

RISK ASSESSMENT RELATING TO MONEY LAUNDERING AND THE FINANCING OF TERRORISM

DECEMBER 2023



NCIP

National Commissioner
of the Icelandic Police

1. PREFACE	4
2. MAIN CONCLUSIONS	8
2.1. RISK CLASSIFICATION OF ASSESSMENT FACTORS	12
3. INTRODUCTION	14
3.1. ICELAND TODAY	15
3.2. LEGAL ENVIRONMENT AND MONITORING	19
3.3. MAKING OF THE RISK ASSESSMENT	27
3.3.1. METHODOLOGY	28
4. MONEY LAUNDERING	32
4.1. TAX FRAUD AS PREDICATE OFFENCE OF MONEY LAUNDERING	40
4.2. CASH AND CRYPTO-ASSETS	47
4.2.1. CASH – TRANSPORT TO AND FROM ICELAND	49
4.2.2. CASH TRANSACTIONS	53
4.2.3. CASH IN CIRCULATION, LARGE BILLS	57
4.2.4. CRYPTO-ASSETS	60
4.3. FINANCIAL MARKET	65
4.3.1.1 ID NUMBERS FOR FOREIGN CITIZENS	69
4.3.2. DEPOSIT-OPERATIONS	71
4.3.3. LOAN OPERATIONS	73
4.3.3.1 SIMULATED CONTRACTS	75
4.3.4. PAYMENT SERVICES	76
4.3.5. REMITTANCES	80
4.3.6. FOREIGN EXCHANGE TRANSACTIONS WITH CASH	82
4.3.7. ISSUE OF ELECTRONIC MONEY	85
4.3.8. TRADE AND SERVICES WITH CRYPTO-ASSETS	87
4.3.9. TRADE AND SERVICES FOR FINANCIAL INSTRUMENTS	90
4.3.10. OPERATION OF FUNDS	93
4.3.11. OPERATION OF PENSION FUNDS	95
4.3.12. LIFE INSURANCE OPERATION	97
4.3.13. DIGITAL FINANCIAL SERVICES MONITORED BY OTHER STATES	98

4.4. SPECIALISTS	102
4.4.1. ATTORNEYS	104
4.4.2. ACCOUNTANTS	108
4.4.3. BOOKKEEPERS	111
4.4.4. ESTATE AGENTS AND REAL ESTATE BUSINESS	114
4.4.5. SHIP BROKERS	118
4.4.6. CAR DEALERSHIPS, CAR DEALERS, AND VEHICLE TRANSACTIONS	120
4.4.7. JEWELLERS AND GOLD-BUYERS, PRECIOUS METALS AND GEMS	122
4.4.8. ART DEALERS AND ART BROKERS, ART OBJECTS MARKET	124
4.5. GAMBLING	127
4.5.1. LOTTO	129
4.5.2. LOTTERIES	131
4.5.3. SWEEPSTAKES	133
4.5.4. GAMING MACHINES – SLOT MACHINES AND LOTTERY MACHINES	135
4.5.5. GAMBLING ON THE INTERNET – FOREIGN OPERATORS	138
4.6. COMPANY OPERATIONS	141
4.6.1.1. BENEFICIAL OWNER	146
4.6.2. PRIVATE LIMITED COMPANIES	153
4.6.3. LIMITED COMPANIES, LIMITED PARTNERSHIPS, AND SELF-GOVERNING INSTITUTIONS	155
4.6.4. OTHER COMPANIES WITH A FINANCIAL PURPOSE	155
4.6.5. NON-GOVERNMENTAL ORGANISATIONS AND ORGANISATIONS	156
4.6.6. NON-PROFIT ORGANISATIONS	158
4.6.6.1. RELIGIOUS AND LIFESTYLE ASSOCIATIONS	158
4.6.6.2. FUNDS AND ORGANISATIONS OPERATING UNDER A CERTIFIED CHARTER	161
4.6.6.3. OTHER NON-PROFIT ORGANISATIONS	163
5. TERRORIST FINANCING	166
5.1.1. TRANSPORT OF CASH ACROSS BORDERS	171
5.1.2. TRANSPORT OF ASSETS TO AND FROM ICELAND THROUGH THE FINANCIAL SYSTEM	173
5.1.3. TRANSPORT OF ASSETS TO AND FROM ICELAND BY MONEY REMITTANCES	175
5.1.4. TERRORIST FINANCING, OPERATION OF NON-PROFIT ORGANISATIONS ACROSS BORDERS	177
6. LIST OF THE MOST IMPORTANT ABBREVIATIONS	180
7. SOURCES	181
8. APPENDIX	186
8.1 RISK CLASSIFICATION OF ASSESSMENT FACTORS – COMPARISON	186

1. PREFACE

This risk assessment of money laundering and terrorist financing for Iceland is the fourth one to be published. The first risk assessment for Iceland was issued in 2017, and since then it has been updated twice, in the years 2019 and 2021. The risk assessment involves the re-examination and update of the risk assessment of 2021, which was issued that year in March.

The history of the risk assessment goes back to September 1991, when Iceland entered into collaboration with the Financial Action Task Force (FATF) which is an international action group against money laundering and terrorist financing. This task force has issued recommendations on the measures member states shall take in response to the threat stemming from money laundering and terrorist financing. The task force's 40 recommendations have become global guidelines. Amongst other things, the European Union's (EU) directives have been in accordance with these guidelines.¹ By joining FATF, Iceland has obliged itself to coordinate its legislation with the task force's recommendations.

Following the FATF's evaluation of Iceland's defences against money laundering and terrorist financing in 2017–2018, which revealed various weaknesses in the Icelandic legislation regarding this, Iceland began working on its response, which entailed, amongst other things, implementing the European Union's Fourth Anti-Money Laundering Directive. In accordance with the requirements that may be inferred from FATF Recommendation no. 1, it is assumed in the aforementioned directive that all member states shall carry out a risk assessment of the main threats and weaknesses stemming from money laundering and terrorist financing within the areas each member state controls. Such risk assessment is fundamental when it comes to assessing whether anti-money laundering and anti-terrorist financing measures are adequate. The obligation to carry out a risk assessment in this country was introduced by Article 4 of the Act on Measures against Money Laundering and

¹ *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations.* FATF, Paris 2023.

Terrorist Financing, no. 140/2018 (the AML Act.) Under the provision, the National Commissioner of the Icelandic Police (NCIP) sees to the preparation of the risk assessment that must be updated every two years, or more often if needed. Since the publication of the last risk assessment, various things have happened in Iceland regarding this issue category. One could say that the beginning is traceable to the serious deficiencies in Iceland's defences that emerged in FATF's mutual evaluation report published in April 2018.² Major improvements were made here in Iceland since the draft of the report became available at the start of 2018. The improvements were based on the close cooperation of many governmental units and institutions that accomplished a Herculean task in dealing with these matters. Then again, in October 2019, FATF decided to place Iceland on its "grey list" of states deemed to have unsatisfactory defences against money laundering and terrorist financing. Work began immediately to get Iceland off this list. For this purpose, the Minister of Justice and the Minister of Finance and Economic Affairs launched preparations for a report on what led to Iceland ending up on FATF's "grey list."³ and the reasons for this. Iceland stayed on the FATF's list for one year, until October of 2020.

This risk assessment is a step in fulfilling Iceland's obligations to fulfil FATF's standards in this regard. The intention, therefore, is to provide a comprehensive analysis of the existing risk of money laundering and terrorist financing in Iceland. Amongst other things, it entails an assessment of the known markets and operations that may be particularly exposed to such risk. It is anticipated that the risk assessment will be utilised by not only the Icelandic government but also other parties with stakes in defending against money laundering and terrorist financing.

The risk assessment is prepared in accordance with the methodology on which FATF builds its instructions for such assessments, with one proviso: The methodology is not intended as a general template for preparing for such risk

² Mutual Evaluation Report of Iceland. FATF, Paris 2018.

³ Report of the Minister of Justice and the Minister of Finance and Economic Affairs on what led to Iceland ending up on FATF's "grey list". Ministry Offices, Reykjavík 2019.

assessments when it comes to either money laundering or terrorist financing.⁴ More precisely, the methodology entails flexibility and efficiency to consider the circumstances in each country. In essence, the methodology entails first analysing the threats and weaknesses related to money laundering and terrorist financing before analysing the nature, magnitude, and likelihood of money laundering and its possible consequences, as well as an assessment of necessary measures to reduce risk that may exist.

The risk assessment has provided governmental authorities and other stakeholders with a powerful weapon against money laundering and terrorist financing. It lays the epistemic foundation necessary to enable the analysis and understanding of the problem being addressed and thus ensuring that the existing defences are as powerful and efficient as possible. It is also assumed that the risk assessment will be utilised to not only directly improve defences against money laundering and terrorist financing but also for other purposes like allocating and prioritising funds, disseminating information, and general prevention of risk and crime.

In accordance with the declared policy of the government in this policy area, a steering committee against money laundering and financing of terrorism headed by the Minister of Justice will prepare a plan of action following the publication of the risk assessment, where advice will be given regarding how to confront the risk and mitigate the weaknesses which became evident at its preparation.

⁴ FATF Guidance. National Money Laundering and Terrorist Financing Risk Assessment. FATF, Paris 2013.

2. MAIN CONCLUSIONS

Risk factors from money laundering are divided into the following categories within the risk assessment; *money laundering predicate offences, cash and crypto-to-assets, financial market, specialists, gambling, and the operation of companies*. Terrorist financing is subdivided into four assessment factors. Several changes have occurred within this policy area in the space of more than two years since the publication of the previous risk assessment. Few changes have occurred, however, to the risk classification of assessment factors. The main conclusions of the risk assessment relating to money laundering and terrorist financing are as follows:

MONEY LAUNDERING PREDICATE OFFENCES

Tax fraud is still considered the most common form of money laundering in Iceland and the analysed risk thereof is deemed very high. Offences related to the misuse of the VAT-system, for instance with the use of bogus invoices, are systemic and extensive. Several changes have been made in the preceding years to counter this, for example, to the organisation of investigations and prosecution of tax law violations and laws regarding income tax and value added tax. The task force appointed by the Minister of Finance and Economic Affairs also submitted various proposals for actions to counter the misuse of the tax system earlier in the year and they are worth considering.⁵

CASH AND CRYPTO-ASSETS

Cash and its use is, as ever, deemed the most severe single risk factor of money laundering in this country, as well as elsewhere in the world. Iceland has no restrictions on the use of cash. Cash can be used for payment almost anywhere and its use is poorly monitored. Smuggling cash to and from this country is deemed easy, while a few cases involving transport of cash across borders have come under the investigation of the Directorate of Customs in recent years. Monitoring of the transport of cash to and from the country is insufficient and legal remedies are to

⁵ *Issuance of Bogus Invoices - The Nature of the Behaviour and Possible Scope - Proposals for Actions*. The Ministry of Finance and Economic Affairs, Reykjavik 2023.

some extent limited. The analysed risk from *cash transactions and the transport of cash to and from Iceland* is deemed very high.

