United Nations Convention Against Transnational Organized Crime (Palermo Convention) in which trafficking in human beings is defined as follows: 'the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Ex- ploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs'.

of the gains generated by it. According to an estimate produced by the International Labour Organization (ILO), forced labour generates USD 150.2 billion each year.[250] Even though trafficking in human beings is one of the most rapidly growing types of crime,[251] the authorities now also have a better understanding of the phenomenon, and measures are taken to tackle it, both nationally and internationally.

In Finland, the topic is primarily studied and monitored at the official level by such bodies as the Non-Discrimination Ombudsman, Finnish Immigration Service, and the European Institute for Crime Prevention and Control (HEUNI).[252] The post of Anti-Trafficking Coordinator has also been established in the Ministry of Justice. The Non-Discrimination Ombudsman acts as Finland's National Rapporteur on Trafficking in Human Beings. The assistance system for victims of human trafficking operates under the auspices of the Finnish Immigration Service. The assistance system supports and helps victims of human trafficking and their underage children. Statistics indicate that an increasing number of human trafficking victims seek help from the system and the number of customers has almost tripled over the past few years.[253]

To ensure the effectiveness of the prevention of human trafficking and the phenomena of money laundering and terrorist financing connected with it at national level, all parties involved should recognise that human trafficking also occurs in Finland and be familiar with its different forms. Trafficking in human beings is often a cross-border activity and Finland mainly serves as a country of transit and destination of human trafficking. At national level, crime connected with trafficking in human beings has mainly manifested itself in labour exploitation, sexual exploitation and exploitation in connection with criminal activities. In human trafficking carried out as part of criminal activities, the victims are forced to carry out illegal acts and the proceeds of these crimes go to the parties exploiting the victims. There have also been reports of human trafficking connected with forced marriages and begging.[254] From the perspective of combating money laundering, it is also important to identify the proceeds of crime generated by human trafficking. In labour exploitation, the proceeds of crime are generated by not paying any wages to the employees, or they are substantially underpaid and/or charged an excessive fee for accommodation and other living costs. The cases often involve shadow economy and accounting offences.[255] Cleaning, restaurant, home help, picking of wild and cultivated berries, and the construction industry are some of the sectors vulnerable to labour exploitation.

250 FATF 2018, p. 3.

251 FATF 2018, p. 3.

252 For more information, visit: www.heuni.fi, www.ihmiskauppa.fi and www.syrjinta.fi.

253 The assistance system for victims of human trafficking, press release 15 July 2020, referred to on 26 August 2020.

254 Police: Trafficking in human beings, referred to on 26 August 2020; The assistance system for victims of human trafficking, 2020, pp. 5 and 11.

255 HEUNI 2019, p. 6.

4.3.1 Links between human trafficking and money laundering

According to expert assessments, trafficking in human beings is also closely connected with money laundering. This is because criminals try to obliterate the proceeds of crime generated by human trafficking by means of money laundering. Identifying and preventing human trafficking also help to prevent money laundering. In fact, **inadequate awareness** of human trafficking and associated indicators and operating models in Finland is seen as a money laundering risk. If the parties involved were better placed to identify the phenomenon and different ways of human trafficking, criminal activities could already be tackled at an early stage. For example, actors specified as obliged entities in the Anti-Money Laundering Act might also be able to detect trafficking in human beings or suspicious activities suggesting human trafficking when monitoring the transactions of their customers. FATF has also identified a number of indicators helping actors to identify such events as suspicious account transactions.[256]

Trafficking in human beings is **hidden crime**, which makes it more difficult to detect. All victims are subject to coercion and many of them are already in a vulnerable position.

Victims rarely report human trafficking to the police. Trafficking in human beings is often concealed by means of shell companies and by exploiting existing structures (for example, by opening bank accounts for employees that are actually used by other parties). In other words, in the national operating environment, trafficking in human beings is **concealed by using seemingly legitimate operating models**.

Detecting suspicious activities and human trafficking is difficult because they often take place **across national boundaries** and involve international connections. As many of the victims are foreigners, the threshold for seeking assistance is high. Difficulty of detecting trafficking in human beings also leads to **supervision-related problems** in both public and private sectors. In fact, establishing a police group specialising in the uncovering and investigation of human trafficking offences was set out as a goal in the 2019 Government Programme. This is because the view in many European countries is that with such units, offences involving human trafficking can now be investigated more effectively.[257]

The use of foreign personnel leasing companies and long subcontracting chains make it more difficult to detect trafficking in human beings. Detecting human trafficking requires active and proactive measures by the authorities, companies and other actors.

256 Links between human trafficking and money laundering are also discussed in the 2020 report 'Uncovering labour trafficking' by the European Institute for Crime Prevention and Control. The indicators facilitating the identification of trafficking in human beings are described on pages 66- 70 of 'Financial Flows from Human Trafficking' published by FATF in 2018. The European Institute for Crime Prevention and Control also referred to the FATF publication in its own report.

257 HEUNI 2020, p. 58.

Supervision-related problems and enhancing the legitimacy of the operations are key issues with regard to foreign service providers.

Legislative limitations and inadequacies are also one of the money laundering risks associated with trafficking in human beings. According to expert assessments, inadequacies concerning the exchange of information should be addressed notwithstanding secrecy provisions. Moreover, short time-barring periods for such offences as extortionate work discrimination and mild sentences for human trafficking make the operating environment more attractive to criminals.

Between 2015 and 2019, a total of 14 sentences were given for trafficking in human beings, 6 for aggravated trafficking in human beings and 14 for extortionate work discrimination. For comparison, more than 200 criminal investigations on trafficking in human beings and more than 150 criminal investigations on extortionate work discrimination were opened between 2015 and 2018. On average, fewer than ten criminal investigations on aggravated human trafficking are opened each year.[258] Only a small proportion of the criminal investigations lead to human trafficking sentences.

Cases investigated by the authorities of more than one country involving links between human trafficking and money laundering include situations in which the perpetrators deposit or transfer substantial sums to the victims' accounts. After this, the funds are transferred from the victims' accounts to other countries or converted into other property. In other words, the victims have been used as intermediaries without their knowledge.[259]

4.3.2 Links between trafficking in human beings and terrorist financing

According to expert assessments, money laundering is more extensively connected with human trafficking than terrorist financing. **Lack of evidence of the links between human trafficking and terrorist financing at national level** is seen as the most significant risk in terms of terrorist financing. This means that there is no evidence of connections between terrorist financing and human trafficking at the national level. However, it is possible that such links exist.

According to a report by the Counter-Terrorism Committee of the United Nations, there is evidence that terrorists finance their activities by means of human trafficking by kidnapping women and children, by demanding ransom payments or by selling victims

258 Statistics Finland and PolStat.

259 HEUNI 2020, p. 48.

as sex slaves. Terrorist activities are also financed through organ trafficking and selling of slaves.[260]

The geographical dimension is seen as a risk concerning human trafficking and the terrorist financing associated with it. **Links of the perpetrator (or suspect) with conflict zones or regions adjacent to them** also increase the terrorist financing risk. If both the perpetrator and the victim have links with conflict zones, the risk is considered even higher.

Human trafficking offences involve illicit transactions and the victims are often unaware of the actual destinations of the payments. According to experts, there may be cases in which the proceeds of labour exploitation are channelled to terrorist groups.

4.4 Legal persons

A legal person is a legally competent actor with the right to decide on its own rights and obligations. Legal persons are non-natural persons, such as companies, that own assets and may decide on them independently.[261] The following legal persons structured as companies[262] are examined in this risk assessment:

- limited liability companies referred to in chapter 1(2) of the Limited Liability Companies Act (624/2006)
- general partnerships and limited partnerships referred to in chapter 1(1) of the Partnerships Act (389/1988)
- cooperatives referred to in chapter 1(2) of the Cooperatives Act (421/2013).

The purpose of the company forms examined here is to generate profits for their shareholders or pursue economic or business activities. According to the Trade Register, there were a total of about 300,000 limited liability companies, general partnerships, limited partnerships and cooperatives in Finland on 1 July 2020.[263] An individual can also pursue

260 CTED 2019, pp. 31-37.

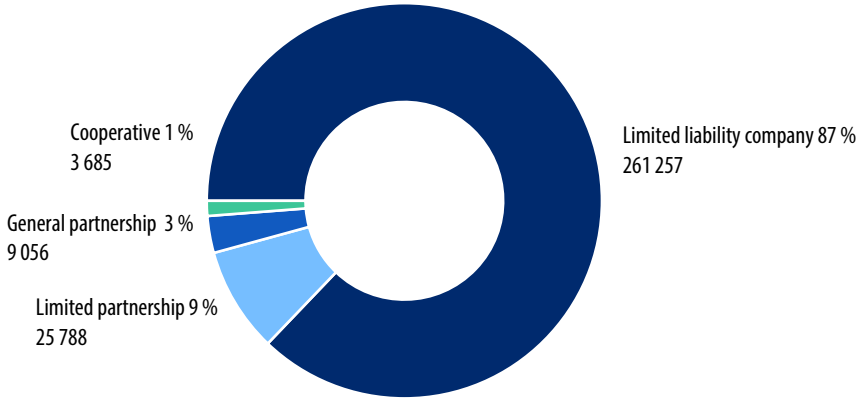
261 Villa 2018, p. 34 and HE 95/1993 vp, p. 27.

262 Even though foundations and registered associations can also be considered as legal persons, only legal persons structured as companies are examined in this section. Foundations and associations are discussed separately in chapter 5 of the risk assessment (NPO sector).

263 Finnish Patent and Registration Office: Number of enterprises in the Trade Register, referred to on 9 November 2020.

business activities as a private trader. However, private traders are not considered as independent legal persons, as they enter into commitments under their own name.[264]

Figure 3. Number of limited liability companies, general partnerships, limited partnerships and cooperatives in the Trade Register on 1 July 2020.



Under chapter 6 of the Anti-Money Laundering Act, the above-mentioned organisations must keep the details of their beneficial owners up to date. A beneficial owner is a natural person who, directly or indirectly, owns more than 25 per cent of the shares of a legal person or who otherwise owns a similar share of the legal person. The following natural persons are also considered beneficial owners: 1) a natural person who, directly or indirectly, holds more than 25 per cent of the voting rights of a legal person and these voting rights are based on ownership, membership, articles of association, partnership agreement or other similar rules; and 2) a natural person who exercises its controlling interest in a legal person in other ways. Most companies[265] had to submit the details of their beneficial owners to the Trade Register between 1 July 2019 and 1 July 2020. The obligation applied to about 300,000 companies and about 123,000 of them submitted the details by the deadline.[266] Failure to enter the details of the beneficial owners in the

264 Suomen Yrittäjät: Private trader, referred to on 9 November 2020. According to the Trade Register, there were about 220,000 private traders in Finland on 1 July 2020, which is a large number when compared with the total number of companies in Finland. See Finnish Patent and Registra- tion Office: Number of enterprises in the Trade Register. Available: https://www.prh.fi/fi/kauppa- rekisteri/yritystenlkm/lkm.html, referred to on 9 November 2020.

265 Limited liability companies and cooperatives must submit the details of their beneficial owners to the Trade Register. General partnerships must submit the details of their beneficial owners that are not natural persons serving as partners. Limited partnerships must submit the details of their beneficial owners that are not natural persons serving as general partners.

266 Press release of the Finnish Patent and Registration Office of 2 July 2020, referred to on 29 July 2020.

Trade Register or to keep them up to date may negatively impact the operations of the company.

Limited liability companies, general partnerships, limited partnerships and cooperatives must enter their details in the Trade Register kept by the Finnish Patent and Registration Office. Under chapter 2 of the Auditing Act (1141/2015), organisations must appoint an auditor and conduct an audit.[267] Limited liability companies and cooperatives must always enter their financial statements in the Trade Register. General partnerships and limited partnerships must enter their financial statements in the Trade Register when specific requirements are met.[268]

The activities and sector of the legal person must also be considered when money laundering and terrorist financing risks are assessed. This is because when a legal person pursues business activities falling within the scope of the Anti-Money Laundering Act, it can become an obliged entity under the act.

The Grey Economy Information Unit has listed four ways of using companies for fraudulent purposes:

1. Establishing a company for fraudulent purposes
2. Acquiring a company in difficulty
3. Hijacking a company operating in accordance with the law
4. Exploiting the name of a company operating in accordance with the law

Intermediaries acting in their own name while at the same time acting covertly on behalf of other individuals are often appointed as persons in charge of the company. Professional exploitation of companies is fraud.[269] Detecting professional exploitation of companies is important because crimes involving fraud are the most important money laundering predicate offences.

---

267 There is no obligation to appoint an auditor for an organisation where no more than one of the following conditions were met in both the last completed financial year and the financial year im- mediately preceding it: 1) the balance sheet total exceeds EUR 100,000; 2) the net sales or com- parable revenue exceeds EUR 200,000; or 3) the average number of employees exceeds three.

268 General partnerships and limited partnerships must enter their financial statements in the Trade Register if one of the following conditions is met: 1) one of the partners or general partners is a limited liability company; 2) one of the partners or general partners is a general partnership or a limited partnership that has a limited liability company as a general partner; or 3) at least two of the following conditions were met in the last completed financial year or in the financial year im- mediately preceding it: a) net sales totalled EUR 12,000,000; b) balance sheet total was EUR 6,000,000; and c) the average number of employees was 50. See Finnish Patent and Registration Office: General partnerships and limited partnerships must enter their financial statements in the Trade Register, referred to on 10 November 2020.

269 Grey economy & economic crime: Professional exploitation of companies is fraud, referred to on 23 December 2020.

Organised criminal groups are a major threat in terms of money laundering and for this reason, there are good grounds for examining the report on business links between organised crime and companies. According to a report on organised criminal groups published in 2015, organised crime in Finland is involved in such sectors as construction, renovation construction, service and cleaning, restaurants, nightclubs, private security services, retail sales of cars, tattooing and sex outlets. Organised criminal groups mainly operate in labour-intensive and low-technology sectors and in sectors that are close to their own cultures and lifestyles and not closely supervised by the authorities. Companies involving organised criminal groups are usually small but they often provide a wide range of different services, such as security services combined with such services as cleaning. More than half of all members of organised criminal groups have a business of their own.[270]

4.4.1 Money laundering risks related to legal persons

As a rule, legal persons are associated with a higher risk of money laundering and terrorist financing because the natural persons behind legal persons are not acting in their own name. It should be noted, however, that the key aim of the Limited Liability Companies Act (624/2006) is to provide companies with more freedom of action and for this reason, the act is intended to be flexible. Legal persons are continuously established and used and increasing their freedom of action in a controlled manner is of great societal importance from the perspective of the prerequisites for entrepreneurship and freedom of association. In fact, when the risks associated with legal persons are examined, the context of the wide corporate dimension should be kept in mind.

To mitigate the risks, companies are obliged to submit the details of their beneficial owners to the Trade Register. However, not all companies fulfil this obligation or keep the information up to date and for this reason, the details of beneficial owners contained in the Trade Register are not always up to date or adequate. This increases the risk that the criminal actors behind the legal persons remain unidentified.

The use of intermediaries in different types of business activity is a general risk facing legal persons. In a survey commissioned by the Grey Economy Information Unit, more than two thirds of the respondents[271] had noted use of intermediaries.[272] The use of intermediaries has been identified as an extremely common way of concealing the identity of the actors or beneficiaries. Even though the use of intermediaries is not only

270 OCP 2015, pp. 168–169.

271 More than 600 respondents in 19 government agencies.

272 Grey Economy Information Unit 2019, p. 25.

connected with internationalisation, the use of foreigners as intermediaries provides shadow economy actors with more opportunities and makes criminal investigations more difficult. Use of intermediaries is seen as a well-established method and no concrete action has been taken by the authorities to address the phenomenon.[273] Moreover, the use of intermediaries is not explicitly prohibited under the law.

The use of intermediaries, the use of companies for fraudulent purposes, identity fraud, the use of 'end-of-life caregivers', professional actors and organised crime were all listed as extremely serious phenomena in the survey conducted by the Grey Economy Information Unit. It also emerged from the responses that the shadow economy is becoming increasingly professional in nature.[274]

When the risk are assessed, attention should also be paid to companies that are outwardly in compliance with the law and take care of their statutory payments and other obligations but that in reality have been established to conceal suspicious business activities. To ensure unhindered criminal activities, criminals may try to dispel any suspicions of illegal activities by convincing the authorities that their company adheres to the law. It has also been noted that the risk facing the persons in charge of the companies is higher if they have criminal backgrounds. According to the report by the Grey Economy Information Unit, there are many short life-cycle companies among the companies managed by persons with criminal backgrounds, and such companies are seen as a risk in terms of money laundering. Short life-cycle companies can be used for such purposes as circumventing statutory obligations.[275] It should also be noted that there is no legislation on supervising compliance with the organisations' auditing obligation and the registration authority does not inspect the contents of the financial statements. Ways to ensure better supervision of compliance with the auditing obligation are expected to be discussed in conjunction with the overhaul of the trade register legislation.[276]

Exploitation and hijacking of existing companies by criminals has been identified as a potential risk scenario. Inactive companies in particular[277] may be targeted and money laundering attempts may lie behind the activities. The number of inactive companies is relatively high in Finland and in 2020, the Finnish Patent and Registration Office removed nearly 20,000 companies and other organisations from the Trade Register. Inactive companies may be enterprises that do not actively submit information to the

273 Grey Economy Information Unit 2019, p. 30.

274 Grey Economy Information Unit 2019, p. 27.

275 Grey Economy Information Unit 2018, p. 9. However, a company's life cycle may also be short because of reasons arising from the nature of its business operations (such as projects).