The use and skill of offenders in laundering the profits of illegal activities with crypto-assets is increasing. Also, crypto-assets are a common means of payment for illegal goods and services. The most recent risk assessment of the EU considers the money laundering risk of crypto-assets very high for the first time.⁶ The scope of crypto-assets in Iceland is not known but surveys suggest that Icelanders trade in crypto-assets as much as other European states do. Also, there are indications that offenders in this country have begun allocating profits from criminal activities into purchasing crypto-assets. The lack of necessary equipment, protocols and expertise to investigate cases related to *crypto-assets* within the Financial Intelligence Unit (FIU,) police, and other monitoring agencies is a weakness, and the risk from crypto-assets is deemed very high.

FINANCIAL MARKET

Within the previous risk assessment, the risk of *money remittances* is considered very high. However, the scope of this activity has significantly decreased as monitoring has been increased and, therefore, the analysed risk of money remittances is deemed high at this time. Risk related to *deposit operations, payment services, foreign exchange transactions with cash, issue of electronic money, and transactions and services with crypto-assets* is also deemed high, while the risk of the latter assessment factor is considered to have increased concurrently with the increased use of crypto-assets and risk related thereto. For the first time the risk of *digital financial services accessible in Iceland while subject to monitoring by other states* is assessed, where the operators aren't parties subject to mandatory reporting in this country. This assessment factor involves very diverse services, such as digital banks and other financial technology services. As in the case of crypto-assets, the scope and use of this service by Icelanders is not known, oversight is limited, and the FIU receives very few reports regarding it. Also, there are indications that offenders in this country have been using these financial technology services and the risk is on the whole deemed high.

SPECIALISTS

The risk assessment considers various groups of specialists who are subject to mandatory reporting according to the AML act. Amongst other things, the focus will be on whether their services are misused for money laundering purposes, regardless of whether or not the specialists are aware of it. As in the previous risk assessment, risk related to *attorneys, accountants, and car salesmen* is deemed high. The same applies to the profession of *real estate agents*, as the risk assessment also emphasises real estate business in general, regardless of the participation of the real estate agent, as there are indications that profits from criminal activities

⁶ *Supra-National Risk Assessment Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. SWD(2022)/554. EU, Brussels 2022, pg. 101.*

in this country tend to be laundered through real estate transactions. Art sellers are assessed for the first time, and the risk related to them is deemed medium.

GAMBLING

Of the forms of gambling permitted in Iceland, the greatest risk is related to *slot-machines*. In the previous risk assessment it was deemed very high but considering increased monitoring and more extensive defences by operators, it is now deemed high. There are plans for changes to laws related to slot-machines, geared towards reducing the risk and reacting to the discussion in the previous risk assessment, and it is important that those legal amendments succeed. In the risk assessment, the risk from *gambling on the internet operated by foreign operators* are also assessed, and within the current risk assessment of the EU, the risk of online gambling is deemed very high for the first time.⁷ The access of consumers in Iceland to foreign gambling forums online are not subject to any restrictions and domestic monitoring is limited. The extent of participation in gambling on such websites among individuals residing in this country is considered significant, and the risk of online gambling is deemed high.

COMPANY OPERATIONS

As before, *private limited companies* are the company form most commonly used to launder unlawfully acquired gains and to conceal beneficial ownership. Analysed risk from private limited companies is still considered very high. Many methods which offenders use to launder money through companies have been left unrestricted in Iceland, seemingly permitted by a certain culture and lack of monitoring, legal resources, and penalties. Several things have been done in recent years to try to prevent misuse of companies. For example, laws were enacted in 2019 on the registration of beneficial ownership, and several laws have been amended in the aim of preventing ID number-hopping, for example, with an operational ban. The effects of these changes have yet to fully emerge and it's clear that, in order to curb misuse of companies for money laundering purposes, more actions will be required.

TERRORIST FINANCING

In September 2022, the police announced an investigation into an alleged terrorist offence, the first investigation and charge of terrorism in Iceland. No confirmed cases have emerged in this country related to terrorist financing. The risk of terrorist financing is assessed through four assessment factors this time, whereof three are new; transport of cash across borders, transport of assets to and from Iceland through the financial system, and transport of assets to and from Iceland by money remittances. Analysed risk is deemed medium for those risk factors and low for risk from the operation of non-profit organisations across borders.

⁷ *Supra-National Risk Assessment Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. SWD(2022)/554. EU, Brussels 2022, pg. 236.*

2.1. RISK CLASSIFICATION OF ASSESSMENT FACTORS

The conclusions of risk classification of the assessment factors examined during the preparation of the risk assessment can be seen in the summary below. In the appendix, the conclusions of risk classification for the years 2019 and 2021 may be seen in comparison. A thorough discussion of each assessment factor may be seen in the following sections.



MONEY LAUNDERING

Money laundering predicate offences	2023
Tax fraud as predicate offence of money laundering	
Cash and crypto-assets	
Cash – transport to and from Iceland	
Cash transactions	
Cash in circulation, large bills	
Crypto-assets	
Financial market	
Deposit operations	
Loan operations	
Payment services	
Remittances.	
Foreign exchange transactions with cash	
Issue of electronic money	
Trade and services with crypto-assets	
Trade and services for financial instruments	
Operation of funds	
Operation of pension funds	
Life insurance activity	
Digital financial services monitored by other states	

Specialists	2023
Attorneys	Orange
Accountants	Orange
Bookkeepers	Yellow
Estate agents and real estate transactions	Orange
Ship brokers	Green
Car dealerships, car dealers and vehicle transactions	Orange
Jewellers and gold-buyers, precious metals and gems	Yellow
Art dealers and art brokers, art objects market	Yellow
Gambling	
Lotto	Green
Lottery	Green
Sweepstakes	Yellow
Gaming machines – slot machines and lottery machines	Orange
Gambling on the internet – foreign operators	Red
Operation of companies	
Private limited companies	Red
Limited liability companies, limited partnerships, and self-governing institutions	Yellow
Other companies with a financial purpose	Green
General associations and NGOs	Orange
Religious and lifestyle associations	Orange
Funds and associations operating under a certified charter	Orange
Other non-profit organisations	Yellow
Terrorist financing	
Transport of cash across borders	Yellow
Transport of assets to and from Iceland through the financial system	Yellow
Transport of assets to and from Iceland by money remittances	Yellow
Non-profit organisations operating across borders	Green

3. INTRODUCTION

3.1. ICELAND TODAY

In recent years, several things have occurred in the international arena which affect Icelandic society and actions to counter money laundering and terrorist financing. Primarily, the Covid-19 pandemic, the invasion of Ukraine, and the increased danger of climate change. Also, great changes have occurred within the fields of technology and science, and the fourth industrial revolution is constantly becoming actualised, as witnessed by, amongst other things, huge progress in the fields of artificial intelligence and high-speed cellular and internet networks.

NATIONAL COMPOSITION

According to Statistics Iceland, 394,200 people lived in Iceland at the end of July 2023,⁸ and population growth has been great in Iceland in recent years. In the year 2022, the population grew by 11,510, or by 3.1%, which is the greatest increase in one year as far back as population numbers for Iceland go.⁹ The population increase in the year 2023 is thought to be even greater, with the inhabitants of the country exceeding 400,000 by the end of the year.¹⁰ The average age of the nation was 38.4 years in 2021.¹¹

The great population increase is attributable to immigrants and a natural increase in the population within the nation. By the middle of the year 2023, foreign citizens numbered 70,540, or about 18% of the total population, and the ratio has grown in recent years. The ratio of immigrants working in the Icelandic labour market has quadrupled from the year 2003, rising to just over 20% in the year 2022.^{12, 13} Considering the uncertainty in the world today, i.e. wars and refugee crises, it's considered likely that the number of foreign citizens seeking to settle down and/or work in this country will continue to rise in the near future.

Of the total population within the country, most live in the greater Reykjavík area. In the beginning of 2023, just under 63% lived in the greater Reykjavík area, i.e. the continuously inhabited area between Hafnarfjörður to Mosfellsbær. Just under 6% lived within the second most populated area, Keflavík and Njarðvík, and just over 5% lived in Akureyri and its environs.¹⁴

⁸ [Population in 2. quarter 2023 – Statistics Iceland](#)

⁹ [Population 1. January 2023 – Statistics Iceland](#)

¹⁰ [Monthly report of the economics department of HMS for August 2023 | Housing and construction authority](#)

¹¹ [Average age of Icelanders 1841–2021 by Year and Gender. PxWeb \(hagstofa.is\)](#)

¹² [Population in 2. quarter 2023 – Hagstofa Íslands](#)

¹³ [Monthly report of the economics department of HMS for August 2023 | Housing and construction authority](#)

¹⁴ [Population 1. January 2023 – Statistics Iceland](#)

SOCIAL AND FINANCIAL ISSUES

The Icelandic economy was characterised by high employment and low unemployment. In 2022, for example, employment was measured at about 80%, the proportion of the population working was about 77% and unemployment stood at about 3.7%.¹⁵ Average wages are high compared with other countries and they reflect the great wealth creation which is taking place in this country, which is the basis of the good living standards and welfare system.^{16, 17, 18} Another thing which is characteristic of Icelandic society is the widespread membership of wage-earners in trade unions and, furthermore, the fact that membership in pension funds is mandatory, cf. Act no. 129/1997.¹⁹

Iceland has its own monetary policy and its own currency, the Icelandic króna (ISK.) Because of how small it is, the króna is somewhat susceptible to fluctuations in the main markets of the country. Furthermore, unstable inflation and interest rates have been a characteristic of Icelandic society. In recent years, inflation and interests have remained at a historical low. Inflation decreased a little during the Covid-19 pandemic, but after all restrictions were lifted it rose again, concurrent with increased economic activity. By the end of the year 2019, the development of annual inflation was 1.7%, but had reached 9.6% by the end of the year 2022.²⁰ In addition to the negative economic impact of the pandemic, this great increase is attributable to the global situation, for example, the war following the invasion of Ukraine and the energy crisis in Europe. Interest rates have also risen in Iceland, along with inflation. The key interest rate of the Central Bank of Iceland (cbl) at the end of the year 2019 stood at 3%. They decreased during the first part of the year 2020, down to 0.75%, before undergoing a sharp increase up to 9.25% in September of 2023.²¹ The low interest-rate environment which was created caused an increase in debts and there was a significant shift among real estate loans from indexed loans to non-indexed loans. A great part of these non-indexed loans bear a fixed-rate of interest which will be reviewed in the years 2024 and 2025 which will then result in a greater burden of debt on loans.²² So far, an increase in the number of defaults because of increased debt burden has not been evident but in 2023, it has become evident that individuals increasingly again opt for loans of the indexed kind.²³

Within *Financial stability* from the cbl 2023/2 it is stated that the standing of the great commercial banks is strong and that the stress-test of the cbl on the one hand and that of the International Monetary Fund on the other have illustrated that the banks are very resistant to external shocks within the economy. Also, the equity ratio of the banks is high, profitability from the regular operation is good, and the number of defaults by households and companies is at a minimum.²⁴

In *Financial Matters*, a quarterly publication of the cbl from 23 August 2023,

¹⁵ [Labour market in the year 2022 – Statistics Iceland](#)

¹⁶ [Educational status – Statistics Iceland](#)

¹⁷ [Wage indexes – Statistics Iceland](#)

¹⁸ [Spotlight on the facts \(sa.is\)](#)

¹⁹ [Trade Union Dataset \(oecd.org\)](#)

²⁰ [Inflation \(sedlabanki.is\)](#)

²¹ [Key interest rate sj \(sedlabanki.is\)](#)

²² *Financial stability, 2022(2)*. cbl, Reykjavik, Volume 31. 28 September 2022, pg. 20..