276 Ministry of Economic Affairs and Employment 2020, pp. 12, 26 and 31.

277 FATF MER 2019, p. 137.

Trade Register but that nevertheless pursue business activities. The risk arising from such companies involves concealing of operations, which can manifest itself in the failure to submit financial statements or give details of the persons in charge of the company.[278] Newly established or dormant companies that are waiting to be activated are also considered inactive companies. Such companies are vulnerable to the hijack- ings referred to above because the owners only check the companies' situation when the annual notifications must be submitted to the authorities.[279] The third type of inactive companies involves businesses that have ceased operations. These companies are also vulnerable to hijackings.[280]

The risk of money laundering facing **limited liability companies** is estimated as **significant**. The current ease of establishing a limited liability company is seen as a factor contributing to the risk. Since July 2019, share capital has no longer been a requirement for establishing a limited liability company. Prior to that, at least EUR 2,500 had to be invested in a new company as share capital. The change has made it easier to establish limited liability companies as front companies. In a limited liability company, owners can also conceal their holdings and complex ownership arrangements can be hidden behind the structure of a limited liability company. A strictly limited personal liability also makes this company form attractive. Low costs and the chance to use companies' accounts to transfer legal and illegal funds may provide a good cover for money laundering.

The registration of limited liability companies is not seen as a factor substantially mitigating the risk because the risk is often connected with the business operations themselves. The risk of a company becoming a victim of money laundering unintentionally is low when its internal monitoring arrangements are in place. When limited liability companies are compared with other types of legal person, it can be concluded that the ownership structure, connections with foreign owners and the ease of establishing the company are factors increasing the risk.

The risks concerning bearer shares are not seen as significant in terms of money laundering or terrorist financing. Since 1980, giving bearer shares has been illegal in Fin- land,

278 Such companies are subject to collection measures in connection with the process of the removal of the financial statements or the details of the persons in charge from the Trade Register, and the companies concerned react to these measures in order to prevent the removal from the Trade Register.

279 The Finnish Patent and Registration Office provides companies with services giving protection against hoaxes and hijackings. For example, a company can subscribe to a service in which it is automatically notified of changes in its details or pending notifications.

280 At the conclusion of the process of the removal of the financial statements or the details of the persons in charge, these companies are removed from the Trade Register.

and only a small number of such shares still exists.[281] When the risks are small, they can be kept under control using the existing legislation.

The money laundering risk facing **general partnerships and limited partnerships is seen as moderately significant**. The risk is mitigated by the personal liability of the partners. At the same time, personal liability[282] also allows the partners to make decisions and facilitates the use of company funds. However, in both general and limited partnerships, there are limitations to making control-related arrangements.

For cooperatives, the money laundering risk is estimated as **moderately significant**. In a cooperative, assets are not divided in the same manner as in other company types because generating profits for the owners is not the main purpose of a cooperative. Under chapter 4(14) of the Cooperatives Act, cooperatives must keep lists of their members and owners if the shares of the cooperative are not incorporated into the book-entry system. The reporting obligation referred to in the Anti-Money Laundering Act may materialise if the cooperative is engaged in savings fund activities, which falls within the scope of the Anti-Money Laundering Act.

For other types of legal person, such as European companies, mortgage societies, right-of-occupancy corporations and unincorporated state enterprises, the money laundering risk is **extremely low**.

4.4.2 Terrorist financing risks related to legal persons

For limited liability companies, the risk of terrorist financing is seen as **significant**. The risk is higher in situations in which establishing a legal person is easy. Furthermore, challenges arising from the identification of the actual and beneficial owners and the use of intermediaries play a key role when the risk of terrorist financing is assessed. Companies with short lifecycles may also be a risk from the perspective of money laundering and terrorist financing. Even though proactive risk prevention at the establishment of a legal person is difficult, the freezing list kept by the National Bureau of Investigation is nevertheless seen as an efficient retroactive instrument. The distribution of the assets is strictly regulated, which is seen as a factor mitigating the risk.

281 Finland has a total of about 8,800 active limited liability companies established before 1 January 1980 and in principle these may have bearer shares.

282 A limited liability company may also act as a general partner but in this context, the risk specifically refers to situations involving personal liability.

For general and limited partnerships, the risk of terrorist financing is also seen as **significant**. The personal liability of the partners and the ease of transferring and using the funds must be taken into account in the activities. The risk is higher if, for example, the activities are managed as a company-form family-internal business because outsiders have few chances of detecting any irregularities.

For cooperatives and other types of legal person, such as European companies, mortgage societies, right-of-occupancy corporations and unincorporated state enterprises, the risk of terrorist financing is **less significan**t. However, there may be attempts to use such actors (especially cooperatives) for terrorist financing purposes.

4.5 Preventing the proliferation and financing of weapons of mass destruction (counter proliferation financing)

The work on counter proliferation financing was carried out during the early stages of the risk assessment process. Finland's national CBRNE strategy presented in 2017 and the Mutual Evaluation Report on Finland prepared by FATF show that there is a need for a national-level assessment of counter proliferation financing, at least from a theoretical perspective. The section on proliferation was prepared by interviewing experts on weapons of mass destruction and counter proliferation.[283]

Weapons of mass destruction refer to chemical, biological and nuclear weapons.[284] However, material for these weapons, such as chemical, biological or radioactive substances as well as related knowhow and expertise can also be considered as weapons of mass destruction.[285]

The threat arising from the proliferation of weapons of mass destruction and the materials required for them is regulated through international agreements, arrangements and political initiatives as well as national legislation and measures. The most important instruments designed to prevent the proliferation of weapons of mass destruction are the conventions prohibiting and limiting the development, use and possession of weapons of mass destruction (such as the Chemical Weapons Convention), UN Security Council Resolution 1540, export control arrangements, and national and international strategies

283 Experts from the Ministry for Foreign Affairs, Ministry of Defence and the Finnish Security and Intelligence Service were interviewed for the assessment.

284 Ministry for Foreign Affairs: Arms control and disarmament., referred to on 5 August 2020.

285 Expert statement.

(such as the EU Strategy against the Proliferation of Weapons of Mass Destruction).[286] The conventions prohibiting or limiting the use, development and possession of weapons of mass destruction impose obligations on individual states and describe the operating environment in which the threats arising from weapons of mass destruction exist. Under Recommendation 7 of FATF, member countries should implement targeted financial sanctions to comply with United Nations Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. In October 2020, FATF also adopted amendments on proliferation financing to Recommendations 1 and 2.

The supervisory and licencing authorities responsible for issues concerning weapons of mass destruction operate under the auspices of several government agencies. Disarmament and arms control matters are the responsibility of the Ministry for Foreign Affairs and the Ministry of Defence. Export controls and licencing of dual-use goods are the responsibility of the Ministry for Foreign Affairs. Export licences of civilian weapons are the responsibility of the National Police Board, while export licences for defence materiel are granted by the Ministry of Defence. In addition to the above authorities, Finnish Customs and the Finnish Security and Intelligence Service are also involved in the controls of export items.

Ensuring that the proliferation of weapons of mass destruction or exports of conventional weapons to countries subject to arms embargoes is not promoted from Finland, through Finland or using Finnish natural or legal persons is at the core of counter proliferation supervision by the Finnish Security and Intelligence Service. Close cooperation at the national and international level plays an important role in counter proliferation. According to the Mutual Evaluation Report on Finland prepared by FATF, there is a satisfactory level of cooperation and coordination in Finland in matters concerning the combating of proliferation financing.[287]

In addition to export controls, counter proliferation financing also involves the international sanctions referred to above. A variety of different methods are used to circumvent the sanctions, including offshore and joint ventures or third parties (foreign co-perpetrators) so that the role of the real actors or beneficiaries can be obliterated. Sanctions are also circumvented by smuggling cash and gold. There is also an urgent need to control virtual currencies because according to observations made by the UN they are used to circumvent sanctions. The methods used by parties promoting the proliferation

286 Ministry of the Interior 2017, p. 11.

287 FATF MER 2019, p. 6.

of weapons of mass destruction to circumvent sanctions also allow them to finance their activities.[288]

There is no concrete definition of proliferation financing and counter proliferation financing at the national level. Moreover, proliferation financing has not been criminalised. Moreover, national legislation poses challenges to such matters as reporting on suspected proliferation financing as there is no nationally specified reporting channel.

According to experts, technological advances may threaten to accelerate proliferation of weapons of mass destruction and proliferation financing as they have made products more easily available. Building weapons of mass destruction is easier and more actors have the capability to do it. Transferring expertise and knowhow across national boundaries are also seen as a threat as such activities are difficult to identify and supervise.[289]

Increasing awareness (especially among private sector actors) can also be seen as a factor preventing the proliferation of weapons of mass destruction and proliferation financing. The threat of proliferation of weapons of mass destruction and proliferation financing can also be reduced by increasing the awareness of dual-use goods and materials used in weapons of mass destruction among private sector actors.[290]

4.6 Other international phenomena

4.6.1 Professional football and match manipulation

Money laundering and terrorist financing risks associated with professional football were discussed in the 2019 supranational risk assessment of the EU for the first time. Football is the world's most popular sport and a global business with major economic impacts at the international level. According to the supranational risk assessment, professional football's complex organisation and lack of transparency have created a fertile ground for the use of illegal resources.[291] Leading Finnish experts in professional football were interviewed for the section on professional football so that an accurate risk picture of the sector could be produced.

288 United Nations Security Council (S/2020/151), pp. 5 and 62.

289 Interview with an expert.

290 Interview with an expert.

291 EU SNRA 2019, p. 4.

Veikkausliiga (Veikkaus league) is Finland's premier professional football division.[292] However, there are only between 250 and 350 professional players in Finland as many of the Veikkausliiga players are non-professionals. Ykkönen ('Number one') is the second-highest division of men's football in Finland. It is semi-professional and the Ykkönen clubs have an annual turnover of less than EUR 1 million. There are between 60 and 70 foreign players in Veikkausliiga and Ykkönen each year. Kakkonen ('Number two') is the third highest division of men's football in Finland. Local-level divisions are organised by districts of the Football Association of Finland.[293] The examination of money laundering and terrorist financing risk associated with football in Finland must include all divisions and not only the premium professional league. Lower (and less strictly supervised) divisions provide a fertile and lucrative operating environment for criminal activities, especially from the perspective of match manipulation and player contracts.[294]

The Council of Europe Convention on the Manipulation of Sports Competitions[295] was signed in 2014. The convention entered into force in autumn 2019 after it had been ratified by five EU Member States. Seven countries had ratified the convention by February 2021 and in all of them, it had also entered into force. Finland has signed but not yet ratified the convention.[296] The purpose of the convention is to prevent and identify manipulation of sports competitions and to improve exchange of information between actors.[297] Article 16 of the convention concerns laundering of the proceeds of criminal offences relating to the manipulation of sports competitions.

The following are some of the phenomena behind manipulation of sports competitions:[298] corruption, organised crime and growth in international betting markets.[299] According to an international survey conducted by FIFPro[300] in 2012, some 11.9 per cent of all professional football players had been approached by match manipulators. Some

292 The annual turnover of the clubs is EUR 1–4 million.

293 The summary is based on the website of the Football Association of Finland.

294 Interviews with experts.

295 Council of Europe Treaty Series - No. 215: Council of Europe Convention on the Manipulation of Sports Competitions.

296 As of 3 February 2021.

297 Especially in national-level and international cooperation between the authorities, sports organisations and betting companies.

298 Manipulation of sports competitions is a deliberate arrangement, activity or act of negligence aimed at influencing the end result of a sports competition or its course by eliminating, in full or in part, the unpredictability characteristic of sports competitions so that it will bring benefits to the perpetrator or others.

299 SUEK 2019, p. 4.

300 Fédération Internationale Des Associations de Footballeurs Professionels (FIFPro) is the international umbrella federation of football players' associations.

23.6 per cent of the respondents also said that there had been match manipulation in their own divisions. In fact, it has been estimated that 80 per cent of the manipulation of sports competitions takes place internationally in football.[301]

In betting-related manipulation of sports competitions, the aim is to achieve financial gains through betting, either directly or indirectly. Direct financial gains refer to cash winnings won in betting and indirect financial gains mean proceeds of money laundering.[302] Indirect financial gains describes a scenario in which the proceeds of crime are placed as bets on a specific match and using manipulation, efforts are made to influence the result in advance. Thus, money laundering can be seen as a motivation behind manipulation of sports competitions. At the same time, direct financial gains are criminal proceeds whose origin may be obliterated using different methods of money laundering.

Money laundering and terrorist financing risks associated with professional football and manipulation of sports competitions

The money laundering risks facing professional football are more significant than terrorism financing risks. For this reason, the issue is examined below from the perspective of money laundering.

There are differences between divisions in terms of risk levels. There is less supervision of match manipulation in **lower divisions**, which also means more potential for misconduct. Kakkonen is the lowest division in which matches are offered for betting by national gambling companies. Lower-division matches are only offered for betting by non-Finnish gambling companies.

It has also been noted that **applying provisions on bribery offences to match manipulation is problematic.**[303] Provisions on bribery offences (giving or accepting bribes in business) are currently applied to cases involving match manipulation. Applying the essential elements of bribery offences to match manipulation is seen as difficult because the essential elements do not include any of the characteristic features of match manipulation. It is also difficult to apply fraud provisions to match manipulation because the misled party may not be known.

301 SUEK 2019, p. 7.

302 SUEK 2019, p. 5.

303 The essential elements of the following types of offence listed in the Criminal Code might be applicable to match manipulation: petty fraud, fraud, aggravated fraud, money laundering, aggravated money laundering, giving of bribes in business, aggravated giving of bribes in business, acceptance of a bribe in business and aggravated acceptance of a bribe in business.

Football clubs in financial difficulties are seen as a significant risk.[304] Economic distress may make a club vulnerable to misconduct and small clubs are associated with a particularly high risk. The view is that the risk has also increased during the COVID-19 pandemic as national-level clubs find themselves in an increasingly difficult financial situation.

304 Example: sentence given by the Turku Court of Appeal (13/857).

Case involving a betting agent

The sentence for aggravated money laundering given by the Turku Court of Appeal in 2013 (13/857) concretised the links between money laundering and match manipulation. In the case in question, the managing director and the former board chair of a Finnish football club received sentences for illegal activities. At the time of the offence, the club was in financial difficulties and had accepted funds totalling more than EUR 300,000 from a foreign actor*. The money was paid partly in cash. The club used the money to pay its debts. In return for the fund transfer, the club had concluded a preliminary agreement on using foreign players but these plans never materialised. According to the court of appeal, using the funds to pay debts helped to conceal or obliterate the sources of the criminal proceeds. The court of appeal also stated that the sum offered and the acceptance of it without providing anything in return were already unusual. The cooperation agreement offered as part of the arrangement was also considered unusual. It was without precedent on the Finnish football scene and should have raised suspicions about the real reasons for the offer. The amount of money and acceptance of it were unusual considering the size of the cash payments. According to the court of appeal, the proceeds of crime were of extremely high value and the act is of aggravated nature when considered as a whole. The sentence is legally valid.

** The foreign actor had received a sentence in the Lapland District Court in 2011 for giving bribes in business after he was found to have manipulated match results of another Finnish club between 2008 and 2011.*

Team owners with foreign backgrounds have been identified as a risk in professional football in Finland and monitoring the assets of such owners and establishing their origin is difficult. Furthermore, identifying and determining the interests of foreign owners play a key role when identifying and assessing the money laundering risk even though there is no statutory obligation to identify the risks. This refers to determining why a foreign citizen would like to invest in the team in question. Even though the teams themselves are not obliged entities under the Anti-Money Laundering Act, the risk of a negligent money laundering offence exists. **Betting and betting-related arrangements and opportunities to influence match results** are also seen as a risk. International betting is a particularly high risk as international betting activities are not regulated or supervised at the national level. Thus, matches played in Finland can also be exploited in money laundering in other countries even though the activities do not fall within the scope of supervision and

the Anti-Money Laundering Act. **Sales of players and player contracts** have also been identified as a risk from the perspective of money laundering.