²³ *Financial Stability, 2023(2)*. cbl, Reykjavik, Volume 33. 20 September 2023, pg. 17..

²⁴ *Financial Stability, 2023(2)*. cbl, Reykjavik, Volume 33. 20 September 2023, pg. 4.

it is estimated that economic growth in Iceland in 2023 will amount to 3.5% which is close to the average growth of the years 2012-2019. Also, the CBI estimates that economic growth will reach 2.5% in the years 2024 and 2025.²⁵

THE MAIN REVENUE-GENERATING INDUSTRIES

In the past few decades, the Icelandic economy has undergone considerable changes, become more diversified, and the foundations of the economy are more numerous than before. Powerful tech companies and innovation companies have emerged and made a niche for themselves in various industries within the economy. One of the consequences is that direct foreign investment in technology and innovation in Iceland have risen concurrently with the success of those companies.

Despite the success of Icelandic companies within the sector of innovation and technology, it is primarily the rapid growth of the tourism industry which has transformed the appearance and job creation of Icelandic society during the past 15 years. During the past decade, the tourism industry has become one of the main industries of the country, and foreign investors see the build-up of tourism related services in Iceland as a good option. The tourism industry recovered rapidly from the great blow which it was dealt by the Covid-19 pandemic, when the number of foreign tourists decreased from two million in 2019 to just under half a million in 2020. As early as 2022, the number of tourists had risen to just over 1.7 million. During the year 2023, the number of tourists is expected to exceed two million, and the Icelandic Tourist Board predicts that in 2025 the number will have reached almost three million.^{26, 27}

Also, the traditional industries of fisheries, farming, energy production, and heavy industry have shaped the economy of the country for some time to come and adapted to the change of the times by increased technological advances, efficiency, and steady innovation. Fisheries is one of the most important pillars of the economy in this country and jobs directly involved with fisheries have numbered between eight and nine thousand in recent years. About 98% of all Icelandic marine products are exported and sold in foreign markets, and they create a great part of the export earnings of the nation.²⁸ The third of the large revenue-creating industries is energy production and sale of electrical energy for heavy industry. Several international industrial companies operate within Iceland and use a large part of the electrical energy produced in Iceland in their operation. Pure aluminium made from Icelandic energy is exported to foreign markets where it is used for the construction industry and the vehicle industry. The Icelandic aluminium industry is one of the greatest export sectors of the country.

It's clear that the Icelandic economy is no longer exclusively based on fisheries. However, it is susceptible to fluctuations in the global market price of marine products and aluminium and access to foreign markets, in particular markets within the EU, which are crucial for Icelandic companies. The infrastructure of

²⁵ [Money Affairs, 2023\(3\). CBI, Reykjavik, Volume 93. 23 August 2023, pg. 12–13.](#)

²⁶ [Total number of foreign tourists | Icelandic Tourist Board \(ferdamalastofa.is\)](#)

²⁷ [Summary of predictions for the number of tourists | Icelandic Tourist Board \(ferdamalastofa.is\)](#)

²⁸ [Front page | Fisheries Iceland \(sfs.is\)](#)

Iceland is considered well integrated with EU legislation. For example, Iceland is a member of the European Economic Area (EEA,) the Schengen area, and the European Free Trade Association (EFTA.) A large part of the legal framework of the EU has been implemented in Iceland, and Iceland participates, admittedly without a right to vote, in the operation of several organisations and plans of the EU, including the field of commerce, economic matters, education, and research. Two thirds of the external trade of Iceland is with the member states of the EU.²⁹

ICELAND IN COMPARISON WITH THE INTERNATIONAL MARKET

If one examines Icelandic society through the lens of international standards, it is evident that Iceland rates high when it comes to quality of life, equality, security and technological advances.

- Iceland came in third place with regard to the UN Human Development Index in September of 2023. The index measures the likelihood of survival from birth, the proportion of those considered literate among adults, the proportion of inhabitants engaging in studies on all education levels, and quality of life measured in gross domestic product and purchasing power in American dollars.³⁰
- According to the findings of the World Economic Forum (WEF) in 2023, no place in the world was found to have more gender equality than Iceland and Iceland came in first for the 14th year in a row. The standards on which the assessment of the WEF is based involves measurements of four societal factors related to gender equality in the fields of health, education, economy and politics.³¹
- The Icelandic economy has long been open to technological advances and has increasingly made use of the innovations characteristic of the fourth industrial revolution. According to the data of The World Bank, Iceland had 100% internet coverage and cellular phone subscriptions numbered 457 thousand in the year 2022, i.e. about 123% of the population.^{32,33}
- According to the *Global Peace Index*, Iceland was the most peaceful and secure state in the world in 2023 and has been at the top of the list since the index was first created in 2008.³⁴ A rather low crime rate and low rate of riots and violent protests contribute significantly to that status.
- Finally, corruption has usually been found to be quite low in this country. According to *Transparency International*, Iceland came in 14th place of countries with the least corruption in 2022.³⁵

²⁹ [Iceland \(europa.eu\)](https://europa.eu)

³⁰ [Human Development Index | Human Development Reports \(undp.org\)](https://data.undp.org/)

³¹ *Global Gender Gap Report 2023 – Insight report*. World Economic Forum, Cologne/ Geneva 2023, pg. 27.

³² [Individuals using the Internet \(% of population\) – Iceland | Data \(worldbank.org\)](https://data.worldbank.org/)

³³ [Mobile cellular subscriptions \(per 100 people\) – Iceland | Data \(worldbank.org\)](https://data.worldbank.org/)

³⁴ *Global Peace Index 2023: Measuring Peace in a Complex World*. Institute for Economics & Peace, Sydney 2023, pg. 2.

³⁵ [2022 Corruption Perceptions Index: Explore the... – Transparency.org](https://www.transparency.org/)

3.2. LEGAL ENVIRONMENT AND MONITORING

FATF

The international action group FATF was established in July 1989 at a summit meeting of the seven main industrial states of the world in Paris. The organisation was founded for the purpose of preparing measures to prevent the misuse of the financial system to get ill-gotten money into circulation. In 2001, the organisation stepped up its battle against terrorist financing by adding it to its project list following the terrorist acts in the United States of America on 11 September of that year. Related to the implementation of UN Security Council Resolutions in 2007, the organisation also began combating the financing of weapons of mass destruction.

The role and field of the FATF has, with regard to its main policy, been divided into three parts. Firstly to prepare standards for the actions of member states against money laundering and terrorist financing. Secondly, to assess the actions of individual states in implementing these standards and, thirdly, to investigate and familiarise themselves with the methods of those who launder money and finance terrorism. Based on this, the FATF has prepared recommendations to its member states on actions to combat money laundering and the financing of terrorism.

The FATF conducts inspections of the legislation, regulations and efficiency of each member state and issues reports regarding their actions. Wherever appropriate, the organisation's member states have agreed to pressure one another by placing individual states on a special list over so-called uncooperative states if they fail to fulfil the requirements set by the organisation. Such pressure can also involve stricter requirements of those states or entities who reside there, regarding financial instruments or issuing warnings that engaging in business with entities within those states may involve risk of money laundering.

LEGAL FRAMEWORK

Act no. 64/2006 on Measures against Money Laundering and Terrorist Financing legalised the third Directive of the EU no. 2005/60/EC. Previously, Act no. 80/1993

on the same matters had been in force. The act was drafted for the purpose of adapting Icelandic legislation to the Directive of the Council of the European Union no. 91/308/EEC on anti-money laundering measures. However, that was amended following a re-examination and amendments to the above directive with the European Union's Directive no. 2001/97/EU. The European Union's fourth anti-money laundering and anti-terrorist financing directive no. 2015/849/EC was legalised in this country with the Act on Measures against Money Laundering and Terrorist Financing no. 140/2018 that entered into force on 1 January 2019. The act also adopted selected provisions from the fifth anti-money laundering Directive of the European Union no. 2018/843/EC. Several minor changes were made to the Act on Measures against Money Laundering and Terrorist Financing since it entered into force, in response to, amongst other things, the comments of the ESA, the EFTA Surveillance Authority, which conducted an assessment of the implementation at the end of the year 2019. Also, laws have been amended to respond to later changes to the recommendations of the FATF, to coordinate them with changes to other domestic laws and to make to laws clearer after their enforcement has been tried.

Iceland now has a comprehensive and developed statutory and regulatory scheme addressing money laundering and terrorist financing. The regulatory scheme is intended to prevent money that was possibly obtained unlawfully from entering into circulation in the traditional financial system or being used for financing terrorism.

According to Article 1 of the AML Act, the aim of the act is to prevent money laundering and terrorist financing by obligating parties engaging in operations that may be used for money laundering or terrorist financing to know their customers and their operations and notify the competent authorities if their suspicion is aroused, or they become aware of such unlawful operations. Accordingly, the act applies to parties subject to mandatory reporting under the act and defined as such. The act imposes duties on these parties, including instructions regarding the duty to:

- Carry out a risk assessment on operations and transactions.
- Have a documented policy, controls and processes to reduce and control risk stemming from money laundering and terrorist financing.
- Investigate their customers' reliability in defined instances.
- Have an appropriate system, processes, and procedures to evaluate whether a domestic or foreign customer or beneficial owner (BO) falls into a risk group because of political ties.
- Notify the Financial Intelligence Unit (FIU) of suspicious transactions.

The act also provides that, in instances defined in more detail, it is forbidden to:

- Offer anonymous transactions.
- Participate in or promote transactions intended to conceal beneficial ownership.
- Initiate or continue transactions with shell banks.

The act also prescribes the drafting of a risk assessment, reports of transactions to the FIU and analysing of the reports, procedure of entities subject to mandatory reporting and training of their employees, monitoring of defined supervisors under the act, as well as coercive remedies and penalties for violations of the act and regulations set under it.

MONEY LAUNDERING

A provision of Article 264 of the General Penal Code (GPC) no. 19/1940 defines money laundering as punishable. Under Paragraph 1 of the provision, whoever accepts, utilises, or otherwise benefits from an offence under the act, or from a criminal offence under another act, or converts such benefit, transports it, sends, stores, or assists in delivering it, conceals it or information on its origin, nature, location, or disposition shall be sentenced to imprisonment for up to 6 years. Under Paragraph 2 of the provision, someone who has committed a predicate offence and also commits an offence under Paragraph 1 of the provision shall be sentenced to the same punishment as the rules of the act on determining punishment regarding two or more offences apply, as relevant. This then involves “self laundering,” i.e. when the same individual commits a predicate offence of money laundering and a money laundering offence. Also, offences which occur within Icelandic borders are punishable according to Article 264 of the act even if the predicate offence which yielded the profit was committed abroad, and without consideration of who was responsible for it.

The wording of the provision, as amended in 2009, looked to Article 6 of the United Nations' Convention against Transnational Organized Crime, approved by the General Assembly of the United Nations on 15 November 2000 and signed by the Icelandic State on 13 December that year. Also, the provision's drafters considered FATF's comments in its report on anti-money laundering measures in Iceland in October 2006.

The definition of money laundering in the AML Act takes note of the definition of the concept in Article 264 of the GPC. Under Icelandic law, all criminal offences under the last-specified act, or a special criminal act, can be predicate offences of money laundering. All offences leading to financial gain, such as drug offences, tax law offences, human trafficking, and theft can therefore fall

under this rule. In addition, it is deemed to be money laundering when the involvement of an individual or legal person in the handling of gains fits with the basic definition of the concept.

TERRORIST FINANCING

Under the provisions of the AML Act, terrorist financing is deemed to be when money is acquired, whether directly or indirectly, for the purpose of using it or with knowledge that it is to be used, wholly or in part, to perpetrate violations punishable under Article 100 (a. – c.) of the GPC. Under Article 100 (a) of the GPC, the punishment for terrorism shall be up to life imprisonment for someone committing one or more of the offences listed in the provision for the purpose of causing substantial public fear or unlawfully coercing the Icelandic Government or a foreign government or an international institution to do something or refrain from doing something, or for the purpose of weakening or damaging the constitutional system or political, economic, or social foundations of a state or international institution.

Article 100 (b) of the GPC also provides that anyone directly or indirectly supporting a person, organisation or group that commits or has the purpose of committing terrorist acts under provision (a) of the article, by contributing money or providing other financial support, supplying or collecting money, or otherwise making money available shall be sentenced to imprisonment for up to 10 years. Article 100 (c) provides for imprisonment of up to 6 years for supporting, in words or deeds or by persuasion, urging or otherwise supporting criminal operations or a mutual goal of an association or group that has committed one or more offences under Article 100 (a) or (b) of the GPC, and operations or goals entailing the commission of one or more such offences.

The above legal provisions have roots in amendments to the General Penal Code in 2002. These involve necessary amendments to fulfil the Icelandic State's duties under three international anti-terrorist resolutions under the auspices of the United Nations. First, this involved an international agreement from 15 December 1997 on preventing terrorist bombings. Second, this involved an international agreement from 9 December 1999 on preventing funding of terrorist activities, and third, this involved Resolution no. 1373 of the United Nations Security Council, from 28 September 2001. The amendments entailed that "terrorism" was defined in criminal law, and such deeds were deemed to be amongst the most serious offences in Icelandic law. In addition, financial support for terrorist activities was made an independent criminal offence.

RECOVERY AND SEIZURE OF UNLAWFUL GAINS

Regarding authorisation to seize gains from money laundering offences or terrorist financing, Article 69 of the GPC provides general authorisation to seize

gains from an offence or money corresponding to it, in whole or in part. The same applies to objects purchased with such gains or replacing it. In addition, when it is not possible to fully prove the amount of gain, the provision authorises estimating the amount. As examples of where the provision was applied in an indictment and conviction for money laundering, see the judgements of the Supreme Court of Iceland on 25 November 2021 in case no. 28/2021 and on 15 December 2016 in Case no. 829/2015. Both judgements also show the importance of investigating financial activities in parallel with predicate offences of money laundering.

OTHER BODIES OF LAW

Examples of other bodies of law related to the issue category include the Act on Criminal Procedure no. 88/2008. Mention must also be made of recent legislation having the goal of strengthening defences against money laundering and terrorist financing. The first is the Act on the Registration of Beneficial Owners no. 82/2019. Its purpose is to ensure that correct and reliable information on BOs of legal persons is available at all times to analyse and prevent money laundering and terrorist financing. Second comes the Act on the obligation of non profit organisations to register no. 119/2019 which stipulates the obligation of companies who distribute funds for the public good and who operate across borders to register. And third, the Act on the Implementation of International Sanctions and Freezing of Funds no. 68/2023, which prescribes the freezing of assets in line with specified sanctions to hinder terrorist financing and the scope and the proliferation and financing of weapons of mass destruction.

LAW ENFORCEMENT INSTITUTIONS AND SUPERVISORS

Numerous governmental parties have been involved in matters related to money laundering and terrorist financing. These parties either see to supervision, policy formulation, or monitoring of the implementation of the AML Act or direct the investigation and/or prosecution of such offences. Below is a review of the most important parties related to the issue category. For a more comprehensive overview, reference is made to the following organisation chart.

Steering Committee on measures against money laundering and terrorist financing: Sees to, for example, policy formulation and works on integrating measures against money laundering and terrorist financing. All authorities mentioned in this section have a representative within the steering committee.

**STEERING COMMITTEE ON MEASURES AGAINST MONEY LAUNDERING AND TERRORIST FINANCING
UNDER THE AUSPICES OF THE MINISTRY OF JUSTICE**

Figure 1



MINISTRY OF JUSTICE MOJ

Supervises the issue category, including legislation on measures against money laundering and terrorist financing. The Minister of Justice appoints a steering Committee on measures against money laundering and terrorist financing:

MINISTRY OF FOREIGN AFFAIRS MOFA

Responsible for supervision. Amongst other things, responsible for the Act on the Implementation of International Sanctions and Freezing of Funds no. 68/2023. The ministry shall, amongst other things, keep registries regarding sanctions in this country and against whom they are levied.

MINISTRY OF CULTURE AND BUSINESS AFFAIRS MOCBA

Responsible for supervision. Issues of the directory division of the Directorate of Internal Revenue are, amongst other things, handled by the Ministry. Is also responsible for the Act on the Registration of Beneficial Owners no. 82/2019 and the Act on the obligation of non profit organisations operating across borders to register no. 119/2019.

THE MINISTRY OF FINANCE AND ECONOMIC AFFAIRS MOFEA

Responsible for supervision. Issues of the cbi are, amongst other things, the responsibility of the Ministry, as is legislation regarding financial markets as a whole.

CENTRAL BANK OF ICELAND CBI

Monitors that the parties specified in Paragraph 1 (a.-j.) of Article 2 of AML Act conduct themselves in accordance with the act's provisions. This involves, for example, financial undertakings, electronic money companies and pension funds. FSA, which was previously an independent institution, is part of the Central Bank of Iceland (CBI) under provisions in the Act on the Central Bank of Iceland no. 92/2019.

ICELAND REVENUE AND CUSTOMS ALSO THE DIRECTORATE OF INTERNAL REVENUE

The agency that the Directorate of Internal Revenue and Customs operates, following the amendment of various acts with Act no. 141/2019, which entailed the merger of the Directorate of Internal Revenue and the Directorate of Customs. Iceland Revenue and Customs operates the Business Registry, Register of Annual Accounts, Register of Beneficial Owners (BO Register,) and Money Laundering Surveillance (the Money Laundering Division of the Directorate of Internal Revenue,) which monitors whether the parties specified in l to u of Paragraph 1 of Article 2 of AML Act conduct themselves in accordance with the act's provisions. This applies, amongst other things, to audit firms, law firms, real estate brokerages and car agencies. Also, the Money Laundering Division of the Directorate of Internal Revenue monitors NPOs regarding money laundering and terrorist financing under Act No. 119/2019 on the Obligation of Non-profit Organisations to Register. Finally, the Directorate of Internal Revenue supervises customs affairs and is entrusted with enforcing other laws and administrative rules regarding the importation and exportation of goods in accordance with the provisions of

Customs Act no. 88/2005. Customs Iceland is a special unit within the Directorate of Internal Revenue and Customs that sees to customs. The Customs Manager sees to the daily supervision and operation of Customs Iceland as the agent of the Directorate of Internal Revenue. On 1 May 2021, Iceland Revenue and the Directorate of Tax Investigation (DTI) merged, after an act was passed in April of that year which stipulated it. The Directorate of Tax Investigation is, therefore, no longer an independent agency but part of the division of surveillance and investigations within Iceland Revenue. The Directorate of Tax Investigations is responsible for investigations under the Act on income tax no. 90/2003 and other acts on taxes and dues under his auspices, or whose implementation is delegated to him.

FINANCIAL INTELLIGENCE UNIT FIU

Independent administrative unit within the District Prosecutor's Office. Receives notices of transactions suspected to involve money laundering or terrorist financing. Sees to the analysis of received notices, gathers necessary additional information, and disseminates analyses to competent parties.

DISTRICT PROSECUTOR'S OFFICE DPO

Exercises prosecutorial authority in cases involving terrorist offences under Article 100 (a.-c.) of the GPC and sees to investigating and prosecuting serious offences under the provisions of Article 264 of the same act related to money laundering.

POLICE

Investigate violations under the supervision of the District Prosecutor or Chief of Police. Police chiefs also file criminal cases other than those filed by the Director of Public Prosecutions or the District Prosecutor.

NATIONAL COMMISSIONER OF THE ICELANDIC POLICE NCIP

Handles police matters on behalf of the minister, based on Police Act, no. 90/1996. The National Commissioner of the Icelandic Police is also responsible for preparing national risk assessment under the AML Act and seeing to investigations related to terrorism, including the financing of terrorism.