Technological development is seen as a current and emerging risk facing the activities. Using advanced technology, players can be given instructions and orders in real time. Moreover, technological advances and more cross-border activities make it easier to approach players and manipulate matches, while at the same time, contacts can be anonymous.

Direct and indirect links between **organised criminal groups** and match manipulation are seen as an existing or emerging risk. Players may be manipulated or threatened directly or indirectly to ensure the desired result. Organised criminal groups are also seen as a risk from the perspective of money laundering because international observations suggest that match manipulators use their activities to launder money.[305] It has been noted that international criminal groups are involved in the betting markets in three ways: 1) they pay bribes in order to manipulate matches; 2) they place bets on these results; and 3) they launder the proceeds of criminal activities.[306] It has also been noted that international criminal groups have arranged ghost games to launder money. These are matches that never take place as they are used as a cover for money laundering.[307]

4.6.2 Free ports

Free-trade zones are discussed in the supranational risk assessment and the focus in the document is on free ports. According to the country-specific list of free-trade zones prepared by the EU, Finland does not have any free-trade zones, or free ports meeting the criterion of the supranational risk assessment.[308]

4.6.3 Investor citizenship and residence schemes

Money laundering and terrorist financing risks associated with investor citizenship and residence schemes are discussed in the supranational risk assessment. Finland cannot grant citizenship or right of residence to investors or on the basis of investments and thus, these matters are outside the scope of the national risk assessment of money laundering

305 Interview with an expert.

306 Peurala, J. 2013. Match-manipulation in football – the challenges faced in Finland. International Sports Law J. 13, 268–286.

307 KCOOS 2017, p. 10.

308 EU SNRA 2019 - Commission Staff Working Document, p. 244.

and terrorist financing. Both investor citizenship schemes and investor residence schemes are discussed in the supranational risk assessment.[309]

Even though Finland does not grant the above-mentioned citizenship rights or rights of residence to investors or on the basis of investments, the provisions on the entrepreneur's residence permit contained in the Aliens Act were amended in 2018. In the amendment, a new criterion for a residence permit was added to the act. A residence permit can be granted to a foreign citizen that has established or intends to establish a start-up enterprise of any type in Finland. The amendment arises from the need to facilitate the immigration of entrepreneurs and top experts and to boost Finland's economic growth and employment prospects.[310] However, the residence permit is not granted solely on the basis of ownership as the person in question must work in the enterprise and perform the work in Finland.[311]

309 EU SNRA 2019 - Commission Staff Working Document, p. 250.

310 In the past, a foreign entrepreneur serving as the managing director of their limited liability company could not receive an entrepreneur's residence permit even though the person in question had been the sole shareholder of the company.

311 Government Proposal No. 129/2017, pp. 1, 21.

5 NPO sector

5.1 Abstract

The focus in the section of the national risk assessment of money laundering and terrorist financing discussing the NPO sector (non-profit organisations) is on the operating environment of the sector and the identification of the threats, vulnerabilities and risks facing the sector and assessment of their levels. There are good grounds for discussing the NPO sector separately in the risk assessment. The threats, vulnerabilities and risks facing the NPO sector are examined here from the perspective of money laundering and terrorist financing. In its Mutual Evaluation Report on Finland, FATF also urged Finland to take into account the risks facing the NPO sector.[312]

The NPO section was prepared during the early stages of the risk assessment process before the sections on money laundering and terrorist financing. A wide range of different authorities, supervisory bodies referred to in the Anti-Money Laundering Act, and NPOs of different sizes took part in the work. The work on NPOs started with an overview of the NPO sector, in which the main task was to produce a definition of an NPO for the national risk assessment and make the necessary specifications. The threats and vulnerabilities facing the NPO sector were reviewed in a one-day workshop attended by experts[313] and in interviews with sectoral actors and experts. A survey was also carried out among NPOs.[314]

Key observations of Finland's NPO sector:

- The Finnish NPO sector is fairly large; there are about 100,000 associations entered in the Finnish Register of Associations. In addition, there are about 2,700 foundations entered in the Finnish Register of Foundations.[315]
- The definition of an NPO contained in the national risk assessment emphasises the non-profit nature of the actors and the fact that NPOs receive and/or use or relay funds or other economic support for specific non-profit purposes.

Key observations of the threats, vulnerabilities and risks related to the national NPO sector:

312 FATF MER 2019, p. 38.

313 The experts comprised public authorities and supervisory bodies referred to in the Anti- Money Laundering Act.

314 See section 5.4.2 for more details of the survey conducted among NPOs.

315 The figures are based on the situation on 1 January 2020.

- Cross-border activities of the NPOs and infiltration of criminal actors into legal activities are seen as the most significant threats facing the NPO sector.
- The following factors are seen as the key vulnerabilities facing the NPO sector: fragmented nature of the official supervision, insufficient transparency of NPO activities and deficiencies affecting the internal processes of NPOs.
- The following factors are seen as the key risks facing the NPO sector: activities of small NPOs,[316] exploitation of legal NPO activities for criminal purposes, transport of cash to crisis countries and the fact that NPOs do not conduct adequately critical self-evaluations of their own activities.

Figure 4. Levels of threats, vulnerabilities and overall risk facing the NPO sector.

The levels of threats and vulnerabilities facing NPOs and the overall risk arising from them are based on expert estimates. The experts placed the threats and vulnerabilities on a scale of 1 to 4 (less significant – very significant) and the overall level of threats and vulnerabilities is based on their average. The risk level is based on a combination of threats and vulnerabilities in which threats had a weight of 40 per cent and vulnerabilities 60 per cent. The overall risk facing the NPO sector is at level three (**significant**).

316 A small NPO is not defined in the national risk assessment. An organisation with modest turnover or with less than ten persons on its payroll can be considered a small NPO. The minimum size of an association obliged to conduct audits can also be used as the definition of a small NPO (see section 1.6.1 'Identified terrorist financing vulnerabilities facing the NPO sector').

5.2 NPO risk assessment

5.2.1 Purpose and background of the risk assessment

The purpose of the NPO section of the risk assessment is to examine Finland's NPO operating environment and identify and assess the threats, vulnerabilities and risks associated with the NPO sector. This is the first large-scale[317] survey of the money laundering and terrorist financing risks facing the Finnish NPO sector.

In addition to the recommendations issued by FATF, the supranational risk assessment of the EU also recommends the preparation of national NPO reports so that the typical features and risks of NPOs can be identified in the context of money laundering and terrorist financing. According to the 2017 supranational risk assessment, NPOs are one of the sectors to which particular attention should be paid in national risk assessments.[318] This recommendation was repeated in the 2019 supranational risk assessment in respect of both risk identification and risk management measures.[319] In the FATF context, the call for possessing adequate knowledge of the NPO sector is connected with Recommendation 8, in which the member countries are required to review the NPO sector in general and take measures to identify the risks associated with the sector.[320]

Both the EU-level requirements and FATF recommendations concerning adequate knowledge of the NPO sector and risk assessment are in many respects similar. However, there are slight differences between them in terms of priorities. For FATF, the focus is on NPOs vulnerable to terrorist financing abuse[321] whereas in the supranational risk assessment consideration is given to the risks in the NPOs' field of operations in terms of money laundering and terrorist financing. However, it is stated in the supranational risk assessment that a separate assessment of threats and vulnerabilities associated with money laundering in the NPO sector would not be useful as these issues can be examined in the context of the threats and vulnerabilities associated with terrorist financing.[322] In this NPO section, the potential of NPOs to be associated with both contexts is recognised but in accordance with the example of FATF, the priority is on the assessment of the threats and vulnerabilities related to terrorist financing.

317 The topic has already been discussed in the report 'Terrorismin rahoitus ja yleishyödylliset yhteisöt' (Terrorist financing and non-profit organisations) published in 2009.

318 EU SNRA 2017, p. 16.

319 EU SNRA 2019, p. 14.

320 FATF 2019, p. 43.

321 FATF 2019, p. 43.

322 EU SNRA 2019 - Commission Staff Working Document, pp. 228 and 231.

The need for a separate NPO section can be justified with the general requirements concerning the NPO sector issued by FATF and the EU, and the observations made by FATF in its Mutual Evaluation Report on Finland. According to the Mutual Evaluation Report, the threats facing the NPO sector and the terrorist financing risks associated with them have until now been inadequately identified in Finland, which also impacts risk-based supervision and monitoring.[323] The observations contained in the Mutual Evaluation Report concerning the national-level understanding of the risks facing NPOs have guided the preparation of the NPO section of the national risk assessment.

5.2.2 Scope of the NPO risk assessment

The NPO sector is extensive and diverse and for this reason, it has been necessary to limit the scope of the review to ensure proper assessment of the risks facing NPOs.

This assessment of the risks facing Finland's NPO sector is limited to registered actors so that the qualitative and quantitative data can be combined in a reliable manner. Thus, the NPOs reviewed in this assessment have a legal form that can be verified from registers. This also means that non-registered actors (such as non-registered associations) are outside the scope of the assessment. The absence of quantitative data on non-registered actors is problematic from the perspective of analysis, and in this risk assessment, solely relying on qualitative data is not seen as an appropriate approach to assessing threats and vulnerabilities. Limiting the assessment to registered actors is also seen as justified because this is the first extensive assessment of the risks facing the Finnish NPO sector. However, future reviews should also include non-registered NPOs so that information about the money laundering and terrorist financing risks facing such actors can be obtained. The purpose of this first extensive review of the NPO sector is to provide a basis for a more detailed examination of the sector, which in the future could be supplemented with quantitative and qualitative data on non-registered actors.

The section on NPOs examines potential threats and vulnerabilities associated with money collection and NPOs engaged in humanitarian aid and development cooperation.[324] In addition to the non-profit nature of the activities, fundraising is, already on the basis of the FATF definition, the second essential feature common to NPOs. This means that limiting the review to actors meeting these requirements is justified. At the same time, parties engaged in humanitarian aid and development cooperation are, already on account of the nature of their activities, potential victims of exploitation from the perspective of terrorist financing.

323 FATF MER 2019, p. 174.

324 The same applies to the general grants given to non-governmental organisations for activities associated with Finland's foreign and security policy and international commitments.

This is because aid organisations often operate in conflict zones or in regions where terrorist organisations are also present[325] and in regions with an inadequate AML/CFT framework.

5.3 Definition of an NPO

5.3.1 Definition of an NPO in international context

FATF defines an NPO as follows:

> *'A legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works.'*[326]

The purpose of raising and using funds and the non-profit nature of the activities are clearly identifiable from the FATF definition as key elements of an NPO. The FATF definition is functional, which means that it arises from the activities and typical features of NPOs that can make the actors in question vulnerable to the risk of terrorist financing. In such cases, the non-profit nature of an NPO should not be the determining factor.[327] In the FATF definition of an NPO, the emphasis on functionality can be considered as providing flexibility in the creation of a national definition for an NPO. This is because when national NPOs are examined, the nature of their activities should be taken into account. For this reason, it is not practicable that the national definition of an NPO should be identical with that presented by FATF.[328]

The terminological definition of an NPO contained in the supranational risk assessment is also based on the FATF definition.[329] Recommendation 8 of FATF only covers NPOs providing services (service NPOs), whereas in the supranational risk assessment, consideration is also given to NPOs engaged in expressive and other leisure time activities (expressive NPOs).[330] In accordance with the supranational risk assessment, Finland's own national risk assessment considers both categories of NPOs. According to FATF, identifying and understanding the typical features of the NPO field of activities is an essential prerequisite for understanding the risks associated with the NPO sector.[331] However,

325 EU SNRA 2019 - Commission Staff Working Document, p. 226.
326 FATF 2019, p. 43.
327 FATF 2019, p. 43.
328 FATF 2019, pp. 44-45.
329 EU SNRA 2019 - Commission Staff Working Document, p. 225.
330 EU SNRA 2019, p. 4.
331 FATF 2019, p. 44.

the view in Finland has been that creating a national definition for an NPO for the risk assessment context should be the starting point of the national risk assessment work. This is the best way to identify the NPOs with the highest risks nationally and to focus measures set out in the action plan in an effective manner.

5.3.2 Definition of an NPO in the national risk assessment

The definition of an NPO used in the national risk assessment is based on the FATF definition and consideration was also given to the conclusions on the FATF's NPO definition contained in the supranational risk assessment, results of the NPO survey conducted among the national risk assessment working group, comments presented in the national risk assessment working group and the observations made in the NPO workshop. In the national risk assessment, an NPO is defined as follows:

> *'NPOs are legal persons, groups and groupings that primarily operate on a non-profit basis. An actor engaged in profit-driven activities may also be an NPO if the activities are partially on a non-profit basis. An NPO raises, receives and/or uses or relays funds or other economic support for charitable, religious, educational, social, fraternal or ideological purposes or for other types of charity, or for sports, leisure-related, artistic, cultural or advocacy activities. Most of the NPOs operate as non-profit associations, foundations, federations, political parties or other organisations.'*

A wide range of different terms is used to describe Finland's NPO sector: in addition to the term 'non-profit activities', the words 'third sector',[332] 'civil society', 'non-governmental organisations' and 'voluntary civic activities'[333] are also used. Some of the NPO activities can be examined from the perspective of 'common good', in which the emphasis is on the legal aspect.[334] *Common-good activities* are activities pursued for general social, cultural, educational or ideological purposes, or other general non-governmental activities, such as those referred to in section 2 of the Money Collection Act.

The concept 'common good' has also been defined for taxation purposes, but this definition differs from the definition used in the Money Collection Act. Under section 22 of the Income Tax Act, *a common-good organisation is an organisation that* exclusively and directly acts for common good in material, non-material, ethical or societal sense. Its activities are not limited to any specific group of individuals and it does not generate

332 Virén 2014, p. 9.

333 University of Jyväskylä, Kansalaisyhteiskunnan tutkimusportaali: Kolmas sektori [*The assistance system for victims of human trafficking*] , referred to on 24 July 2020.

334 Virén 2014, p. 9.

financial benefits to the parties involved. The definition of common good used for taxation purposes is not intended for use in a wider context.

5.4 Finland's NPO sector and its operating environment

5.4.1 Administrative environment and national regulation

Under section 13 of the Constitution of Finland, everyone has the freedom of association. Freedom of association entails the right to form an association without a permit, to be a member or not to be a member of an association and to participate in the activities of an association.

The Associations Act (503/1989) applies to **associations**. All associations established to promote non-profit purposes fall within the scope of the act. A registered association may be granted rights, it may enter into commitments and it may be party to legal proceedings. The Associations Act also applies to non-registered associations that are outside the scope of the NPO sector discussed in this section. Non-registered associations may not be granted rights, enter into commitments or act as defendants or injured parties in legal proceedings.

In addition to associations, **foundations** are also an important group of registered NPOs. Under the Foundations Act (487/2015), foundations must have a purpose serving the common good and to support or engage in activities promoting this purpose. The Finnish Patent and Registration Office maintains a Register of Associations and a Register of Foundations. The Finnish Patent and Registration Office also acts as the authority supervising foundations as it is tasked with ensuring that foundations comply with the Foundations Act and their own rules. The supervision is carried out retroactively on the basis of the annual reports submitted by the foundations.

NPOs also **include religious communities**, and provisions of them are contained in the Act on the Freedom of Religion (453/2003). For the purposes of the act, a religious community means the Evangelical Lutheran Church of Finland, the Orthodox Church of Finland and any religious community registered in the manner provided in chapter 2 of the act. The Finnish Patent and Registration Office maintains the Register of Religious Communities; however, the Evangelical Lutheran Church of Finland, the Orthodox Church of Finland and their parishes are not entered in the register.

The provisions on beneficial owners contained in chapter 6 of the Anti-Money Laundering Act also apply to associations, religious communities and foundations operating in the NPO sector. Under the Anti-Money Laundering Act, an association entered in the Register

of Associations, a religious community entered in the Register of Religious Communities and a foundation entered in the Register of Foundations must appropriately obtain and maintain accurate and up-to-date details of their beneficial owners. However, the registration obligation concerning the beneficial owners of the above-mentioned parties differs substantially from the obligations of companies. Associations, foundations or religious communities do not have to separately enter the details of their beneficial owners in the Trade Register. This is because under the Associations Act, Foundations Act and the Act on the Freedom of Religion, the following parties are considered beneficial owners of such actors: board members entered in the Register of Associations, Register of Foundations or the Register of Religious Communities and for foundations also the members of the board of trustees.

The key authorities pertaining to the NPO sector act in a variety of different roles, such as the supervision and registration of NPOs, legislative work, supervision of money collection and taxation, and in the carrying out of activities concerning humanitarian aid, development cooperation and other areas of foreign and security policy.

Table 9. Key national actors and their tasks from the perspective of the NPO sector.