3.3. MAKING OF THE RISK ASSESSMENT

The risk assessment is the responsibility of NCIP, which sees to its operations in broad and close consultation with the Minister of Justice's Steering Committee on measures against money laundering and terrorist financing. Preparation of the risk assessment began in September 2022. In carrying out the risk assessment, an attempt was made to consult extensively with all stakeholders. There was extensive collection of data from supervisors, law enforcement institutions, FIU, and other public law bodies. During the data collection, the reference source was the manual of the Organisation for Security and Co-operation in Europe on data collection for risk assessment regarding money laundering and terrorist financing.³⁶ Resources included available statistical information, as relevant. In addition, data collectors relied on the expertise of those involved in the issue category. During the update of the risk assessment, the primary focus was the status at the time when the risk assessment was prepared and the changes which had occurred in the issue category since the publication of the preceding risk assessment were considered. As statistical information was presented, the figures were from the years 2021 and 2022 unless otherwise stated.

The aim of the risk assessment is to identify, analyse and assess in a comprehensive manner the risk of money laundering and terrorist financing in Iceland. It is anticipated that the risk assessment will be utilised by all those with stakes in defending against money laundering and terrorist financing, such as:

- *Governmental authorities*, for example, when formulating policy for the issue category, making an action plan to mitigate an identified risk, producing educational materials, and setting rules and when allocating and prioritising funds.
- *Supervisors*, for use with risk-based surveillance and emphases in surveillance.
- *The justice system*, during investigations and analysis of the methodology of money laundering and terrorist financing.

³⁶ *OSCE Handbook on Data Collection in Support of Money Laundering and Terrorism Financing, National Risk Assessments*. Organization for Security and Co-operation in Europe, Vienna 2012.

- *Parties subject to mandatory reporting*, when preparing a risk assessment, and to strengthen areas where weaknesses have been identified, e.g. with enhanced controls, due diligences, work processes and employee training.
- *Scholars*, when researching money laundering and terrorist financing.
- *The public*, to draw attention to risks of money laundering and terrorist financing.

3.3.1. METHODOLOGY

The risk assessment is done in line with FATF's methodology for doing such assessments. It was based on the preparation of the risk assessments in 2019 and 2021.^{37, 38} In examining the methodology, the basic concepts are as follows:

- *Risk* consists of three elements: threat, weaknesses/mitigating elements, and consequences. The interplay of weaknesses and mitigating factors is that when a mitigating factor exists for a specific risk factor, it reduces weaknesses of the same risk factor and vice versa. In that sense, these factors work together.
- A *threat* can be an individual or a group of people, operations, or behaviours that can possibly cause damage, e.g. to the interests of a state, society, and/or the economy. Considering money laundering and terrorist financing, a threat can stem from criminals, criminal groups, terrorist organisations, and/or their supporters, funds controlled by the above parties, as well as operations of money laundering and financing of terrorist activities, in the past, present, and future. A threat marks a definite beginning point for understanding the risk of money laundering and terrorist financing. For this reason, it is important to understand, e.g. the environment of the predicate offences of money laundering and gains from criminal activities, considering the nature, size, and scope of an assessment of the risk of such operations. Also, a separate threat evaluation can be a precursor to a risk assessment for money laundering and terrorist financing.

³⁷ FATF Guidance. *National Money Laundering and Terrorist Financing Risk Assessment*. FATF, Paris 2013.

³⁸ FATF Report. *Terrorist Financing Risk Assessment Guidance*. FATF, Paris 2019.

- A *weakness* consists of elements that can affect a threat, e.g. support or facilitate operations where a threat exists. In the context of risk assessment regarding money laundering and terrorist financing, one must distinguish between weaknesses and threats, e.g. to remedy the factors that are weaknesses when it comes to defences against money laundering and terrorist financing, keeping in mind supervisory control and how well states are prepared to cope with weaknesses. Weaknesses can also include certain operations, a financial product or type of service and can expose it more to risk regarding money laundering or terrorist financing. The reciprocal applies to mitigating factors.
- The word *consequences* refers to the effect or damage which money laundering or terrorist financing can have on a state's interests. The consequences can be long-term or short-term in nature and can, amongst other things, effect the economy and the reputation of the country and, thus, international interests. Considering the challenges of determining consequences in each case, the FATF, in its methodology, emphasises a good understanding of threats and weaknesses in the assessment of risk.
- *Inherent* risk is risk before controls and other methods to reduce or manage risk have been taken into account.
- *Residual* risk is risk which remains after controls and other methods to reduce or manage risk have been taken into account.

The first step of the risk assessment was to analyse the main threats of money laundering and terrorist financing besetting Icelandic interests and assess them considering weaknesses and mitigating factors. After analysing these assessment factors, relevant data and information were collected, analysed, and evaluated to reach a conclusion on risk classification. In structuring the risk assessment, the current risk assessments of the European Union and other states were considered. The methodology can be described in greater detail as follows:

Definition, which entails defining the existing threats, weaknesses and mitigating factors, in addition to considering consequences. The operations or factor examined each time is mapped and evaluated as to whether threats or weaknesses/mitigating factors are present. A determination of which operations or factors are at greatest risk and/or pose the greatest threat and is necessary to map builds on risk events, i.e. known examples and cases of money laundering and terrorist financing. It also builds on risk factors, i.e. known details leading to specified operations, or a factor deemed more exposed to money laundering.

Analysis, which entails analysing the nature, scope, and likelihood of money laundering and terrorist financing, considering all the defined threats and weaknesses, after taking mitigating factors into account. Based on the analysis, the risk is assessed and classified.

A *matrix*, partially based on the European Union's matrix, was used for the risk classification. As threats and weaknesses and mitigating factors were assessed and rated, certain guidelines were used. Broadly speaking, the threat determined the risk classification and the classification conclusion could be on the scale of 1-4 depending on whether the analysed risk was deemed low, medium, high or very high. After a threat had been evaluated, an assessment was made of whether the presence of weaknesses or mitigating factors would affect both the threat and risk classification. The four categories of weaknesses and mitigating factors (further details below) each received a rating on the scale 1-4 depending on whether the effect of mitigating factors against the threat, considering weaknesses, were determined low (now risk reduction,) medium (2.5% reduction,) high (5% reduction,) or very high (7.5% reduction.) The lowering effect of the four categories for weaknesses and mitigating factors was added up and then subtracted from the assessed threat and, therefore, the total lowering could amount to 30% at most. Finally, that number was rounded up to the closest integer, which was then the conclusion of the risk classification of the assessment factor.

LOW**MEDIUM****HIGH****VERY HIGH**

In assessing the threat, the following factors, among others, were considered:

- *Environment*: Location and geographic factors, culture, and methods of transporting and/or handing over money.
- *Operation*: Knowledge, risk exposure, and innovations.
- *Partners*: New, unknown, trust etc.

The four categories of weaknesses and mitigating factors were:

- *Exposure to risk*, e.g. how easy it is to misuse specified operations.
- *Risk awareness*, i.e. how aware parties are of a risk of money laundering.
- *Rules and controls*, i.e. whether satisfactory rules and controls are in place. A distinction was made when assessing rules. For them, enacted laws and administrative directives were referred to. However, when assessing controls, the internal rules of companies and agencies were considered.
- *Eftirlit*, i.e. whether surveillance is in place and operating.

These factors could, due to their nature, increase risk due to weaknesses or, as the case may be, reduce the threat in the case of a mitigating factor. Since vulnerabilities could not have the same percentage increase effect as mitigating factors had for a decrease, it was also separately assessed on a case-by-case basis whether the vulnerabilities were serious enough to affect the existing threat and its assessment.

Part of the methodology of the risk assessment is to assess whether measures need to be taken to reduce the assessed risk and, if so, to specify which measures are appropriate. The steering committee of the Minister of Justice on measures against money laundering and terrorist financing will continue to work on the proposals which emerged during the structuring of the risk assessment and prepare action plans to respond to them.

4. MONEY LAUNDERING

Money laundering in this country is characterised by active participation in the financial system and the use of a currency which is usually invalid outside the country. The financial system is, therefore, most often a necessary element of the methods of perpetration used to launder the gains of domestic criminal activities. However, the small size of the financial system and the Icelandic króna do not prevent international money laundering from taking place in Iceland. Gains from this criminal activity are utilised within this country, usually laundered through real estate transactions, commercial transactions or the operation of corporations and companies engaged in operations which are otherwise legal, as well as abroad, e.g. through the purchase of currency or other liquid assets which are smuggled out of the country. Money laundering methods require differing levels of expertise and there are indications that offenders in Iceland have ready access to specialists who assist them, wittingly or unwittingly, in various aspects of money laundering, for example in book-keeping, real estate transactions, and business with banking institutions. Many documented money laundering methods and cases are related to cash. However, relatively few cases have come up in this country related to crypto-assets, although it is considered almost certain that their number will increase in parallel to their expanded use, and as offenders develop methods to utilise them.

The assessment factors of money laundering discussed in the risk assessment deal with, amongst other things, the methods which have been described here. Also, methods which the FATF has called attention to in recent years, such as methods related to gambling, will be taken into consideration. Assessment factors can be divided into the following categories; tax fraud as a money laundering predicate offence, cash and crypto-assets, financial market, specialists, gambling and the operation of companies. Each assessment factor is covered well in the following chapters but first there will be a discussion of the three stages of money laundering, the scope of money laundering and the main predicate offences of money laundering in Iceland.

THE THREE STAGES OF MONEY LAUNDERING

Money laundering may be divided into three stages. During the first stage, illegal gains are placed into the economy, e.g. through the financial system (*placement*.) During the second stage, the profits are in the financial system and they are moved around within it, even more than once, to isolate it from its illegal origins and disguise its original ownership (*layering*.) During the third stage the profits are utilised and integrated into the economic system, e.g. by purchasing a legal asset, such as a property, a car, a work of art or a share (*integration*.)³⁹

SCOPE OF MONEY LAUNDERING

Due to its nature, it is almost impossible to assess the scope of money laundering in Iceland and international organisations tend to offer differing assessments of the proportion of gross domestic products which is involved in money laundering. The most common practice is to refer to the assessment of the International Monetary Fund which estimates that the scope of money laundering is between 2-5% of gross domestic product worldwide and more international institutions have the same estimate of money laundering.^{40,41} It bears mentioning, though that in Europol's threat assessment of organised criminal activity, which was published at the end of 2021, it states that the scope and complexity of money laundering within the EU have been severely underestimated thus far.⁴² Iceland fares adequately compared with other states with regard to risk related to money laundering and terrorist financing.⁴³ Also, a recent survey by the International Monetary Fund revealed that foreign cash flow through the Icelandic financial system is relatively low-risk when compared to other Nordic countries.⁴⁴ In this context it's important to bear in mind that the Icelandic financial system is comparatively small and that Iceland is not an international financial centre. However, it is imprudent to assume otherwise than that money laundering is similar in scope in this country as in other western states. All numerical information about the scope of money laundering is to be taken with a grain of salt and it is first and foremost important to realise that the amounts in question are considerable and the consequences cannot be great.