Actor	Key tasks
Finnish Patent and Registration Office	Maintains the Register of Associations Maintains the Register of Foundations Maintains the Register of Religious Communities Supervises compliance with the Foundations Act and the rules of the foundations
National Police Board/Gambling Administration	Grants money collection licences Supervises money collection activities Grants raffle and bingo licences Supervises licensed lotteries in all parts of Finland
Police departments	Receive notifications of small-scale money collections Grant raffle licences Supervise lotteries held in their areas
Ministry for Foreign Affairs	Funds projects and programmes in developing countries Decides on granting assistance for development cooperation and humanitarian aid activities and on funding concerning non-governmental activities pertaining to other areas of Finland's foreign and security policy and international commitments Supervises the use of the funds and monitors and assesses the projects and their results
Ministry of Justice	Is responsible for enacting legislation on associations and foundations
Ministry of the Interior	Is responsible for enacting money collection legislation Is responsible for lotteries legislation
Finnish Tax Administration	Taxes common-good associations

5.4.1.1 Money collection activities

Money collection does not explicitly fall within the scope of the Anti-Money Laundering Act. However, the Money Collection Act contains provisions the main purpose of which is to prevent misuse and criminal activities. As money collection is an important fundraising method for NPOs,[335] it is appropriate to include money collection activities in the assessment of money laundering and terrorist financing risks.

335 National Police Board/Gambling Administration: Money collection and the prevention and investigation of money laundering and terrorist financing, referred to on 2 July 2020.

The new Money Collection Act (836/2019) entered into force on 1 March 2020. Despite the entry into force of the new act, money collection licences granted under the old (now repealed) Money Collection Act (255/2006) are still in effect and these licences remain in effect for a maximum of five years. Under the new Money Collection Act, a money collection usually requires a licence granted by the National Police Board. A money collection may only be arranged to raise funds for non-profit activities. Before the licence for such activities is granted, such matters as the purpose of the applicant's activities and the use of the collected funds for non-profit purposes are examined. The money collection licence granted under the new act is in effect until further notice.

Small-scale money collections may also be arranged under the new Money Collection Act. No licence is required for a small-scale money collection; the organisers only need to submit a notification to a police department. A maximum of EUR 10,000 may be collected by means of a small-scale money collection. The organiser of a small-scale money collection must monitor the amount of funds raised and if necessary, stop the collection. The main difference between money collections and small-scale money collections is that when money is collected on a small scale, the organiser does not need to be a non-profit actor and common good does not need to be the purpose of the collection. Despite this, a small-scale money collection may not be arranged to support business activities.[336] Moreover, a small-scale money collection may be arranged by a non-registered group of at least three natural persons. At least one of the persons must be legally competent and all others must be at least 15 years of age, and all must be domiciled in Finland as referred to in the Act on Municipal Domicile (201/1994).

The National Police Board and police departments maintain a money collection register so that they can carry out the tasks laid down in the Money Collection Act. Money collection activities are supervised both proactively and retroactively, with focus being on retroactive supervision.

5.4.1.2 Humanitarian aid and development cooperation

Finnish organisations engaged in aid activities receive funding from a variety of different sources (from the government, church organisations, private donors and companies). The organisations receive most of their funding from the development cooperation appropriations of the Ministry for Foreign Affairs, for which a total of EUR 1,032 million was budgeted in 2020. Development cooperation and humanitarian aid administered by the Ministry for Foreign Affairs accounted for EUR 675 million of this sum.[337] For the NPO risk

336 Government Proposal No. 214/2018, p. 51.

337 Ministry for Foreign Affairs: Development cooperation appropriations and statistics, referred to on 22 July 2020.

assessment, it is particularly important to examine the role of national aid organisations providing humanitarian assistance and engaged in development cooperation from the perspective of the prevention of money laundering and terrorist financing.

The humanitarian aid provided by Finland is based on international humanitarian law, human rights conventions, refugee law and the humanitarian principles adopted by the United Nations. The aid is given on a discretionary basis and it is intended to save human lives and alleviate human suffering in humanitarian crisis situations.[338] In 2019, Finland provided EUR 78.7 million in humanitarian aid and EUR 9.1 million of this total was channelled to Finnish non-governmental organisations.[339] Humanitarian funding can only be granted to Finnish organisations that meet the criteria set by the European Commission's Directorate-General for Civil Protection and Humanitarian Aid Operations (Echo). These include professional general and financial administration and adequate mechanisms to ensure legality and regular nature of the activities. There are currently seven organisations meeting the criteria. Finland does not grant humanitarian funding to non-governmental organisations.

Development cooperation means government-level cooperation with developing countries and other partners to achieve specific goals aimed at developing the partner country. Development cooperation is founded on such documents as the Paris Agreement and the 2030 Agenda of the United Nations. The main goal of development cooperation is to eradicate poverty and reduce inequality.[340] In 2019, a total of EUR 65 million was granted to Finnish non-governmental organisations and foundations for development cooperation. Multi-year programme support intended for long-term development cooperation is one form of the support and a total 19 non-governmental actors in Finland have received this type of support. The Ministry for Foreign Affairs may grant project-specific support to small organisations.[341] The Political Department of the Ministry for Foreign Affairs coordinates the application rounds, in which non-governmental organisations receive general grants for activities that are connected with the principles of Finland's foreign and security policy and its international commitments, and with the area of responsibility of the Ministry for Foreign Affairs in general.

The Act on Discretionary Government Transfers (688/2001) is applied to the project grants for humanitarian aid and development cooperation provided by the Ministry for Foreign

338 Ministry for Foreign Affairs 2019a, p. 11.

339 Ministry for Foreign Affairs: Humanitarian aid provided by Finland in 2019, referred to on 22 July 2020.

340 Ministry for Foreign Affairs: Humanitarian aid provided by Finland in 2019, referred to on 22 July 2020. Ministry for Foreign Affairs: Goals and principles of Finland's development policy, referred to on 22 July 2020.

341 Ministry for Foreign Affairs: Civil society is an important actor and development cooperation partner, referred to on 23 July 2020.

Affairs. The act contains provisions on the use and supervision of the money and on return and recovery of the grants. The parties responsible for the projects must report misuse or suspected misuse of the funds to the Ministry for Foreign Affairs. Private persons may also report on suspected misuse of development cooperation funds.[342] Misused funds are recovered and the suspicions are also reported to the National Audit Office of Finland and, if necessary, to the police. Between 20 and 25 suspected cases of misuse are reported to the Ministry for Foreign Affairs each year and most of them involve human errors or the suspicions are otherwise unfounded. A total of EUR 70,687 was recovered in 2019.[343]

5.4.2 Registered NPOs in Finland

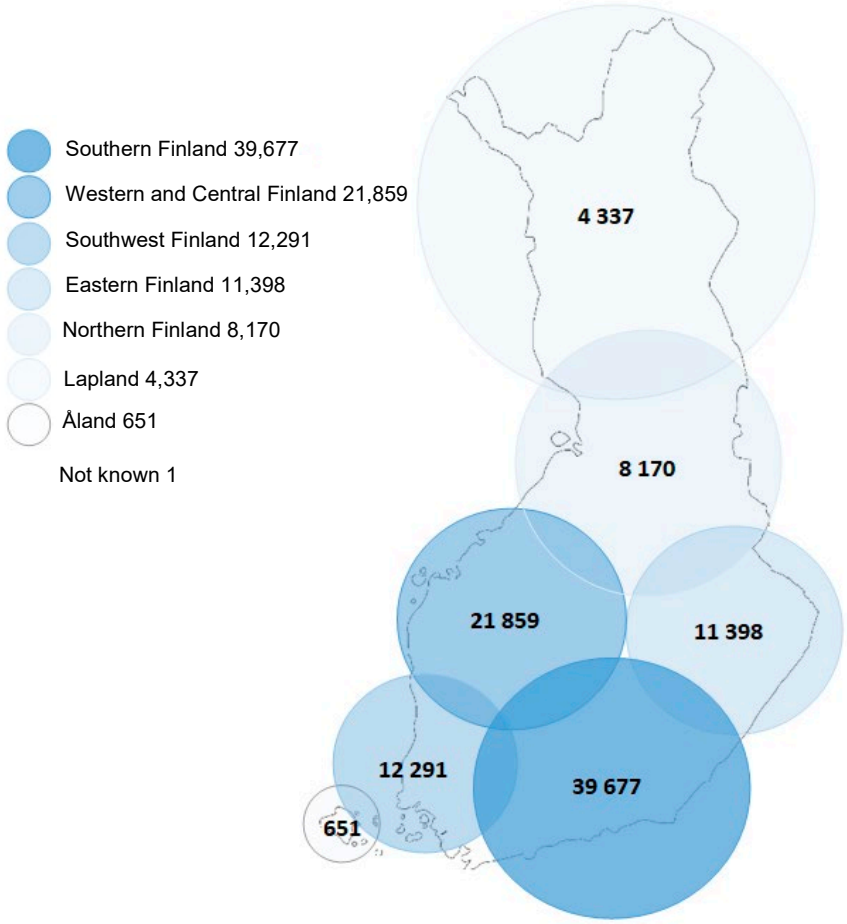
According to the Register of Associations, there were a total of 98,384 active associations in Finland at the start of 2020. Most of them (97,880) were associations with basic structure. The operating sectors of the associations cover a wide range of different fields, from expressive and leisure-time activities to provision of services. At the start of 2020, there were a total of 145 religious communities, 339 congregations and 20 chambers of commerce in Finland. According to the Register of Foundations, Finland had a total of 2,699 active foundations at the start of 2020.[344]

342 Ministry for Foreign Affairs: Report suspected misuse of funds, referred to on 20 October 2020.

343 Ministry for Foreign Affairs: Misuse is addressed, referred to on 23 July 2020 and 17 March 2021. See also Ministry for Foreign Affairs 2019b, p. 45: There were a total of 17 cases of misuse or suspected misuse in the Foreign Affairs Administration in 2019. Seven of the cases involved bilateral development cooperation managed by the Foreign Affairs Administration, seven cases were detected in cooperation involving non-governmental organisations, one case involved unallocated development cooperation funds and two cases involved humanitarian aid. The abovementioned cases have prompted the Ministry for Foreign Affairs to submit reports on misuse in the host country to competent investigation authorities. The ministry has also used different types of administrative procedure in the cases. A number of cases mentioned in the previous year's annual report are still under investigation.

344 The figures are based on the situation on 1 January 2020.

Figure 5. Chambers of commerce, congregations, religious communities and associations, by region, at the start of 2020.



As a rule, associations entered in the Register of Associations are not required to submit details of their operational finances. Certain types of special association falling within the scope of special legislation (such as political parties) are an exception to this rule.[345] Certain associations exceeding specific turnover, balance sheet and personnel limits must also submit their financial statements to the Finnish Patent and Registration Office. Foundations must include their financial statements, report on operations and the auditor's report in the annual report that they submit to the Finnish Patent and Registration Office.[346]

345 Virén 2014, p. 10.

346 Finnish Patent and Registration Office: Foundations – annual report, referred to on 24 July 2020.

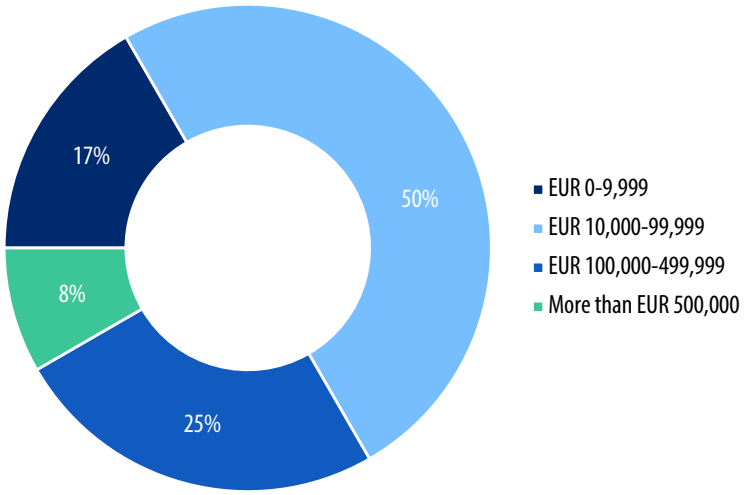
Survey conducted among NPOs

A survey was carried out among NPOs registered in Finland in July 2020. In the survey, the actors were asked questions about their operating environment, and their awareness of money laundering and terrorist financing risks. The questionnaire was sent to a total of 100 actors on the basis of random sampling and the response rate was 17 per cent. At the general level, the respondents' awareness of money laundering and terrorist financing risks was low and none of the actors described high-risk operating models associated with their sector. It should be noted, however, that the sample was extremely small in relation to the total number of associations in Finland.

Religious activities, development cooperation, animal rights work, sports, supervision of members' interests and child and youth work were given as the main types of activity of the NPOs participating in the survey. Nearly all respondents gave registered association as the legal form of their organisation.

Half of the respondents stated that their annual turnover is less than EUR 100,000. Annual turnover figures ranged between less than EUR 10,000 and several million euros. A total of 44 per cent of the associations stated that their activities involve transfer of funds to foreign countries.

Figure 6. Annual turnover of the organisations participating in the NPO survey.



Most of the organisations participating in the survey were located in the Uusimaa region. Most of the organisations were engaged in nationwide or regional activities in Finland, two organisations had European-wide activities and three were global organisations or engaged in activities outside Europe. The organisations with foreign activities added that they also operate in Finland.

The organisations were also asked to give the registers to which they submit information. Many of them stated that they give information to the Finnish Tax Administration,[347] the police, Finnish Patent and Registration Office, and bank and insurance sector actors. Other actors included the Regional State Administrative Agency and the Finnish Food Authority. A small number of organisations replied that they do not submit information to any registers.

5.5 Money laundering and terrorist financing threats facing the NPO sector

In an analysis based on expert assessments, it was determined that the overall threat of money laundering and terrorist financing facing the Finnish NPO sector is at level three (**significant**).

5.5.1 Terrorist funding threats facing the NPO sector

The most significant money laundering and terrorist financing threats are highlighted in this national risk assessment in the manner set out in Recommendation 8 of FATF. The overall threats facing the Finnish NPO sector are as follows:

- Cross-border activities of NPOs
- Terrorist groups
- New technologies
- New payment methods
- Transfer of funds to countries of destination through unofficial channels
- Use of cash

347 Information that is necessary for taxation purposes is submitted to the Finnish Tax Administration. Thus, associations do not necessarily provide the Finnish Tax Administration with other information about their activities and the agency does not collect register data that is irrelevant to taxation purposes.

Geographical factors are one of the most significant threats facing NPOs. In cross-border activities, it is difficult to verify the purpose of the funds, or it may be impossible to determine the sources of funds originating from outside Finland. Activities in or cooperation with countries that have a particularly inadequate anti-money laundering and/or terrorist financing legislation are also considered a threat. Cooperation with parties in conflict zones is also seen as a threat.

From the perspective of terrorist financing, terrorist groups are a particularly serious threat to NPOs in both Finland and internationally. Members of terrorist groups may infiltrate NPOs or NPOs may be victims of thefts or misuse perpetrated by terrorist groups in conflict zones. It is also stated in the supranational risk assessment that infiltration of existing NPOs is a more significant risk than new NPOs established by terrorists.[348]

New technologies and payment methods are also seen as a significant threat to the NPO sector. New FinTech actors, payment gateway providers, payment service providers and providers of virtual currencies are examples of the latest money transfer and money remittance services. Technological advances pose challenges to NPOs and the authorities. However, the impact of technological development on NPO-associated threats works both ways. This is because even though crowdfunding[349] or blockchains[350] can be misused in NPO activities, such technologies can also be used to improve the traceability of the funds.[351]

Transferring funds using means other than reliable and easily traceable bank connections is seen as a threat in terms of money laundering and terrorist financing. Hawalas[352] are one channel used to make unofficial cross-border money transfers. Money transfers through unofficial channels or using cash are making it increasingly problematic to verify money laundering and terrorist financing. This is because the funds are difficult to trace. The impact of unofficial fund transfer channels on the risk faced by NPOs is also recognised

348 EU SNRA 2017 - Commission Staff Working Document, p. 186.

349 Money for projects launched by individuals or organisations and for business activities can be collected through crowdfunding. The money is usually collected in small sums from a large number of people to meet the funding target. Crowdfunding is carried out using crowdfunding platforms or websites specialising in different types of fundraising. Crowdfunding can also be used to obtain donations or to pursue sales activities. Crowdfunding-based donations are used as a fundraising method by common-good organisations and foundations, and they require a money collection licence. See National Police Board/Gambling Administration: Crowdfunding and money collection, referred to on 16 October 2020

350 A blockchain is a technology that enhances trust between its users. It allows the sharing of online information and agreement on transactions between users and recording of them in a verifiable, secure and irreversible manner. At the same time, a blockchain is also a protocol (communication procedure) defining the methods and rules used in the communication. See European Commission: Blockchain Technologies and European Economic and Social Committee (2019/C 353/01), referred to on 16 October 2020

351 EU SNRA 2019 - Commission Staff Working Document, p. 228.

352 In the definition of hawala, see 'Providers of payment services, including currency exchange and hawala systems'.

in the supranational risk assessment. It is concluded in the supranational risk assessment that the refusal of banks to make services available to NPOs is a key reason why unofficial systems are becoming more popular.[353]

5.5.1.1 Threats related to terrorist financing in money collection activities

In money collection activities, the threat of terrorist financing is considered more significant than in the NPO sector as a whole. The following are seen as the most significant threats associated with money collection activities:

- Arranging illegal money collections
- Arranging small-scale money collections
- Exploitation of legal money collection events
- Small NPOs as organisers of money collection activities

Arranging an illegal money collection using such platforms as social media without a money collection licence or a small-scale money collection notification is seen by experts as a significant threat in terms of money laundering and terrorist financing. According to the supranational risk assessment, existing NPOs can be used in situations involving the misuse of money collections or an NPO may be established for the purpose.[354] Small-scale money collections are also seen as a high-threat activity nationally as they only require a notification, which means that the funds may in reality be collected within a small inner circle. The upper limit of EUR 10,000 applied to small-scale money collections must be considered a substantial sum in terms of terrorist financing.

There is potential for misuse in legal money collections because over the past four years, between about 400 and more 700 money collection licences have been granted annually. Since the entry into force of the new Money Collection Act, a total of 383 small-scale money collection notifications have been submitted during a period of four months.

Social media and small-scale money collection notifications make it easier for small and non-organised NPOs to collect funds. These may involve situations in which low-threshold collections are arranged to raise funds for good causes in social media. However, there may only be a single person behind the collection and this individual channels the funds to a specific party, which is not the party mentioned in connection with the money collection. The case of the toy smuggler discussed in section 5.5.2 is an example

353 EU SNRA 2019 - Commission Staff Working Document, pp. 227-228.

354 EU SNRA 2019 - Commission Staff Working Document, p. 226.

of such activities. Vagueness of responsibilities within NPOs is a typical feature of such unorganised activities, which makes the actors involved more vulnerable.

5.5.1.2 Threats associated with terrorist financing faced by actors providing humanitarian aid and engaged in development cooperation

Based on an overall assessment, the threat of terrorist financing faced by actors providing humanitarian aid and engaged in development cooperation is seen as less significant than the threats facing the NPO sector as a whole. Actors granted public funding are not specified in the threat assessment. However, according to the supranational risk assessment of the European Union, the threats of terrorist financing faced by such actors are also seen as less significant.[355] The following are seen as the threats faced by actors providing humanitarian aid and engaged in development cooperation:

- Recruited persons in charity organisations in countries of destination or in associations in countries of origin
- Channelling funds as aid to conflict zones or other high-risk regions
- Complexity of the criminal methods generating threats

Individuals recruited in charity organisations constitute a threat to NPOs when the local partner in the country of destination has not been adequately identified. The supranational risk assessment also highlights the exploitation of legal NPOs from within.[356] The size of the NPO also matters in this respect. This is because monitoring of the partners is easier in the largest international charity organisations than in small operators.

In the case of NPOs providing humanitarian aid and engaging in development cooperation and acting to meet the international commitments based on Finland's foreign and security policy, the international dimension gives rise to a potential threat. The aid is mainly channelled to foreign countries, which means that the transfer of funds may also be by means of complex arrangements. Ensuring that the funds go to the right recipients, identifying the fund end users and verifying the required documents may be extremely difficult from Finland.

Even though the most serious threats facing NPOs are associated with the raising and use of funds, there are also other methods generating threats. Instead of funds, material aid intended for humanitarian purposes may fall into terrorists' hands and it can then be used for terrorist activities or converted into funds to finance terrorism. For NPOs providing

355 EU SNRA 2019 – Commission Staff Working Document, p. 228.

356 EU SNRA 2019 - Commission Staff Working Document, pp. 226-227.

humanitarian aid and engaged in development cooperation, the threat may materialise because aid organisations also supply items that terrorist groups may use in their activities. However, a distinction should be made between actors providing humanitarian aid and actors engaged in development cooperation because the activities are different in nature. The purpose of humanitarian aid is to save human lives and alleviate human suffering and thus the threat faced by actors carrying out such work is less significant. At the same time, due to the nature of the activities, the threat may be more concrete in development cooperation.

5.5.2 Money laundering risks faced by the NPO sector

In Recommendation 8 of FATF, the threats facing the NPO sector are examined from the perspective of terrorist financing.[357] The supranational risk assessment also recognises the money laundering threats facing NPOs but it is not considered necessary to assess them separately from terrorist financing threats.[358] Terrorist financing is also the focus area in the national expert assessments of the threats faced by NPOs. However, they also highlight organised criminal groups, members of organised criminal groups, supporting members and other related parties as a money laundering threat to NPOs.

The sentence given by the Helsinki Court of Appeal on 29 May 2020[359] in the case of the 'toy smuggler'[360] is an example of money laundering carried out as part of NPO activities.

357 FATF 2019, p. 43.

358 EU SNRA 2019 - Commission Staff Working Document, p. 228.

359 Sentence of the Court of Appeal of Helsinki, 29 May 2020 No. 20/118778. The legal validity of the sentence was checked on 4 January 2021; the district prosecutor has applied for a leave to appeal in the case.

360 No state funding was granted for the activities in this case.

Case of the toy smuggler

The case involved an illegal money collection carried out in the name of an or- ganisation engaged in charity work in Syria. The funds were used and converted in a manner that had essential elements of aggravated money laundering. The sentenced individual, the real actor in the organisation, was considered guilty of a money collection offence committed as a money laundering predicate offence. He had collected funds without a proper money collection licence and provided the licence authorities with false information. The person in question had used funds obtained by means of the money collection offence to purchase a cottage in an allotment garden. The Court of Appeal stated that by purchasing the cottage, the person in question had made himself guilty of aggravated money laundering notwithstanding the provisions on self-laundering. The sentence is not yet legally valid.

5.6 Money laundering and terrorist financing vulnerabilities faced by the NPO sector

According to an analysis based on expert assessments, the overall vulnerability of the NPO sector to money laundering and terrorist financing is at level three (**significant**).[361]

5.6.1 Terrorist financing vulnerabilities faced by the NPO sector

The most significant money laundering and terrorist financing vulnerabilities are highlighted in this national risk assessment in the manner set out in Recommendation 8 of FATF. In general, the following factors have been identified as vulnerabilities facing the NPO sector:

- Challenges arising from the exchange of information
- Concrete high-risk actors have not been adequately identified
- Deficiencies in NPOs' internal audit processes
- Deficiencies concerning the reporting obligation
- Fragmented supervision and lack of powers

361 According to the supranational risk assessment, the vulnerabilities of NPOs engaged in the collecting and transfer of funds to terrorist financing are at level two (moderately significant). (EU SNRA 2019 - Commission Staff Working Document, p. 231.)

- Lack of transparency in the activities
- Legislative deficiencies
- Uneven capacity of the actors to detect unusual transactions of NPOs
- Blind spots in inter-authority cooperation

The challenges arising from information sharing mainly impact cross-border activities. Obtaining information from other countries may be a slow process or even impossible or information may only be provided on a sector-specific basis. There may also be gaps in inter-authority cooperation and exchange of information at national level because many NPOs fall within the purview of more than one government agency. This makes it more difficult to produce a unified overall picture. Cooperation between the authorities and their ability to react to any misuse are also hampered by lack of knowledge about NPOs' operating models. This in turn makes it more difficult to focus resources on such matters as supervision. The experts' view thus reaffirms the views presented in the Mutual Evaluation Report that there are inadequacies in Finland's ability to identify risks associated with the NPO sector.[362]

Moreover, national NPOs have not adequately identified high-risk actors in their own activities, which are significantly affected by the inadequacy of the actors' own compliance procedures. NPOs lack the ability to identify the highest-risk actors in their own sectors and the operating models used by them. As a result, NPOs are incapable of applying correctly proportioned preventive measures. In the survey conducted among NPOs, most of the participants also admitted that they are unfamiliar with the risks related to money laundering and terrorist financing. It should be noted, however, that many of the large NPOs participating in the survey are working to improve their internal audit processes and enhance transparency, which in the future will probably prompt NPOs to take a more realistic view of the misuse threatening and affecting their activities. Similar observations about the NPO sector as a whole were also made in the supranational risk assessment of the EU.[363]

The vulnerability concerning deficiencies in the reporting obligation means that the reporting and due care obligation referred to in the Anti-Money Laundering Act does not apply to NPOs. In addition, many of the actors do not fall within the scope of any other reporting obligation either.[364] To this can be added the vulnerabilities concerning supervision-related challenges and lack of transparency. Supervision of NPOs is mostly on a fragmented basis as the authorities only supervise foundations, actors meeting the

362 FATF MER 2019, p. 83.

363 EU SNRA 2019 - Commission Staff Working Document, p. 230.

364 An association may be an obliged entity if it is a taxpayer or when arranging a small-scale money collection.

taxation-related common-good criterion and parties granted a money collection licence. However, such parties as registered associations are not as a rule obliged to report on their own activities and thus they are outside the scope of official supervision.

Moreover, there is no overall supervisor overseeing the NPO sector as the supervisory duties are divided among several different authorities and their powers have been found to be relatively limited. This is also seen as a vulnerability. Auditors and operations inspectors supervise certain aspects of the activities. The obligation to appoint an operations inspector arises when an actor meeting specific requirements does not need to have an auditor.[365] Moreover, most of the supervisory methods are applied on a 'spotcheck basis' and retroactively, which can be considered a vulnerability affecting the sector. The lack of supervisory powers also means that the activities of the NPO sector are not transparent or open.

Legislative inadequacies have been widely identified as vulnerabilities and they contribute to the lack of transparency. For example, registered non-profit or profit-driven associations only need to submit their financial statements to the Trade Register when at least two of the following and relatively high limits have been exceeded in the last completed financial year or the financial year immediately preceding it: net sales EUR 12,000,000, balance sheet total EUR 6,000,000 or an average of 50 employees. The problem concerning legislative inadequacies is also connected with the above-mentioned lack of supervisory powers because under the law, there is no single body responsible for supervising all NPO activities.

Vulnerabilities facing NPOs have also been identified in the private sector. The focus in the assessment of vulnerabilities affecting banks, payment gateway providers, payment service providers and FinTech companies is on their ability to identify unusual transactions involving NPOs. The key challenge facing banks is the development of automated monitoring (especially with regard to NPO activities). This is because the business operating models of NPOs are significantly different from those used by natural persons and companies. The challenging nature of the business operating model also impacts the ability of hawalas and providers of virtual currency services to identify unusual transactions. Observations regarding the vulnerabilities facing FinTech actors, payment gateway providers and providers of payment services concern the fragmented nature of

365 Under chapter 2(2) of the Auditing Act (1141/2015), there is no obligation to appoint an auditor in an organisation in which no more than one of the following conditions were met in both the last completed financial year and the financial year immediately preceding it: 1) the balance sheet total exceeds EUR 100,000; 2) the net sales or comparable revenue exceeds EUR 200,000; or 3) the average number of employees exceeds three. However, under chapter 6(38a) of the Associations Act, an association must elect an operations inspector if no auditor is appointed.

the monitoring systems and the occasional nature and short duration of the customer relationships.

Challenges arising from the blind spots in the cooperation and exchange of information between the authorities have emerged as a major NPO-related vulnerability. In the exchange of information, there have also been legislative challenges, which gives rise to differing interpretations concerning information disclosures. There are no separate provisions on the exchange of information and it may be hampered by the secrecy obligations concerning official information and documents. Moreover, Finland does not have any national information sharing coordinator or coordination mechanism. Even though the details of money collections are publicly accessible, the information is disclosed if a request for information is submitted.[366]

5.6.1.1 Vulnerabilities associated with terrorist financing faced in money collection activities

In money collection activities, the vulnerabilities associated with terrorist financing are considered more significant than in the NPO sector as a whole. The following are considered as the most significant vulnerabilities facing money collection activities in the NPO sector:

- Trust in NPOs and exploiting people's willingness to help
- Emphasis in supervision is on retroactive supervision
- Money collection legislation

In particular, NPOs engaged in charitable activities may collect substantial funds by directly appealing to the public for help. The organisations are considered actors working for good causes and for this reason, there is strong trust in them and their motivations are rarely questioned. Even if an NPO engaged in charity work does not collect money for questionable purposes, criminal actors might try to exploit the organisation for money laundering and terrorist financing by infiltrating the activities.

Money collection activities are supervised at national level but the emphasis on retroactive supervision can be seen as a vulnerability as it means that any misuse can only be dealt with after it has taken place. Small-scale money collections in particular can

366 For example, under section 33 of the Money Collection Act, 'notwithstanding the provisions of section 16, subsection 3 of the Act on the Openness of Government Activities (621/1999), the National Police Board may disclose information from the money collection register via a public information network to inform the general public regarding money collection licence holders, smallscale money collection organisers, purpose of the money collection as well as the income and expenses of an organised money collection. However, the authorities may not disclose the code element of the money collection organiser's personal identity code'.

be launched quite quickly[367] after the required notification has been submitted, which means that the dishonest activities may already be under way before the authorities have reacted.[368]

The fact that money collections and the actors arranging money collections do not explicitly fall within the scope of the Anti-Money Laundering Act is seen as a vulnerability with regard to the money collection legislation. This means that unlike the obliged entities, the activities of the NPOs arranging money collections are not directly assessed from the perspective of the prevention of money laundering and terrorist financing even though one purpose of the supervision is to prevent money laundering and terrorist financing.[369] The parties concerned should, however, take into account the FATF recommendations binding on Finland and the obligation of the Anti-Money Laundering Act to keep up-to-date records of beneficial owners and, if necessary, to disclose this information to the parties that are obliged entities under the Anti-Money Laundering Act.

5.6.1.2 Terrorist financing vulnerabilities affecting actors providing humanitarian aid and engaged in development cooperation

Based on an overall assessment, the vulnerabilities associated with terrorist financing that affect actors providing humanitarian aid and engaged in development cooperation are seen as less significant than those facing the NPO sector as a whole. Actors receiving public sector funding are not specified in the assessment of vulnerabilities but in such documents as the supranational risk assessment of the EU, the vulnerabilities associated with terrorist financing that affect such actors are also considered less significant.[370] The vulnerability is at level two (**moderately significant**). The following factors are seen as vulnerabilities that affect actors providing humanitarian aid and engaged in development cooperation:

- International crises
- Parties that are obliged entities under the Anti-Money Laundering Act are not familiar with international humanitarian law
- The actors are not familiar with regulation of anti-money laundering and combating of terrorist financing
- Limited case law

367 Under section 19 of the Money Collection Act, a small-scale money collection may be launched when the organiser has received the small-scale money collection number, or, at the latest, five working days after filing the notification of a small-scale money collection.

368 Government Proposal No. 214/2018, p. 71.

369 National Police Board/Gambling Administration: Money collection and prevention, and investigation of cases of money laundering and terrorist financing, referred to on 2 July 2020.

370 EU SNRA 2019 – Commission Staff Working Document, p. 231.

It has been noted that the actors providing humanitarian aid and engaged in development cooperation are affected by the same vulnerabilities as the NPO sector as a whole. However, due to the special nature of their work, organisations providing aid are facing particular types of vulnerability (such as the impact of international crises). The crises may manifest themselves in armed conflicts and related unrest, situations arising from large-scale refugeeism and forced displacement, natural disasters or other emergencies that create disorder leading to vulnerabilities. Aid organisations must react quickly when international crises erupt because the aid is often needed immediately. When quick action is required, the audit processes and verification of the partners may be inadequate or non-existent (especially in new regions).

Unfamiliarity with the international sources guiding the aid activities among obliged entities is seen as a vulnerability. The activities of the NPOs providing aid can only be considered acceptable if they comply with international obligations. When parties considered as obliged entities under the Anti-Money Laundering Act are unfamiliar with these obligations, all exceptional activities may be seen as acceptable because the real nature of the activities is not known. Inadequate awareness of AML/CFT functions may also prompt parties to submit unnecessary reports to the Financial Intelligence Unit.

It has also been noted that NPOs are not sufficiently familiar with anti-money laundering and anti-terrorist financing legislation. If the actors do not fully understand these obligations, they may become vulnerable to exploitation. Here too, the size of the NPO is an important factor: it has been noted that at least one major NPO is better-placed that small actors to check whether its own internal processes are in compliance with the official sources guiding the activities.[371]

Absence of case law can be seen as a vulnerability because it indicates that the capacity to extensively detect misuse may be lacking. It has also been highlighted in the supranational risk assessment that only in a very small number of cases has it been established that terrorist organisations have exploited NPOs by collecting and transferring funds through them. Despite the small number of cases, the risk can nevertheless be considered as significant.[372]

371 Official sources refer to such documents as international treaties and FATF recommendations.

372 EU SNRA 2019 - Commission Staff Working Document, p. 227.

5.6.2 Money laundering vulnerabilities facing the NPO sector

Most of the vulnerabilities associated with money laundering and facing the NPO sector are similar to those associated with terrorist financing. However, legislative deficiencies are more clearly seen as vulnerabilities in money laundering and they have prompted the view that the NPO sector is not open or transparent. NPOs do not directly fall within the scope of the Anti-Money Laundering Act or EU-level anti-money laundering legislation. However, they have to comply with the provisions applying to beneficial owners and customers of obliged entities.[373] National experts, too, identified the absence of the reporting obligation under the Anti-Money Laundering Act as a vulnerability associated with money laundering.