THE CONSEQUENCES OF MONEY LAUNDERING

The negative consequences of money laundering for society and its financial system are manifold:

- Money laundering threatens the financial interests of the state treasury which is depleted of considerable revenue each year related to money laundering and tax evasion. Thus, money laundering has a grand impact on financial stability.

³⁹ *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, Second edition and supplement on special recommendation IX.* The World Bank, Washington 2006.

⁴⁰ [Money Laundering: the Importance of International Countermeasures--Address by Michel Camdessus \(imf.org\)](#)

⁴¹ *Estimating Illicit Financial Flows Resulting from Drug Trafficking and other Transnational Organized Crimes – Research Report.* United Nations Office on Drugs and Crime, Vienna 2011, pg. 7.

⁴² *EU Serious and Organised Crime Threat Assessment (SOCTA) 2021 – A Corrupting Influence: The Infiltration and Undermining of Europe's Economy and Society by Organised Crime.* Europol, Luxembourg 2021, pg. 11.

⁴³ *Basel AML Index 2022: 11th Public Edition – Ranking money laundering and terrorist financing risk around the world.* Basel Institute on Governance, Basel 2022, pg. 27.

⁴⁴ *Technical Assistance Report – Nordic Baltic Technical Assistance project: Financial Flows Analysis, AML/CFT Supervision, and Financial Stability.* IMF Country report no. 23/320. International Monetary Fund, Washington 2023.

- Money laundering hinders free competition and keeps market forces from blossoming. This conduct skews the competitive position in the market to the extent that parties who either commit such offences themselves or hire the services of subcontractors who do may be able to offer lower prices than parties with legal operations who do not commit such offences.
- In societies where money laundering is left unhindered, the credibility of the economic system and judicial system is undermined, as well as the confidence of the public in the police, the prosecution and other authorities. The consequences can include, furthermore, a bad reputation, within the country and abroad, thus harming the economy of Iceland significantly.
- Also, money laundering is followed by a series of other offences. This refers not to the predicate offence but other offences which become necessary along with money laundering, either as a method of perpetration in money laundering or subsequent independent offences, such as misuse of other people's identification and forgery.
- Finally, money laundering incentivises offenders to commit more offences. When offenders can utilise the profits of the offences which they commit, that can be an incentive to commit more offences.

In light of all this, it's important that the government is trusted and conduct visible surveillance, seeing to it that money laundering cases are adequately investigated and that those who commit such offences be subjected to legitimate penalties. Similarly, the private sector has an important role to play as the first line of defence against money laundering and the sharing of information and good cooperation between public entities and the private sector is therefore very important. Finally, money laundering is international in nature and efficient international cooperation between law enforcement agencies and other stakeholders is a key factor in the struggle against these offences.

MONEY LAUNDERING PREDICATE OFFENCES

Predicate offences of money laundering are offences resulting in unlawful gains that are later the object of money laundering. Below there is a general discussion of the predicate offences of money laundering and their main types, but no specific risk classification of such offences is involved. On the other hand, a specific discussion of tax fraud as a predicate offence of money laundering will follow, and those offences will be risk classified based on the risk assessment's methodology.

Iceland is deemed one of the safer countries in the world regarding crime and the frequency of offences, particularly regarding serious violent offences.⁴⁵ Despite

⁴⁵ [OECD Better Life Index](#)

MAIN MONEY LAUNDERING PREDICATE OFFENCES
Table 1

Each type of offence is mentioned once within the same case, e.g. if an investigation of a tax law violation focuses on more than one party, each type of offence is only counted once. Within each case, however, there can be more than one type of offence belonging to the same offence category, for example, an investigation of tax law violations can focus on more than one type of violation. Therefore, the number of predicate offences investigated in parallel with money laundering may be underestimated.

Types of offences	2021			2021		
	Number of offences total	Number of offences along with ML	Proportion	Number of offences total	Number of offences along with ML	Proportion
Tax law violations	158	135	85%	55*	34	62%
Drug offences	400	31	8%	336	31	9%
Fraud	670	54	8%	580	24	4%
Embezzlement	46	10	22%	57	10	18%
Document violations	276	7	3%	252	12	5%
Theft	4927	29	1%	4596	8	0.2%

* The decrease in the number of tax law violations may in part be traced to amendments of the act. For further discussion, see the section of the risk assessment on tax fraud as predicate offence of money laundering

this, each year there are many offences that can be predicate offences of money laundering. Predicate offences of money laundering can all be offences under the General Penal Code or special penal laws. Examples of common predicate offences are theft, fraud, embezzlement, tax fraud and drug offences.

Information from the police was gathered on the most common predicate offences, where money laundering was investigated in parallel during the years 2021 and 2022, see Table 1. This is based on statistical information regarding cases from the police systems (LÖKE).

Apart from tax law violations, drug offences and embezzlement are the most common predicate offences of money laundering. In the years 2021 and 2022, police investigated 62 cases where money laundering was investigated in parallel with a drug offence and 78 cases where money laundering was investigated in parallel with embezzlement. Embezzlement is also a common form of the predicate offences of money laundering, as in the years 2021 and 2022, 20 money laundering cases where investigated in parallel with embezzlement.

Drug offences entail the production, import, sale and distribution, custody, and handling of narcotics. Offences related to narcotics can be offences against either special penal laws, cf. the Narcotics Act no. no. 65/1974, or the General Penal Code if the offences are major, cf. Article 173a of the Act. The information collected on drug offences solely involves the production, sale, or distribution and import of narcotics

but not custody offences. A report from NCIP on organised crime in 2021 regarding activities that are linked with narcotics states: “On average, one drug offence case comes up each month where the scope of the case and the number of individuals involved indicate that organised crime is involved. Drug offences are also, in many cases, related to other offence categories and other illegal activities.”⁴⁶ Also, it is believed that as these groups grow in strength, it becomes easier for them to cover their tracks, buy expertise and conceal the profits of their activities in legal operations.⁴⁷ Many judgments have been passed down in drug offence cases during the past few years where money laundering was also being investigated in parallel, such as the judgment of the Land’s Court (Lrd.) 21 October 2022 in case no. 187/2022, Lrd. 27 May 2022 in case no. 241/2021, The judgment of the Supreme Court (Hrd.) 25 November 2021 in case no. 28/2021 and Lrd. 18. June 2021 in case no. 39/2020.

Fraud is one type of enrichment offence. It is deemed fraud if one person gets another to do something or not do something by illegally arousing, bolstering, or utilising a wrong or unclear idea of his about events and, thus, obtains money from him or others, cf. Article 248 of the GPC. Fraud cases, where money laundering could be involved, can be insurance fraud, e.g. by staging damage, payment card fraud where payment cards owned by others are used to fraudulently pay for products or services, and other kinds of deception where a criminal acquires unlawful gain. Also, fraud through the internet is common. The following are examples of judgments in fraud cases during the past few years where money laundering was being investigated in parallel; Lrd. 16 June 2023 in case no. 458/2022, Lrd. 24 June 2022 in case no. 390/2021, Lrd. 8 October 2021 in case no. 524/2020 and Lrd. 24 May 2019 in case no. 353/2018.

Embezzlement falls under enrichment crimes, cf. Article 247 of the GPC. Embezzlement is the unilateral and illegal appropriation of things that someone else owns, in whole or in part, but is in the custody of the perpetrator, provided that the appropriation is for the purpose of enrichment.⁴⁸ An example of embezzlement, where money laundering could be involved, is transferring money from another party’s or a legal person’s account into someone’s own account, and these cases are often connected with breaches of trust, cf. Article 249 of the GPC. The following are examples of judgments in embezzlement cases during the past few years where money laundering was being investigated in parallel; Hrd. 13 May 2022 in case no. 33/2021 and Lrd. 11 October 2019 in case no. 725/2018.

Document violations are used to either fraudulently acquire money or pretend to be someone else with various legal instruments, e.g. through forgery of personal identity papers, cf. the discussion below of ID numbers for foreign citizens. Document violations cover forgery, misuse of a document, and wrong use of a stamp or imprint. Of the above categories, most cases involve forgery. A number of these cases are traceable to forged identity papers, resulting from both document alteration and document forging from scratch. From case law it is clear that

⁴⁶ *Organised Criminal Activity 2021. Assessment of the Department of Research and Analysis of the National Commissioner of the Icelandic Police.* National Commissioner of the Icelandic Police, Reykjavík 2011, pg. 16.

⁴⁷ *Organised criminal activity in Iceland. Risk Assessment Report of the Department of Research and Analysis of the National Commissioner of the Icelandic Police.* National Commissioner of the Icelandic Police, Reykjavík 2019, pg. 24.

⁴⁸ *Jónatan Þórmundsson: Episodes of Crimes of Enrichment. Special part.* Reykjavík 2009, pg. 151.

NUMBER OF MONEY LAUNDERING CASES INVESTIGATED FROM 2017–2022
Table 2

Type of money laundering	2017	2018	2019	2020	2021	2022	Total
	Number	Number	Number	Number	Number	Number	
Money laundering, profits from criminal activity	25	31	73	77	65	78	349
Money laundering of the gains of own offence	22	51	126	120	93	40	452
Total	47	82	199	197	158	118	801

NUMBER OF MONEY LAUNDERING JUDGMENTS FROM 2018–2022
Table 3

Money laundering judgments	2018		2019		2020		2021		2022		Total	
	Num-ber	Propor-tion	Num-ber	Propor-tion	Num-ber	Propor-tion	Num-ber	Propor-tion	Num-ber	Propor-tion	Number	Proportion
Conviction	5	71%	17	100%	36	90%	32	71%	22	76%	112	81%
Acquittal	2	29%	0	0%	4	10%	13	29%	7	24%	26	19%
Total	7	100%	17	100%	40	100%	45	100%	29	100%	138	100%

this mainly involves foreign parties coming to Iceland on forged identity papers or using them to obtain an ID number for foreign persons.

Theft, whether perpetrated as pilfering or a break-in, is one kind of enrichment offence and a common predicate offence to money laundering. The definition of theft is the unilateral, and illegal taking of assets or energy reserves owned by another person, in whole or in part, from a custodian's keeping to acquire them for enrichment.⁴⁹ NCIP's department of research and analysis has called attention to an increase in these kinds of offences in reports on organised criminal activities. There are examples of groups of offenders coming to this country repeatedly the sole purpose of committing organised burglaries and theft.⁵⁰

MONEY LAUNDERING INVESTIGATIONS AND JUDGMENTS

In the past few years, there has been a great increase in the number of money laundering cases. Statistical information regarding money laundering investigations during the period 2017–2022 has been gathered, see Table 2. The number of money laundering cases investigated during the last two years is just under 300, namely 158 cases in 2021 and 118 cases in 2022. By comparison, the total number of money laundering cases under investigation during 2017 and 2018 was 129. This increase is in large part due to the increased focus by police on this issue category.

⁴⁹ Jónatan Þórmundsson: *Episodes of Crimes of Enrichment. Special part.* Reykjavík 2009, pg. 66.

⁵⁰ *Organised criminal activity in Iceland. Risk Assessment Report of the Department of Research and Analysis of the National Commissioner of the Icelandic Police National Commissioner of the Icelandic Police, Reykjavík 2019, pg. 18.*

Along with the increased number of investigations, the number of money laundering judgments has risen, courts having ruled on 140 cases during the last 5 years, see Table 3. Also, the proportion of convictions during this time period amounts to about 80% on average.

One should be wary of the statistical information. Judgments can contain more than one violation and a case under investigation by police can end in ways than a judgment, such as the investigation being dropped or the combination of case units. Finally, it bears mentioning that many money laundering charges have been dismissed by the court for lack of an independent description of the money laundering violation. That was the conclusion of a judgment from the Supreme Court of Iceland on 2 March 2022 in case no. 46/2021 which started this process. In the judgment in question, the conclusion stated that the charge had been lacking a description of the activities of the charged during money laundering (self-laundering) in addition to predicate offences. For this reason, that charge was dismissed by the district court. Since then, several judgments have passed where this has been confirmed.

4.1. TAX FRAUD AS PREDICATE OFFENCE OF MONEY LAUNDERING

RISK CLASSIFICATION



Tax fraud is a criminal offence and one of the most common predicate offences for money laundering. It can take the form of fraudulent conduct with various methods of perpetration with the goal of evading the payment of taxes and governmental fees. Fraud can regard both various special penal laws and the GPC. Main special laws in the field of tax law are the Act on Income Tax no. 90/2003, the Withholding Tax Act no. 45/1987 and the Act on Value Added Tax No. 50/1988. If violations of the above special penal laws are major, they fall under the provisions of Article 262 of the GPC. The analysis in this category utilised, for example, information from the DTI, FIU and police, information and reports from other governmental units and appropriate legislation.

GENERAL

The tax authorities play a key role in gathering revenue for the state through the collection of taxes and fees. Tax fraud causes great harm to society, amongst other things by skewing the competitive position of companies and by posing a threat to the financial interests of the state. According to the definition of the FATF, tax fraud is one of the predicate offences of money laundering. The definition is based on Article 264 of the GPC. The Directorate of Tax Investigations is responsible for the preliminary investigation of all tax law violations and gathering all necessary data before the decision is made as to whether the matter should be referred to the police, cf. the recommendation of the Director of Public Prosecutions no. 6/2021. A change has occurred since the last risk assessment was prepared, namely that the Directorate of Tax Investigations is now part of the division of surveillance and investigations within Iceland Revenue instead of being an independent agency. The merger took place on 1 May 2021.^{51,52} The merger was a response to requirements which resulted from judgments from the European Court of Human Rights in connection with the investigation and prosecution of tax law violations and is meant to prevent the double

⁵¹ [Merger of Iceland Revenue and the Director of Tax Investigation | News and announcements | Iceland Revenue – taxes and fees](#)

⁵² [Merged department of tax inspection and tax investigation | News and announcements | Iceland Revenue – taxes and fees](#)

punishment of parties (*ne bis in idem*.) Today more cases within the tax system end in a guilty verdict as the Directorate of Tax Investigations was granted additional authorisation for fines, given certain conditions, with the aforementioned change in legislation in April of 2021. This results in fewer cases being sent to criminal proceedings than before, as Table 1 here above in the chapter on the predicate offences of money laundering.

It is considered tax evasion if a party deliberately or through gross negligence provides incorrect or misleading information to be used in determining taxes. The same shall apply if a party neglects to provide information which may be of significance, whether for their own tax returns or those of others. An example of this may be insufficient disclosure of the income of an operator, a double system of accounts, the payment of hidden wages and overreported operational expenses, whether unfounded or because of personal expenses.

One type of tax fraud is organised *criminal activities* which entails systematic breaches of the tax system's regulations by organised violations of tax laws. An example of this could be illegal use of sales invoices from companies and individuals that do not engage in any business operations, but rather the accounts are utilised by operators intending to evade the payment of value-added tax and income tax and extract assets to pay hidden wages, i.e. black wages, or for personal use. This conduct may be seen in the form of misuse of companies and also of the names of individuals. Another example of this is the issuance of unfounded reports of value-added tax credits where offenders submit value-added tax reports hoping for a refund without being entitled to one. The basic factor is that a legal person or individual has an open value-added tax number.

Another example is *the hidden economy* which often refers to a "business environment" which is nowhere recorded. Everything is below the surface, and neither income nor expenses are reported. Examples of this worth mentioning are operations that have not been recorded with tax authorities and/or an instance where no application has been made for a value-added tax number. Consequently, no taxes have been paid on these operations. This can be under the auspices of either a company's or an individual's operations.

In the year 2021, the total tax revenue of the state amounted to just over 709 billion ISK while the local tax revenue of municipalities amounted to about 274 billion ISK. In the year 2022, total tax revenue amounted to 861 billion ISK while the local taxes of that year amounted to about 306 billion ISK.^{53, 54} Precise figures on the scope of tax fraud in this country are not available. However, the report of the task force of the Minister of Finance and Economic Affairs on the scope of tax evasion and its recommendations for measures from 2017 stated that tax evasion had been estimated to amount to 3–7% of GDP or about 10% of the total tax revenue.⁵⁵ It may therefore be deduced that tax fraud in Iceland is severe and costly for society.

⁵³ [State Accounts 2022](#) The Ministry of Finance and Economic Affairs, Financial Management Authority, Reykjavik 2023, pg. 21.

⁵⁴ [Local taxes – Icelandic Association of Local Authorities](#)

⁵⁵ [Scope of tax evasion and proposals for actions. Report of task force.](#) The Ministry of Finance and Economic Affairs, Reykjavik 2017, pg. 3.

According to information from the DTI, the majority of cases which have ended in an investigation report in recent years has originated at the directorate itself. Another effect of the merger of Iceland Revenue and the Directorate of Tax Investigations in the year 2021 is that statistical comparisons between the years 2021 and 2022 is not feasible, given the changed laws and regulations. Reports from the FIU have become more numerous in recent years, while the number of new cases investigated on the basis of reports by the FIU numbered 34 in 2021 and 45 in the year 2022.

About 1,500 to 2,000 surveillance cases are registered at the DTI because of tax returns each year deemed worth looking into. A portion of these cases will become tax investigation cases, although most of them are tax surveillance cases. In the year 2021, 265 cases will be registered for investigation and the investigation of 70 cases concluded with a report. In the year 2022, 216 cases will be registered for investigation and the investigation of 42 cases concluded with a report. According to the DTI, the reduction in the number of cases being investigated by the DTI from 2021 to 2022 is traceable to a legal change because of the merger of Iceland Revenue and the DTI on 1 May 2021 and the subsequent reorganisation of Iceland Revenue in 2022.

Cases were concluded with a redetermination of taxes in 51 cases in the year 2021 and 22 cases in the year 2022, a total of 73 cases. Total sums in cases concluded with a redetermination of taxes amounted to about 1.7 billion ISK in the year 2021, and about 2.1 billion ISK in the year 2022, a total of about 3.8 billion ISK. In conclusion, the total amount in cases which concluded with a penalty fine was about 225 million ISK in 2021 and about 650 million ISK in 2022. It should be noted that the procedure of levying fines was not the same in 2022 as in 2021. During the first part of 2021, the taxation reassessment committee levied fines in cases while after the middle of 2021, as act no. 29/2021 was amended, the taxation reassessment committee only levied taxes through a process involving a charge, while the Directorate of Tax Investigations also started concluding cases with fines more often. It should be noted that these figures don't include the sums of court fines in tax investigation cases.

In the year 2021, 76 cases were referred to the district court and 15 cases in the year 2022, a total of 91 cases. The reason why fewer cases were referred to the district court in 2022 is traceable to Act no. 29/2021, as it was stated in a report appended to the bill which became the law, that the policy was to conclude more tax law violation cases within the tax system with a fine determination, resulting in fewer cases being sent to the police for investigation.

THREATS

Tax fraud presents a major threat as it has thus far been considered easy to commit the offences and launder the gains made thereby. Also, cases related

to tax fraud are often very complicated and, thus, their investigation by the authorities takes a long time and the burden of proof in cases with criminal proceedings is substantial. Also, there is a marked increase in the instances of offenders receiving the assistance of specialists in committing tax law violations.

There has been a marked increase in the number of violations related to misuse of the VAT-system. In those cases the determination to commit offences seems to be evident, the violations require organisation and the sums in question are often very high. In many cases, there is a misuse of forms of organisations and the same offenders often appear in one company after another where the companies seem to serve no other purpose than to serve a fraudulent operation. Easy access to companies, amongst other things, appears to enable this. It also seems that organised criminal groups have increasingly begun to use otherwise legal economic activity for tax fraud purposes and money laundering, and the gains of criminal activities are also laundered through companies.

The method used by offenders and organised criminal groups to commit tax fraud is the same, i.e. the issuance of unfounded sales invoices. An example of this is when company A issues an invoice which company B receives and pays. Then company A takes out the money, along with the collected VAT, in cash and doesn't return the VAT to the state. After the money has been withdrawn in cash it becomes impossible to trace and, thus, more difficult to identify the party who profits from the offence and whether the invoices are unfounded or legitimate. Then, once the offences have been uncovered, the offender has more often than not left the company and moved on to "the next ID number" where the same activity is carried on. These offences then lead to offences against other special criminal acts, such as the Income Tax Act or the Act on the Withholding of Public Levies at Source. According to information from the DTI, there is a marked change in the way in which the withdrawal of cash is arranged in the offences. The companies involved in this criminal activity now transfer sums in varying amounts to many individuals who may even pay them to third parties who then withdraw them in cash. According to the DTI, this seems to stem from the increasingly stern regulations of commercial banks regarding cash withdrawals and their limiting effect on the business of these parties.

Also, it has recently become evident that offenders have systematically used another means to misuse the VAT-system. An offender has then come by a company with an old ID number and then utilised the company to send in a request for a VAT refund based on fraudulent information. Because of the number of refund requests in the system of Iceland Revenue it can be difficult to ascertain that all refund requests are rightful. Information about the investigation of such cases are available with the tax authorities and the district public prosecutor.

The scope of tax fraud as a proportion of the total proportion of the pred-

icate offences of money laundering is unclear. However, if one goes by the proportion of GDP, there is reason to conclude that tax fraud is, by far, the most common type of money laundering predicate offence in this country.