In another vulnerability from the perspective of the combating of money laundering, NPOs only have to submit a limited amount of financial information to registers even though associations are subject to indirect supervision as they have to appoint an auditor or an operations inspector. Furthermore, taxation information is, as a rule, confidential, which is also seen as a factor limiting transparency.

5.7 Risks facing the NPO sector

Experts have highlighted key risks arising from the combination of vulnerabilities and threats facing the NPO sector. The overall risk level facing NPOs is estimated at three (**significant**).

Irrespective of the field of activities, **small NPOs** are seen as a general risk facing the NPO sector as there is still room for improvement in their internal processes designed to prevent money laundering and terrorist financing. As NPOs are not obliged entities under the Anti-Money Laundering Act, the view is that the processes of small actors in particular remain inadequate. The observations suggest that in the case of small NPOs, the functioning of the processes mainly depend on the actors' economic resources, familiarity with money laundering and terrorist financing risks and the ability to address them.

The inability of NPOs to understand money laundering and terrorist financing risks and to evaluate them in a critical manner was also highlighted in the survey among NPOs.[374] The respondents were asked to estimate the risk level of money laundering and

373 EU SNRA 2019 - Commission Staff Working Document, p. 230.

374 The response rate was 17 per cent, which means that fewer than one in five of the recipients took part in the survey. Furthermore, the questionnaire was sent to an extremely small and randomly selected group, considering the size of the NPO sector. Thus the results of the survey do not represent the views of the sector as a whole, but the observations based on the responses and experts' opinions lend support to the view that inadequate understanding and lack of critical analysis among NPOs is a major risk facing the sector.

terrorist financing from the perspective of their own activities and on a sector-specific basis. The assessment had to be made using a four-level scale (low, medium, high, very high). All respondents put the terrorist financing risk at level one (low), both in their own sectors and in their own organisations. Most of the respondents also put the risk of money laundering in their sectors at the same level. At the same time, all respondents were of the view that in their own activities, the money laundering risk is low. National NPOs' views on risks differ significantly from the views of the authorities and other experts, and thus this discrepancy can also be seen as a factor increasing the risk.

Criminal or terrorist actors posing as legal actors or infiltrating legal organisations have been identified as risks facing money collection activities. Criminals may arrange legal money collections using the facade of legal activities even though the funds are actually raised for criminal purposes. Exploiting NPO activities for money laundering or terrorist financing without the authorities being able to prevent it is also seen as a more general risk. This may be in the form of an activity that does not involve identification or reporting obligations and that thus exploits legislative loopholes and the absence of the registration obligation. Illegal activities in the NPO sector also constitute a risk when they do not come to the attention of the authorities that would have the powers to tackle them.

Carrying cash to crisis countries and distributing aid in cash in the destination countries are seen as significant risks facing humanitarian actors. Poor traceability is a major risk in this respect as it also makes transporting cash an attractive option to criminals. This is because cash can be carried across national boundaries without it being noticed. Individuals carrying cash may also be subject to a high personal risk as terrorist groups might attack them in the hope of obtaining large amounts of cash. In cash transport, the risk of the money ending up in the wrong hands is also more likely than when the money is transferred electronically. According to the supranational risk assessment, the refusal of credit institutions to make their services available to NPOs makes unofficial systems more popular.[375] Moreover, as a rule, cash transported to crisis countries cannot be distributed on location by means of electronic money transfer systems. Thus, in the worst case, the risks accumulate.

375 EU SNRA 2019 - Commission Staff Working Document, pp. 227–228.

SOURCES

Official documents

European Union legislation

Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

Directive (EU) 2015/849 of the European Parliament and of the Council on the preven- tion of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU.

Commission Delegated Regulation of 7 May 2020 amending Delegated Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council, as regards adding the Bahamas, Barbados, Botswana, Cambodia, Ghana, Jamaica, Mauritius, Mongolia, Myanmar/Burma, Nicaragua, Panama and Zim- babwe to the table in point I of the Annex and deleting Bosnia-Herzegovina, Ethiopia, Guyana, Lao People's Democratic Republic, Sri Lanka and Tunisia from this table. Brussels 7.5.2020, C(2020) 2801 final.

International agreements and obligations

Council of Europe Treaty Series - No. 215: Council of Europe Convention on the Manipulation of Sports Competitions.

SopS 74/2002, Tasavallan presidentin asetus kansainvälisen terrorismin rahoituksen torjumisesta tehdyn yleissopimuksen voimaansaattamisesta sekä yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta annetun lain voi- maantulosta. [*Decree of the President of the Republic on the implementation of the International Convention for the Suppression of the Financing of Terrorism and on the entry into force of the Act on the implementation of the provisions of a legislative nature in the Convention*] (SopS [*Finnish Treaty Series*] 74/2002).

SopS 49/2008, Tasavallan presidentin asetus terrorismin ennaltaehkäisyä koskevan Euroopan neuvoston yleissopimuksen voimaansaattamisesta ja yleissopimuksen lain- säädännön alaan kuuluvien määräysten voimaansaattamisesta annetun lain voimaan- tulosta. [*Decree of the President of the Republic on the implementation of the Council of Europe Convention on the Prevention of Terrorism and on the entry into force of the Act on the implementation of the provisions of a legislative nature in the Convention*] (SopS [*Finnish Treaty Series*] 49/2008).

UN Security Council Resolution 1373 (2001).

Other official international sources

CTED (2019)
United Nations Security Council: Counter-Terrorism Committee Executive Directorate CTED – Identifying and exploring the nexus between human trafficking, terrorism, and terrorism financing, 2019.

European Economic and Social Committee (2019/C 353/01)
European Economic and Social Committee: Opinion on 'Blockchain and distributed ledger technology as an ideal infrastructure for the social economy' (own-initiative opin- ion) (2019/C 353/01).

EU SNRA (2017)
European Comission: Report from the Commission to the European Parliament and the Council on the

assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. Brussels 26.6.2017, COM(2017) 340 final.

EU SNRA 2017– Commission Staff Working Document
European Comission: Commission Staff Working Document Accompanying the Document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. Brussels 26.6.2017, COM(2017) 340 final.

EU SNRA (2019)
European Comission: Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. Brussels 24.7.2019, COM(2019) 370 final.

EU SNRA 2019 – Commission Staff Working Document
European Comission: Commission Staff Working Document Accompanying the Document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. Brussels 24.7.2019, COM(2019) 370 final.

United Nations Security Council (S/2020/151)
United Nations Security Council: Final report of the Panel of Experts submitted pursuant to resolution 2464 (2019), S/2020/151, 2.3.2020.

National law

Act on the Bank and Payment Accounts Control System (571/2019)
Act on Preventing Money Laundering and Terrorist Financing (444/2017)
Act on the Financial Intelligence Unit (445/2017)
Act on the Freezing of Funds with a View to Combating Terrorism (325/2013)
Money Collection Act (863/2019)
Criminal Code of Finland (39/1889)
Foundations Act (487/2015)
Associations Act (503/1989)

Government proposals

Government Proposal No. 95/1993
Government Proposal No. 95/1993 Hallituksen esitys eduskunnalle oikeushenkilön rangaistusvastuuta koskevaksi lainsäädännöksi. [*Government Proposal submitted to Parliament for legislation concerning corporate criminal liability*]

Government Proposal No. 53/2002
Government Proposal No. 53/2002 Hallituksen esitys eduskunnalle eräiden rikoslain talousrikossäännösten ja eräiden niihin liittyvien lakien muuttamiseksi. [*Government Proposal submitted to Parliament for legislation amending certain provisions on economic offences in the Criminal Code of Finland and certain related Acts.*]

Government Proposal No.228/2016
Government Proposal No. 228/2016 Hallituksen esitys eduskunnalle laiksi rahanpesun ja terrorismin rahoittamisen estämisestä, laiksi rahanpesun selvittelykeskuksesta sekä eräiksi niihin liittyviksi laeiksi. [*Government Proposal submitted to Parliament for legis- lation concerning preventing money laundering and terrorist financing, for legislation on the Financial Intelligence Unit and for certain related Acts.*]

Government Proposal No. 129/2017
Government Proposal No. 129/2017 Hallituksen esitys eduskunnalle laeiksi ulkomaalaislain ja ulkomaalaisrekisteristä annetun lain 3 b §:n muuttamisesta. [*Government Proposal submitted to Parliament for legislation amending the Aliens Act and Section 3b of the Act on the Register of Aliens.*]

Government Proposal No. 38/2018
Government Proposal No. 38/2018 Hallituksen esitys eduskunnalle laiksi Finanssivalvonnasta annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi. [*Government Proposal submitted to Parliament for legislation amending the Act on the Financial Supervisory Authority and certain related Acts.*]

Government Proposal No. 167/2018
Government Proposal No. 167/2018 Hallituksen esitys eduskunnalle laiksi pankki- ja maksutilien

valvontajärjestelmästä ja eräiksi siihen liittyviksi laeiksi. [*Government Pro posal submitted to Parliament for legislation concerning the bank and payment account monitoring system and certain related Acts*.]

Government Proposal No. 214/2018

Government Proposal No. 214/2018 Hallituksen esitys eduskunnalle rahankeräyslaiksi ja eräiksi siihen liittyviksi laeiksi. [*Government Proposal submitted to Parliament for legislation concerning a money collection act and certain related Acts*.]

Government Proposal No. 135/2020

Government Proposal No. 135/2020 Hallituksen esitys eduskunnalle terrorismin rahoittamista koskevien säännösten muuttamiseksi. [*Government Proposal submitted to Parliament for amending the provisions concerning terrorist financing*.]

Government Proposal No. 183/2020

Government Proposal No.183/2020 Hallituksen esitys eduskunnalle rikoslain 1 luvun 11 §:n ja 32 luvun 11 §:n muuttamisesta. [*Government Proposal submitted to Parlia- ment for amending Chapter 1 Section 11 and Chapter 32 Section 11 of the Criminal Code of Finland*.]

Other official sources

Ministry of Justice (2020a)

Publications of the Ministry of Justice: Mietintöjä ja lausuntoja [*Reports and statements*] 2020:2 – Terrorismin rahoittamista koskevien säännösten muuttaminen, lausuntotiivistelmä. [*Amendment of the provisions on terrorist financing, summary*]

Ministry of Justice (2020b)

Publications of the Ministry of Justice: Mietintöjä ja lausuntoja [*Reports and statements*] 2020:8 – Terrorismirikosten sääntelyn ajanmukaisuus ja vastaavuus vertailumaiden sääntelyn kanssa, työryhmämietintö. [*The up-to-date nature of the regulation of terrorist offences and correlation with regulation in reference countries, working group report*.]

Ministry of the Interior (2017)

Publications of the Ministry of the Interior 29/2017: National CBRNE Strategy 2017.

Ministry of the Interior (2019)

Publications of the Ministry of the Interior 2019:14: Malkki, Leena ja Saarinen, Juha: Jihadism in Finland.

Ministry of Economic Affairs and Employment (2020)

Publications of the Ministry of Economic Affairs and Employment 2020:38: Companies – Report of the Working Group Preparing the Introduction of a Lighter Review.

Ministry for Foreign Affairs (2019a)

Publications of the Ministry for Foreign Affairs 2019:1: Suomi humanitaarisen avun antajana. [*Finland as a donor of humanitarian assistance*.] Available in Finnish (abstract in English)

Ministry for Foreign Affairs (2019b)

Ulkoministeriön tilinpäätös 2019. [*Foreign Ministry's financial accounts 2019*.] Available in Finnish

Legal cases

Sentence given by the Eastern Uusimaa District Court on 1 November 2019 no 19/148060, case R 19/4373
Sentence given by the Turku Court of Appeal on 25 April 2013 no 13/857, case R12/933
Sentence given by the Helsinki Court of Appeal on 23 March 2016 no 16/111925, case R 15/526
Sentence given by the Helsinki Court of Appeal on 29 May 2020 no 20/118778, case R 19/7
Sentence given by the District Court of Helsinki on 21 March 2018 no 18/112809, case R 17/10068
Sentence given by the District Court of Helsinki on 13 March 2018 no 18/116182, case R 17/10930

Literature, articles and other publications

Black Wallet (2020a)

The National Bureau of Investigation (Finland) – Swedish Police: Black Wallet – Risk Indicators Report, 2020.

Black Wallet (2020b)

The National Bureau of Investigation (Finland) – Swedish Police: Black Wallet – Risk Indicators, 2020.

CTED (2020)

United Nations Security Council – Counter-Terrorism Committee Executive Directorate: CTED Trends Alert

- Member States Concerned By The Growing and Increasingly Transnational Threat of Extreme Right-Wing Terrorism, 2020.

Europol (2015)
Europol / Financial Intelligence Group: Why is cash still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering, 2015.

Europol (2017)
Europol / Financial Intelligence Group: From suspicion to action - Converting financial intelligence into greater operational impact, 2017.

Europol (2020a)
Europol / European Financial and Economic Crime Centre: Enterprising criminals - Europe's fight against the global networks of financial and economic crime, 2020.

Europol (2020b)
Europol: Beyond the pandemic - how COVID-19 will shape the serious and organised crime landscape in the EU, 2020.

Europol (2020c)
Europol: European Union Terrorism Situation and Trend Report (TE-SAT), 2020.

FATF (2012–2020)
FATF: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Paris, France 2012–2020.

FATF (2013)
FATF: National Money Laundering and Terrorist Financing Risk Assessment Guidance. Paris, France 2013.

FATF (2015a)
FATF: Money Laundering Through the Physical Transportation of Cash. Paris, France 2015.

FATF (2015b)
FATF: Emerging Terrorist Financing Risks. Paris, France 2015.

FATF and MENAFATF (2015)
FATF: Money Laundering Through the Physical Transportation of Cash. Paris, France and Manama, Bahrain 2015.

FATF (2018)
FATF: Financial Flows from Human Trafficking. Paris, France 2018.

FATF (2019)
FATF: Terrorist Financing Risk Assessment Guidance. Paris, France 2019.

FATF MER (2019)
FATF: Anti-money laundering and counter-terrorist financing measures – Finland, Fourth Round Mutual Evaluation Report. Paris, France 2019.

FATF (2020a)
FATF: COVID-19-related Money Laundering and Terrorist Financing, Risks and Policy Responses. Paris, France 2020.

FATF (2020b)
FATF: Guidance on Digital Identity. Paris, France 2020.

Finance Finland (2019a)
Finance Finland: Finnish Banking 2019

Finance Finland (2019b)
Finance Finland: Finnish insurance in 2019

Financial Supervisory Authority (2019)
Financial Supervisory Authority: Principles for determining the size of penalty payments and administrative fines 19.6.2019.

Financial Supervisory Authority (2020a)
Financial Supervisory Authority: Valvojakohtaisen rahanpesun riskiarvion yhteenveto, 17.3.2020. [*Summary of the supervisor-specific assessment of inherent risk published on 17 March 2020*]
Available in Finnish

Financial Supervisory Authority (2020b)
Financial Supervisory Authority: Summary of sector-specific assessment of money laundering risk concerning payment service providers, published on 24 August 2020.

Forsman (2020)
Forsman, Markus: 30 years of combating money laundering in Sweden and internationally – does the system function as intended? In: Sveriges Riksbank Economic Review 2020:1.

Grey Economy Information Unit (2018)
Grey Economy Information Unit: Selvitys 21/2018 - Rikostaustaustatiedon merkitys harmaan talouden riskin arvioinnissa, 21.8.2018. [*Report 21/2018 - Importance of information on criminal background in assessment of grey economy risk*.]

Grey Economy Information Unit (2019)
Grey Economy Information Unit: Selvitys 4/2019 - Viranomaisten näkemyksiä harmaan talouden nykytilasta - Kyselytutkimuksen tulokset harmaasta taloudesta, sen torjunnasta ja ilmiöistä. *[Report 4/2019 - Authorities' views on the current state of the grey economy - Survey's results on the grey economy, its prevention and phenomena*]
HEUNI (2019)
HEUNI Report series 92b: Shady business. Uncovering the business model of labour exploitation, 2019.
HEUNI (2020)
HEUNI: Uncovering labour trafficking – Investigation tool for law enforcement and checklist for labour, 2020.
Hoppu – Hoppu – Hoppu (2020)
Hoppu, Esko – Hoppu, Kari – Hoppu, Katja: Kauppa- ja varallisuusoikeuden pääpiirteet. [*Main characteristics of commercial and property law*] Available in Finnish Alma Talent Oy, Helsinki 2020.
The assistance system for victims of human trafficking (2020)
The assistance system for victims of human trafficking: Report 1.1.-30.6.2020.
KCOOS (2017)
Keep Crime out of Sport (KCOOS) 2017: Guidebook on understanding and effectively combating the manipulation of sports competitions. Version 1.
OCP (2015)
Final Report of Project OCP – Organised Crime Portfolio 2015. Savona, Ernesto U. – Riccardi, Michele (ed.).: From illegal markets to legitimate businesses.
PAF (2019)
Ålands Penningautomatförening: Annual report 2019.
Palonen – Laitinen (2011)
Palonen, Ulla – Laitinen, Kari: Näkökulmia poliittiseen, uskonnolliseen ja taloudelliseen terrorismiin. [*Perspectives on political, religious and economic terrorism.*] Available in Finnish In: Susi, Mika – Pekkala, Niina (ed.): Terrorismin rahoitus. [Terrorist Financing] Available in Finnish Police University College, Reports 94 (2011).
Peurala (2013)
Peurala, Johanna: Match-manipulation in football – the challenges faced in Finland. The International Sports Law Journal 13 (3). 2013.
Pohjonen (2020)
Pohjonen, Matti: Jihadist online communication and Finland. In: Paronen, Antti – Saarinen, Juha (ed.): Karavaanin sotapolku: näkökulmia jihadismiin. [*Caravan on the warpath: perspectives on jihadism*.] Available in Finnish National Defence University, Series 1: Research Publications No. 42
National risk assessment of money laundering and terrorist financing (2015)
Jukarainen, Pirjo – Muttilainen, Vesa: National risk assessment of money laundering and terrorist financing 2015. Poliisiammattikorkeakoulun raportteja [*Reports of the Police University College*] 2015.
PRIO (2007)
International Peace Research Institute Oslo (PRIO): Report 3/2007 - Legal, Rapid and Reasonably Priced? A Survey of Remittance Services in Norway.
Financial Intelligence Unit (2018a)
National Bureau of Investigation / Financial Intelligence Unit Rahanpesurikokset oikeuskäytännössä IX - Törkeät rahanpesutuomiot käräjäoikeuksissa 2015 ja 2016. [*Money laundering offences in case law IX - Aggravated money laundering sentences issued by District Courts in 2015 and 2016.*] Available in Finnish
Financial Intelligence Unit (2018b)
National Bureau of Investigation / Financial Intelligence Unit Annual Report 2018.
Financial Intelligence Unit (2019)
National Bureau of Investigation / Financial Intelligence Unit Annual Report 2019.
Financial Intelligence Unit (2020a)
National Bureau of Investigation / Financial Intelligence Unit Semi-annual Report 2020.
Financial Intelligence Unit (2020b)
National Bureau of Investigation / Financial Intelligence Unit Selvitys terrorismin rahoittamisen ominaispiirteistä. [*Report on the special characteristics of terrorist financing.*] Available in Finnish Public version, 2020.
SUEK (2019)
Finnish Centre for Integrity in Sports (SUEK ry): Sopimaton lopputulos, Selvitys urheilukilpailujen manipulaation torjunnasta. [*Unacceptable result, Report on prevention of manipulation of sporting competitions.*] Publication 4/2019.
Finnish Security and Intelligence Service (2020)
Finnish Security and Intelligence Service: National Security Overview 2020.

Finnish Bar Association (2019)
Finnish Bar Association: Rahanpesulain edellyttämä vuosikertomus 2019. [*Annual report required by the Anti-Money Laundering Act 2019*] Available in Finnish
Finnish Institute for Health and Welfare (2019)
Finnish Institute for Health and Welfare, Reports 18/2020: Rahapelaaminen, peliongelmat ja rahapelaamiseen liittyvät asenteet ja mielipiteet vuosina 2007-2019 – Suomalaisten rahapelaaminen 2019. [*Gambling, problem gambling and attitudes and opinions towards gambling in 2007–2019. Finnish Gambling 2019.*] Available in Finnish (abstract in English)
Tuomaala-Järvinen (2020)
Tuomaala-Järvinen, Lotta: Uhkailu, kiristys ja ryöstäminen – pysyvät metodit jihadistiryhmien varainhankinnassa. [*Threats, extortion and robbery – permanent methods of fundraising in jihadist groups*.] In: Paronen, Antti – Saarinen, Juha (ed.): Karavaanin sotapolku: näkökulmia jihadismiin. [*Caravan on the warpath: perspectives on jihadism*.] (Available in Finnish) National Defence University, Series 1: Research Publications No. 42
Villa (2018)
Villa, Seppo: Henkilöyhtiöt ja osakeyhtiö. [Partnerships and limited companies.] (Available in Finnish) Alma Talent Oy, Helsinki 2018.
Virén (2014)
Virén, Matti: Yleishyödylliset yhteisöt Suomessa – Verot, lahjoitukset ja avustukset tutkimuksen kohteena. [*Non-profit organizations in Finland – Taxes, donations and pub- lic support under scrutiny*.] Available in Finnish (abstract in English) Hanken School of Economics Research Report, Helsinki 2014.

Internet sources

Regional State Administrative Agency for Southern Finland: Panttilainauslupaluettelo [*List of licensed pawnbrokers*] (in Finnish) 13.11.2020. Available in Finnish: https://www.avi.fi/documents/10191/5265091/Panttilainauslupaluettelo+4.12.2015/1b1f17f7-c4b8-44e0-82fc-0446e61768d2, referred to on 17 November 2020.
Regional State Administrative Agency for Southern Finland: Perintä. [*Debt collection*.] Available in Finnish: https://www.avi.fi/web/avi/perinta, referred to on 22 July 2020.
Regional State Administrative Agency for Southern Finland: Money laundering supervision register. Available in Finnish: https://www.avi.fi/web/avi/rahanpesun-valvontarekisteri, referred to on 29 July 2020.
Regional State Administrative Agency for Southern Finland: Valuutanvaihto ja yrityspalvelut. [*Currency exchange and business services*.] Available in Finnish: https://www.avi.fi/web/avi/valuutanvaihto, referred to on 5 November 2020.
European Commission: Strategy / Shaping Europe's digital future – Blockchain Technologies. Available: https://ec.europa.eu/digital-single-market/en/blockchain-technologies, referred to on 16 October 2020.
FATF: What is Money Laundering? Available: https://www.fatf-gafi.org/faq/moneylaundering/, referred to on 5 August 2020.
Finance Finland: Pankit merkittäviä kansantaloudelle. [*Banks play a vital role in the national economy*.] Available in Finnish: https://www.finanssiala.fi/finanssialasta/pankit- ja-rahoitus/Sivut/default.aspx, referred to on 2 November 2020.
Financial Supervisory Authority: Warnings concerning unauthorised service providers. Available in Finnish: https://www.finanssivalvonta.fi/rekisterit/varoituslistat/luvattomia-palveluntarjoajia-koskevat-varoitukset/, referred to on 4 August 2020.
Financial Supervisory Authority: FinTech – Finanssialan innovaatiot. [*FinTech – Financial sector innovations*] Available in Finnish: https://www.finanssivalvonta.fi/pankki/fintech--finanssialan-innovaatiot/, referred to on 31 July 2020.
Financial Supervisory Authority: Press release 1 November 2019: The Financial Supervisory Authority granted five registrations as virtual currency provider – scope of supervision is the prevention of money laundering. Available in Finnish: https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/lehdistotiedotteet/2019/finanssivalvonta-myonsi- viidelle-virtuaalivaluutan-tarjoajalle-rekisteroinnin-valvonnan-tavoitteena-on-rahanpesun-estaminen2/, referred to on 11 November 2020.
Financial Supervisory Authority: Payment service providers Available in Finnish: https://www.finanssivalvonta.fi/pankki/toimiluvat-ja-rekisterointi/maksupalveluntarjoajat/, referred to on 22 July 2020.
Financial Supervisory Authority: Investment firms. Available in Finnish: https://www.fi- nanssivalvonta.fi/paaomamarkkinat/sijoituspalvelun-tarjoajat/, referred to on 11 November 2020.

Financial Supervisory Authority: Alternative investment fund managers (AIFMs). Available in Finnish: https://www.finanssivalvonta.fi/paaomamarkkinat/vaihtoehtorahastojen-hoitajat/, referred to on 11 November 2020.
Financial Supervisory Authority: Virtual currency providers. Available in Finnish: https://www.finanssivalvonta.fi/pankki/fintech--finanssialan-innovaatiot/virtuaalivaluutan-tarjoajat/, referred to on 11 November 2020.
Finavia: Finavia airports had 26 million passengers in 2019 – a year of moderate growth in air traffic. Available in Finnish: https://www.finavia.fi/fi/uutishuone/2020/finavian-lentoasemilla-26-miljoonaa-matkustajaa-vuonna-2019-lentoliikenteessa-oli, referred to on 23 November 2020.
Grey economy & economic crime Professional exploitation of companies by fraudsters is an offence. Available in Finnish: https://www.vero.fi/harmaa-talousrikollisuus/ilmi%C3%B6t/ammattimainen-yritysten hyv%C3%A4ksik%C3%A4ytt%C3%B6/, referred to on 23 December 2020.
Grey economy & economic crime Shadow economy in east-west trade. Available in Finnish: https://www.vero.fi/harmaa-talous-rikollisuus/ilmi%C3%B6t/it%C3%A4kaupanharmaa-talous/, referred to on 1 December 2020.
Grey economy & economic crime Koronavirus lisännyt viranomaisten huolta tukipetosten kasvusta. [*Coronavirus has increased the authorities' concerns of an increase in fraud associated with public aid.*] Available in Finnish: https://www.vero.fi/harmaa- talous-rikollisuus/laajuus/harmaan-talouden-mittaaminen/#koronaviruslisannyt, referred to on 21 December 2020.
Grey economy & economic crime prevention. Available in Finnish: https://www.vero.fi/harmaa-talous-rikollisuus/torjunta/rikostorjunta/, referred to on 22 January 2021.
Helsingin Sanomat 20 October 2020: Koronapandemian aikana käteisen käyttö on vähentynyt: [*Use of cash has decreased during the coronavirus pandemic.*] Suuntaus johtaa entistä helpommin rahanpesu-ilmoitukseen ja tietää vaikeuksia rikollisille. [*This trend will lead to an increase in the filing of money laundering reports and will cause problems for criminals.*] Available in Finnish: https://www.hs.fi/kotimaa/art- 2000006675295.html, referred to on 22 December 2020.
The assistance system for victims of human trafficking: Lehdistötiedote [press release] 15.7.2020: uhrien auttamisjärjestelmän asiakkaaksi hakeutuu yhä enemmän Suomessa uhriksi joutuneita. [*rising numbers of victims in Finland contacting the assistance system for assistance.*] Available in Finnish: http://www.ihmiskauppa.fi/ihmiskauppa/ajankohtaista/lehdistotiedote_ihmiskaupan_uhrien_auttamisjarjestelman_asiakkaaksi_hakeutuu_yha_enemman_suomessa_uhriksi_joutuneita.591.news, referred to on 26 August 2020.
University of Jyväskylä: Kansalaisyhteiskunnan tutkimusportaali - Kolmas sektori. [*Civil society research portal - Third sector.*] Available in Finnish: http://kans.jyu.fi/sanasto/sanat-kansio/kolmas-sektori, referred to on 24 July 2020.
Kauppalehti 3 April 2019: Helsinki-Vantaalle alkaa lentää kolme uutta yhtiötä – Kaksi on kiinalaisia. [*Three new airlines will start flying to Helsinki-Vantaa airport – Two of these are Chinese*] Available in Finnish: https://www.kauppalehti.fi/uutiset/kl/f5769e3e-39f5-4d2d-b140-24ee2264ca99, referred to on 23 November 2020.
Kauppalehti 16 August 2020: Saitko puhelun, jossa kyseltiin maksukortin tietoja koronatestauksen takia? – THL varoittaa huijaussoitoista. [*Have you had a phone call asking for payment card details for coronavirus testing? – Finnish Institute for Health and Welfare is warning people about scam phone calls*] Available in Finnish: https://www.kauppalehti.fi/uutiset/saitko-puhelun-jossa-kyseltiin-maksukortin-tietoja-koronatestauksen-takia-thl-varoittaa-huijaussoitoista/48a8e8ef-f777-4824-9c30236d08cd2868, referred to on 21 December 2020.
National Bureau of Investigation: Black Wallet. Available: https://www.poliisi.fi/keskusrikospoliisi/black_wallet, referred to on 31 July 2020.
Federation of Real Estate Agency: Kiinteistönvälitysalan liikevaihto nousi 7,7 % vuonna 2019 – toimiala kasvanut yhtäjaksoisesti viimeiset viisi vuotta, [*Federation of Real Estate Agency's revenue increased 7.7% in 2019 – sector grown continuously over the past five years.*] (Available in Finnish): https://kvkl.fi/kiinteistonvalitysalan-liikevaihto2019/, referred to on 12 November 2020.
Federation of Real Estate Agency: Vanhojen asuntojen kauppa loikkasi vuonna 2019 – joulun alla vauhti vain kiihtyi. [*Sharp rise in sales of old apartments in 2019 – rate in- creased leading up to Christmas.*] Available in Finnish: https://kvkl.fi/vanhojen-asuntojen-kauppa-loikkasi-vuonna-2019-joulun-alla-vauhti-vain-kiihtyi/, referred to on 12 November 2020.
Lotteriinspektionen: Åland och spel. Available in Finnish: https://www.li.ax/aland-och-spel, referred to on 2 November 2020.
Football Association of Finland. Available in Finnish: https://www.palloliitto.fi/, referred to on 16 December 2020.
Finnish Patent and Registration Office: Avoimen yhtiön ja kommandiittiyhtiön tilinpäätös rekisteriin. [*General partnerships and limited partnerships file their financial statements with the Trade Register.*] Available in Finnish: https://www.prh.fi/fi/tilinpaatokset/ilmoitus_suoraan_kaupparekisteriin/avoin_yhtio_ja_kommandiittiyhtio.html, referred to on 10 November 2020.

Finnish Patent and Registration Office: Foundations – annual report. Available in Finn ish: https://www.prh.fi/fi/saatiorekisteri/valvonta/vuosiselvitys.html, referred to on 24 July 2020.
Finnish Patent and Registration Office: Press release 2 July 2020: Osakeyhtiö ja osuuskunta - Tee maksuton edunsaajailmoitus kaupparekisteriin viipymättä. [*Limited liability companies and co-operatives: Submit your financial statements in time*] Available in Finnish: https://www.prh.fi/fi/asiakastiedotteet/2020/P_21238.html, referred to on 29 July 2020.
Finnish Patent and Registration Office: Registration of auditors. Available in Finnish: https://www.prh.fi/fi/tilintarkastusvalvonta/tilintarkastusvalvonta/kertomus_prhn_tilintarkastus-valvonnan_toiminnasta_2019/tilintarkastajien_rekisterointi.html, referred to on 7 January 2021.
Finnish Patent and Registration Office: Number of enterprises in the Trade Register. Available in Finnish: https://www.prh.fi/fi/kaupparekisteri/yritystenlkm/lkm.html, referred to on 9 November 2020.
Police: Narcotics offences. Available in Finnish: https://poliisi.fi/huumausainerikokset, referred to on 21 January 2021.
Police: Trafficking in human beings. Available in Finnish: https://www.poliisi.fi/rikokset/ihmiskauppa, referred to on 26 August 2020.
Police: Organised crime. Available in Finnish: https://poliisi.fi/jarjestaytynyt-rikollisuus, referred to on 21 January 2021.
Police: Manner-Suomen rahapelimarkkinoiden kehitys. [*Development of Mainland Finland's gambling market*.] Available in Finnish: https://poliisi.fi/rahapelimarkkinoiden-kehitys, referred to on 19 January 2021.
Police: Poliisi varoittaa koronahuijareista – huijausten kohteina etenkin iäkkäät. [*Police issues warning about coronavirus scammers – the elderly are the biggest target*.] Avail- able in Finnish: https://www.poliisi.fi/poliisihallitus/tiedotteet/1/0/poliisi_varoittaa_koronahuijareista_huijausten_kohteina_etenkin_iakkaat_89054, referred to on 9 November 2020.
Police: Economic crime. Available in Finnish: https://poliisi.fi/talousrikokset, referred to on 21 January 2021
National Police Board/Gambling Administration: Crowdfunding and money collection. Available in Finnish: https://www.arpajaishallinto.fi/rahankeraykset/rahankeraysluvat/joukkorahoitus, referred to on 16 October 2020.
National Police Board/Gambling Administration: Money collection and prevention, and investigation of cases of money laundering and terrorist financing Available in Finnish: https://www.arpajaishallinto.fi/rahankeraykset/rahanpesu_terrorismin_rahoituksen_estaminen, referred to on 2 July 2020.
Rahanpesu.fi: Rahanpesusäännöksiä täydennetään rikoslaissa. [*Provisions on money laundering will be supplemented in the Criminal Code of Finland*.] Available in Finnish: https://rahanpesu.fi/-/1410853/rahanpesusaannoksia-taydennetaan-rikoslaissa, referred to on 5 January 2021.
Ministry of the Interior: Stepping up the fight against human trafficking through cooperation between authorities and organisations. Available in Finnish: https://intermin.fi/-/ihmiskaupan-torjuntaa-tehostetaan-viranomaisten-ja-jarjestojen-yhteistyolla, referred to on 20 January 2021.
Ministry of the Interior: Tax fraud is the most common economic crime. Available in Finnish: https://intermin.fi/poliisi-asiat/talousrikollisuus-ja-harmaa-talous, referred to on 22 January 2021.
Ministry of the Interior project: Overhaul of the Lotteries Act. Available in Finnish: https://intermin.fi/hankkeet/hankesivu?tunnus=SM051:00/2019, referred to on 25 February 2021.
Ministry of Social Affairs and Health: Statutory insurances against loss of damage. Available in Finnish: https://stm.fi/vahinkovakuutukset, referred to on 8 October 2020.
Finnish Security and Intelligence Service: The terrorist threat assessment is an overview of terrorism. Available in Finnish: https://supo.fi/uhka-arvio, referred to on 17 December 2020.
The Bank of Finland Payments statistics 2019. Available in Finnish: https://www.suomenpankki.fi/fi/Tilastot/maksuliiketilastot/maksuliiketilastot/, referred to on 22 July 2020.
Suomen Yrittäjät: Toiminimi eli yksityinen elinkeinonharjoittaja [Private trader]. Available in Finnish: https://www.yrittajat.fi/yrittajan-abc/perustietoa-yrittajyydesta/yritysmuodot-ja-vastuut/toiminimi-eli-yksityinen, referred to on 9 November 2020.
Finnish Institute for Health and Welfare Coronavirus COVID-19 – Latest Updates. Available in Finnish: https://thl.fi/fi/web/infektiotaudit-ja-rokotukset/ajankohtaista/ajankohtaista-koronaviruksesta-covid-19/materiaalipankki-koronaviruksesta/koronavirusselkokielella, referred to on 7 August 2020.
Finnish Institute for Health and Welfare Wastewater study – narcotics use among the population. Available in Finnish: https://thl.fi/fi/tutkimus-ja-kehittaminen/tutkimukset-ja-hankkeet/jatevesitutkimus, referred to on 22 January 2021.
Finnish Institute for Health and Welfare Arranging COVID-19 vaccinations in Finland Available in Finnish: https://thl.fi/fi/web/infektiotaudit-ja-rokotukset/ajankohtaista/ajankohtaista-koronaviruksesta-covid-19/tarttuminen-ja-suojautuminen-koronavirus/rokotteet-ja-koronavirus/koronarokotusten-jarjestaminen-suomessa, referred to on 14 January 2021.
Finnish Institute for Health and Welfare Gambling. Available in Finnish: https://thl.fi/fi/web/alkoholi-tupakka-ja-riippuvuudet/rahapelit, referred to on 7 January 2021.

Statistics Finland Number of property offences increased by 16.9 per cent. Available in Finnish: https://www.stat.fi/til/rpk/2020/04/rpk_2020_04_2021-01-19_tie_001_fi.html, referred to on 21 January 2021.
Statistics Finland Number of coercive measures performed went up by 3 per cent. Available in Finnish: https://www.tilastokeskus.fi/til/rpk/2020/14/rpk_2020_14_2021-02- 26_tie_001_fi.html, referred to on 23 March 2021.
Statistics Finland Structural business and financial statement statistics. Available in Finnish: https://www.stat.fi/til/yrti/ referred to on 12 November 2020.
Finnish Customs: Bank and Payment Accounts Control System. Available in Finnish: https://tulli.fi/asiointi-info/pankki-ja-maksutilien-valvontajarjestelma, referred to on 2 De- cember 2020.
Finnish Customs: Graphs of Finland's foreign trade 2020. Available in Finnish: https://tulli.fi/documents/2912305/3439475/Kuvioita%20Suomen%20ulkomaankaupasta%20 2020/34d76da6-523f-4ccf-6755-075cbc68d71b/Kuvioita%20Suomen%20ulkomaankaupasta%202020. pdf?version=1, referred to on 23 November 2020
Ministry for Foreign Affairs Arms control and disarmament. Available in Finnish: https://um.fi/asevalvonta-ja-aseidenriisunta, referred to on 5 August 2020.
Ministry for Foreign Affairs Report suspected misuse of funds. Available in Finnish: https://um.fi/ilmoita-epailemastasi-varojen-vaarinkaytosta, referred to on 20 October 2020.
Ministry for Foreign Affairs Civil society is an important actor and development cooperation partner. Available in Finnish: https://um.fi/kehityspolitiikan-kumppanit-kansalaisyhteiskunta, referred to on 23 July 2020.
Ministry for Foreign Affairs Development cooperation appropriations and statistics. Available in Finnish: https://um.fi/suomen-kehitysyhteistyon-maararahat, referred to on 22 July 2020
Ministry for Foreign Affairs Sanctions. Available in Finnish: https://um.fi/pakotteet, referred to on 2 March 2021.
Ministry for Foreign Affairs Humanitarian aid provided by Finland in 2019. Available in Finnish: https://um.fi/documents/35732/0/suomen-humanitaarinen-apu-2019.pdf/8cb02e3e-5b7d-2af0-eaee-a14e2b3e6a01?t=1588573704367, referred to on 22 July 2020.
Ministry for Foreign Affairs Goals and principles of Finland's development policy. Available in Finnish: https://um.fi/suomen-kehityspolitiikan-tavoitteet-ja-periaatteet, referred to on 22 July 2020.
Ministry for Foreign Affairs Sanctions against terrorism. Available in Finnish: https://um.fi/terrorismin-vastaiset-pakotteet, referred to on 4 August 2020.
Ministry for Foreign Affairs Misuse is addressed. Available in Finnish: https://um.fi/vaarinkayttoon-puututaan, referred to on 23 July 2020 and 17 March 2021.
UNODC: Money-Laundering and Globalization. Available in Finnish: https://www.unodc.org/unodc/en/money-laundering/globalization.html, referred to on 4 August 2020.
Ministry of Finance: Valtiovarainministeriön hanke – Hallituksen esitys rahanpesun ja terrorismin rahoittamisen estämisestä annetun lain muuttamisesta [*Ministry of Finance project – Government Proposal for amending the Act on Preventing Money Laundering and Terrorist Financing*]. Available in Finnish: https://vm.fi/hanke?tunnus=VM015:00/2020, referred to on 5 August 2020.
Veikkaus Ltd: Pelipaikat ja pelit [Gaming locations and games]. Available in Finnish: https://www.veikkaus.fi/fi/yritys#!/yritystietoa/pelipaikat-ja-pelit, referred to on 2 November 2020.
Veikkaus Ltd: Press release 28 August 2020: Casino Tampere avautuu joulukuussa 2021 – Veikkauksen kasinoilla edellytetään jatkossa tunnistautumista [*Casino Tampere to be opened in December 2021 – gaming at Veikkaus' casinos will be made subject to authentication*] Available in Finnish: https://www.veikkaus.fi/fi/yritys#!/article/tiedotteet/yritys/2020/08-elokuu/28_casino-tampere-avautuu-joulukuussa-2021, referred to on 2 November 2020.
World Health Organization: Coronavirus disease (COVID-19 pandemic). Available: https://www.who.int/emergencies/diseases/novel-coronavirus-2019, referred to on 7 August 2020.
Yle News 5 April 2020: Suomessa kaupitellaan nyt olemattomia hengityssuojaimia – Koronapandemia pitää rötöstelijätkin kotona, mutta nettirikolliset aktiivisina. [*Non-existent face masks are now being sold in Finland – Coronavirus pandemic is keeping of- fenders at home but online criminals active*.] Available in Finnish: https://yle.fi/uutiset/3- 11288563?utm_source=twitter-share&utm_medium=social, referred to on 9 November 2020.

Appendix 1: Methodology

The methodology used in the national risk assessment is based on the FATF guidelines on the stages of risk assessment (identification, analysis and evaluation). The risk assessment was produced using qualitative and quantitative data, which was analysed together and which formed the basis for an overall risk picture. Surveys among the authorities, workshops and interviews with experts and private sector actors were carried out as part of the risk assessment.[376] Data in the possession of the Financial Intelligence Unit and a variety of national and international publications were also used. Statistical information for the work was provided by such parties as the Financial Intelligence Unit, Legal Register Centre, Statistics Finland, Office of the Prosecutor General, National Land Survey of Finland and Finnish Customs.

The definition of the risk sectors was formulated using legislation, expert opinions and the risk sector division presented in the supranational risk assessment of the EU. The sectors are based on the categories of obliged entities falling within the scope of the Anti-Money Laundering Act. Usability of the sectors in the national context is a key feature of the sectoral division used in Finland's national risk assessment. The aim is to ensure that the division also supports the needs of obliged entities and supervisory authorities. Descriptions of the sectors' national reference framework (operating environment) are based on the information provided by the supervisory authorities and national publications and statistics. In the description of the operating environment, the focus was on the size of the sectors, actors and typical features.

The division into phenomena used in the risk assessment was based on the phenomena examined in the 2019 supranational risk assessment of the EU, phenomena highlighted by FATF and the national phenomena associated with money laundering and terrorist financing identified by experts. The working group also used Finnish and international publications to keep up to date with the latest developments.

A risk consists of threats and vulnerabilities. The risks reviewed in the risk assessment may, however, also be weighted towards threats or vulnerabilities. As already stated above, consequences are not discussed in Finland's national risk assessment. Sectorspecific **risk levels** were formulated using risk forms and a risk matrix. The risk forms listed the most significant

376 Surveys and the workshops were mainly intended for the members of the risk assessment group and their organisations. The working group also included experts from the following bodies: Ministry of Finance, Ministry of the Interior, Ministry of Justice, Ministry for Foreign Affairs, Ministry of Social Affairs and Health, Ministry of Economic Affairs and Employment, Financial Intelligence Unit of the National Bureau of Investigation, Finnish Security and Intelligence Service, National Police Board, Gambling Administration of the National Police Board, Finnish Patent and Registration Office, Finnish Customs, Finnish Tax Administration, Regional State Administrative Agency for Southern Finland, Financial Supervisory Authority, Office of the Prosecutor General and the Finnish Bar Association. Experts from the European Institute for Crime Prevention and Control, Finnish Border Guard and the National Enforcement Authority also took part in the workshops.

risks for each sector, which were assessed from the viewpoint of seriousness and probability. The risks facing the sector as a whole were assessed in the risk matrix from the perspective of threats and vulnerabilities. Using the risk forms and the risk matrix, respondents were able to assess each risk and the overall risk level in the sector on a scale of 1-4. The scale is based on the supranational methodology of the EU in which 1=less significant risk, 2=moderately significant risk, 3=significant risk and 4=very significant risk. The risk matrices and the risk forms were sent to the key authorities responsible for the prevention of money laundering and terrorist financing, to the supervisory authorities referred to in the Anti-Money Laundering Act, and private sector actors. The number of respondents in each sector and their subjective views on the level of the expertise were considered in the definition of the risk levels.

Main points of the risk assessment methodology:

1. Identifying threats and vulnerabilities. Known and potential criminal methods, criminal actors and vulnerabilities for each sector examined in the risk assessment and, if necessary, for phenomena.

2. Assessing the significance of threats and vulnerabilities in the risk matrix. Key risk criteria in each sector were assessed using a four-point scale (less significant, moderately significant, significant and very significant). The risk criteria for matrix threats were as follows:

- capacity (actors' preparedness and capabilities as parameters)
- number (number of actors as parameter) and
- extent (prevalence as parameter)

Significance of vulnerabilities and threats was assessed in the same manner. Key risk criteria in each sector were assessed using a four-point scale (less significant, moderately significant, significant and very significant). The risk criteria for matrix vulnerabilities were as follows:

- attractiveness (anonymity and speed as parameters)
- likelihood of charges and punishment (possibility of charges and punishment as parameters)
- legislative framework and supervision (timeliness of the legislation, understanding of AML/CFT process in the sector and AML/CFT cooperation as parameters), and
- chance to detect (cross-border activities and rate of development in the sector as parameters)

Risk matrices for money laundering and terrorist financing were treated separately. Absence of the vulnerability concerning the likelihood of charges and punishment from the terrorist financing matrix constituted the practical difference between the two matrices.

3. Assessing risks in the risk forms. The key risks of each sector were listed on the assessment forms on the basis of identified threats and vulnerabilities. The risks were assessed using a four-point scale, with emphasis on seriousness and likelihood (less significant, moderately significant, significant and very significant).

4. Determining risk level for each sector using the matrix as a basis. A risk level was determined for each combination of threat and vulnerabilities. This was produced using a matrix in which the vulnerabilities had a slightly higher weight (60%) than threats (40%).

5. Determining risk level for each sectoral risk on the basis of risk forms.

6. Need for action. The measures to mitigate risks are presented in the action plan prepared in connection with the risk assessment.

The purpose of the national risk assessment is not to discuss the precise societal or economic impacts of money laundering and terrorist financing as these are in any case negative, and there is currently not enough background material available for a comprehensive evaluation of the consequences. Other Nordic countries have not included the assessment of the significance of the consequences in their risk assessment.

Figure 7. Methodology for national risk assessment for money laundering and terrorist financing.

The methodology is described as a circle because even though the risk assessment is an evolutive process, its updating potential and repeatability as well as obligatory risk assessment stages have been considered in the development of the methodology.

Appendix 2: Sectors and phenomena examined in the national risk assessment

Image 1. Sectors examined in the national risk assessment of money laundering and terrorist financing.

Sectors examined in the risk assessment
Insurance companies
Payment service providers
Gambling operators
Credit institutions
Financial institutions, other providers of financial services and debt collectors
Virtual currency providers
Expert services
1. Real estate brokerage agencies and letting agencies
2. Attorneys-at-law and other providers of legal services Providers of tax advisory services or parties providing tax- related support directly or indirectly
3. Bookkeepers and auditors
4. Providers of business services
5. Pawnbrokers
6. Art dealers

Image 2. Phenomena examined in the national risk assessment of money laundering and terrorist financing.

Phenomena examined in the risk assessment
Cash as a payment method
Trafficking in human beings
Legal persons
Covid-19 pandemic
Weapons of mass destruction
New risk areas identified in the 2019 supranational risk assessment of the EU
a. Professional football
b. Free ports
c. Investor citizenship and residence schemes

Appendix 3: Questionnaire template sent to NPOs

1. Millä tasolla arvioitte rahanpesun ja terrorismin rahoittamista koskevan riskitietämyksenne olevan?
What level do you consider your knowledge of the risks associated with money laundering and terrorist financing to be?

2. Mihin rekisteriin/rekistereihin ilmoitatte tietojanne?
Which register/registers do you report to?

3. Missä roolissa olette organisaatiossanne?
What is your role in your organisation?

4. Mitä toimintaa organisaationne pääasiallisesti harjoittaa?
What is your organisation's main activity?

5. Mikä on organisaationne oikeudellinen muoto?
What is the legal structure of your organisation?

6. Mikä on organisaationne vuosittainen liikevaihtonne?
What is the annual revenue of your organisation?

7. Millä alueella organisaationne sijaitsee?
Where is your organisation located?

8. Millä alueella organisaationne toimii?
In which area/region your organisation operates?

9. Kuuluuko toimintaanne varojen siirtoa ulkomaille?
Does your organisation send funds overseas?

10. Millaiseksi arvioisit terrorismin rahoittamisen riskin…
How would you rate TF-risk…

	1 – Low risk	2 – Medium risk	3 – High risk	4 – Very high risk
…toimialallasi? / *In your sector?*	O	O	O	O
…organisaationne toiminnassa? / *in your organisations activity?*	O	O	O	O

11. Millaiseksi arvioisit rahanpesun riskin…
How would you rate ML-risk?

	1 – Low risk	2 – Medium risk	3 – High risk	4 – Very high risk
…toimialallasi? / *In your sector?*	O	O	O	O
…organisaationne toiminnassa? / *in your organisations activity?*	O	O	O	O

12. Millaisia ovat rahanpesun ja terrorismin rahoittamisen riskiskenaariot toimialallanne?
What are the main ML/TF-risk scenarios in your field of activity?

MINISTRY
OF FINANCE

MINISTRY OF FINANCE
Snellmaninkatu 1 A
PO BOX 28, 00023 GOVERNMENT
Tel. +358 295 160 01
financeministry.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-267-3 (pdf)

May 2022