WEAKNESSES AND MITIGATING FACTORS

Tax fraud is a way for parties to gain considerable financial profits. It has been rather easy to launder the gains of these offences as there are no restrictions on the use of cash. Until now, measures to counter this activity have been deficient, e.g. misuse of the VAT-system with the issuance of bogus invoices. Also, investigating the money laundering end of the offences has proved difficult and many money laundering charges have been dismissed because of a lack of description of the money laundering offence, i.e. the money laundering investigation has been deemed insufficient. However, according to the district public prosecutor's office, this has been countered with education for the employees of the police and the prosecution regarding the investigation of money laundering cases. As the preceding risk assessment states, a general awareness of tax fraud exists, but the public's attitude toward it appears to be more lenient than it is toward other offences. According to special criminal acts on tax affairs, among others Paragraph 1 of Article 109 of the Income Tax Act and Paragraph 1 of Article 40 of the Value Added Tax Act, anyone found guilty of an offence shall be made to pay a fine of up to tenfold the amount of taxes evaded. If the offences are major they can be subject to Paragraph 1 of Article 262 of the GPC. Despite this, the penalties for tax law violations do not seem to have the intended deterrent effect.

In December of 2022, the National Audit Office submitted an administrative profile of the collection of court fines.⁵⁶ The maximum penalty permitted for severe tax law violations is up to 6 years in prison, although an unsuspended conviction is rare. In more cases, the penalty is suspended concurrent with the fine. According to the administrative profile, a large portion of court fines were levied for tax law violations. Throughout the years, court fines in the offence category have been growing. However, it seems that the proportion of collected court fines decreases significantly, the higher the fine is. From 2017 up to and including 2021, 118 judgments were issued for tax law violations. Where the fine exceeded 8 million ISK it had only been paid in seven cases. As the judgments were examined it was discovered that none had resulted in prison sentences. In 44 cases the penalty had concluded with community service. It was also stated in the report that those who were denied community service would not serve their sentence in prison but that their guilt would most likely reach the statute of limitation and become void. This is to a great extent due to the lack of funds of the State Prison Administration. It refers to the response of the Ministry of Justice to ensure ten prison spaces for the serving of substitute punishment.

⁵⁶ *Collection of court fines – Administrative Profile.* National Audit Office, Reykjavík 2022.

However, that proposal only lasted for a few months at the State Prison Administration, due to lack of funds.

The report also states that it seems that the longer tax fraud cases are investigated in the system, the more expensive they are to conclude. Also, the possible deterrent effect of the current penalty clauses of tax laws should be considered. It should be considered that more changes are required to enable Iceland Revenue to intervene in possible tax fraud sooner. Since the last risk assessment, a lot has been achieved in these matters and several mitigating considerations have arisen.

At the end of the year 2019, a committee regarding the investigation and prosecution of tax law violations submitted its proposals.⁵⁷ The committee was entrusted with submitting the proposals to respond to the judgments of the European Court of Human Rights regarding double punishment. The main conclusions of the committee were that it must be ensured that fines should not be levied in cases which should move on to criminal proceedings, that the cooperation of agencies responsible for investigating tax law offences should be enhanced, thereby ensuring the integration of investigations with regard to time and substance. After the report was submitted, a bill was submitted to amend laws on the investigation and prosecution of tax law offences in the aim of legalising the proposals of the committee and that was done with a legal amendment in April of 2021, cf. Act no. 29/2021. Also, the Directorate of Tax Investigations merged with Iceland Revenue and the Directorate of Tax Investigations continues to be responsible for investigating tax law violations. The amendment expanded the parameters of the authorisation of the Directorate of Tax Investigations to levy fines, in the aim of reducing the number of cases submitted to criminal proceedings with the district public prosecutor and the fines of the Directorate of Tax Investigations can amount to up to 100 million ISK. It was also legalised that those cases which would be subject to criminal proceedings would not be subject to fines. This arrangement was further legitimised with the order of the Director of Public Prosecutions regarding tax law violations no. 6/2021 and in Regulation No. 808/2022 on the implementation of tax enforcement and tax investigations.

In April 2022, a task force was appointed to craft proposals to counter misuse of the tax system, which was an item of the action plan of the task force of the Minister of Justice regarding measures against money laundering and terrorist financing due to the current risk assessment of the National Commissioner of the Icelandic Police.⁵⁸ As the proposals were crafted, the focus was on fraud related to the issuance of bogus invoices.⁵⁹ The task force presented several proposals, most of which focused on providing Iceland Revenue with more and clearer authorisation to monitor, and respond more quickly to, possible tax fraud in the value-added tax system. The proposals included:

⁵⁷ *Committee proposals for the investigation and prosecution of tax law violations.* Reykjavík, 2019.

⁵⁸ *Action plan 2021–2023 - Measures against money laundering and terrorist financing.* Steering Committee of the Minister of Justice on measures against money laundering and terrorist financing, Reykjavík 2021.

⁵⁹ *Issuance of Bogus Invoices - The Nature of the Behaviour and Possible Scope - Proposals for Actions.* The Ministry of Finance and Economic Affairs, Reykjavík 2023.

- To fully implement risk-based surveillance of value-added tax.
- To restrict the use of cash in transactions in business activity.
- To examine whether the arrangement of a stringent surrender requirement could be utilised to reduce tax fraud.
- To examine the implementation of electronic dissemination of information to the tax authorities.

In June 2023, Act no. 51/2023 to amend the Value Added Tax Act etc. was approved, legislating a large portion of the proposals of the task force. There Iceland Revenue was, amongst other things, provided with additional authorisation to refuse to register entities of the VAT tax register and to rule that an entity shall be removed from the VAT tax register. The proposal of the task force regarding restrictions on the use of cash has not yet elicited a reaction and cash has played a key part in covering the tracks of funds acquired by tax fraud, amongst other things, with the issuance of bogus invoices.

At the end of the year 2022, Act no. 133/2022 to amend the Bankruptcy etc. no. 21/1991 was approved to deal with so-called “ID number roaming”. Under Article 180 of the act, official receivers are now obligated to require an operational ban on anyone who has worked on managing the company in the last 18 months before the deadline, as they consider the conditions of Article 181 of the act to have been met. The condition for an operational ban is mainly that the individual is deemed unfit to manage a limited liability company because of harmful or indefensible business practices in managing the company. An operational ban, according to the law, lasts for three years.

Several things have been achieved in the issue category since the last risk assessment was published. Several changes have been made to the organisation of investigations and prosecution of tax violations and laws regarding income tax and value added tax. Also, “ID number hopping” has to some extent been addressed with amendments to laws on bankruptcy. The use of cash in business activity has, however, not been addressed, which may be deemed an important factor in countering money laundering. It hasn’t been long since these changes came into force and so it is deemed too early to assess the effectiveness and deterrent effect of the amendments.

RISK CLASSIFICATION

VERY HIGH

Considering the foregoing threats and weaknesses, after taking into account mitigating factors, the risk connected to money laundering where tax fraud is a predicate offence is still very high.

4.2. CASH AND CRYPTO-ASSETS

There can be a risk that the fruits of unlawful conduct in the form of cash will be brought into circulation in operations or transactions where the use of cash is common. The most common form of money laundering is cases where the offender utilises the gains in the form of cash for general support, without making a special effort to conceal their origins, as business can take place without mediators and without the participation of parties who are parties subject to mandatory reporting. More complex forms arise when special methods are employed to install cash in the financial system and make arrangements for its origins to appear legitimate. For offenders, it can be risky to store cash gains for a long period of time and it is difficult to allocate much of it at a time without drawing attention. This especially applies in economies where inflation fluctuates, like Iceland.

According to the information of FIU, the supply of cash in the Icelandic financial system was at minimum a little more than 141 billion ISK in the year 2021. Thereof, the cash supply of legal entities amounted to just over 31 billion ISK and that of individuals about 110 billion ISK. Considering the fact that the use of cash is decreasing in this country in all conventional business with products and services and as the payment of wages it's clear that payments in the form of cash are especially exposed to money laundering. Also, cash appears in most cases which the police is aware are related to organised criminal activity.

Although cash and its use is still considered the most serious single risk factor of money laundering in this country, as well as world-wide, there are many indications that the use of crypto-assets to launder unlawful gains is on the increase and that the skill of offenders in this field is increasing.

A lot is similar with the inherent risk of money laundering related to cash and crypto-assets. Among the threats and weaknesses in common, it should be noted that:

- With cash and crypto-assets, quick and unmediated business is available, which is desirable for offenders.
- There is no registry over the owners of cash or the occupants of addresses which hold crypto-assets, as with e.g. bank deposits or real estate properties. Both can therefore be anonymous and hard to trace and it can be difficult to ascertain the origin of finances or beneficial ownership.

- As a result, the use of cash and crypto-assets for illicit business activity and business with illegal products and services is common, even through the darkweb, such as in business with drugs, weapons and prostitution.
- The smuggling of cash is a common, simple and inexpensive way to get money between countries. There are indications that offenders are increasingly using crypt-asset payments for this purpose, as such payments are much quicker and are considered less risky than traditional bank transfers.
- There are no restrictions or limits on the use of cash in Iceland and cash can be used for almost any transaction. So far, only a few parties accept crypto-assets in exchange for products and services. However, that has been changing quickly, especially worldwide.
- A complete overview and surveillance of the use of cash is lacking and little is known about the use of foreign currency in circulation. The same applies to the use and transaction of crypto-assets with regard to a complete overview. The result is an environment where illegitimate business activity can thrive.
- Finally, it's difficult to produce statistical information from police systems regarding the seizure of cash in police cases, amongst other things because of registration incongruities. Also, there have been very few seizures of crypto-assets, expertise and coordinated procedure for those matters is lacking.

In light of all this, threats and weaknesses related to the use of cash and crypto-assets are discussed especially in this chapter. The discussion of cash is divided into a discussion about: the transfer of cash to and from Iceland, activity where business and cash payments are substantial and matters of dispute related to cash in circulation and the use of larger bills. The analysis and the subsequent risk classification utilised information and reports from institutions and other governmental units, foreign and domestic. information from the police, the DTI and appropriate legislation.

4.2.1. CASH – TRANSPORT TO AND FROM ICELAND

RISK CLASSIFICATION



GENERAL

According to Customs Act no. 88/2005, customs control is the responsibility of Customs Iceland. Immigrants, emigrants and, where appropriate, customs brokers, tourists and merchant sailors are obligated, according to Article 27a of the act to especially notify the customs authorities of money, cash or bearer bonds, including traveller's checks, which are transported to the country from abroad and abroad from the country in the amount of 10,000 euros or more, given the public guideline rate of exchange as listed at each time. Also, Customs, according to Article 162 of the act, has the authority to seize money which is transported to or from this country, according to Article 27b if there is a suspicion that they will be used to commit violations against the provisions of the GPC, such as against money laundering. Furthermore, Customs can seize money which is under the guideline limit for a duty to report if it may be assumed to have been acquired in a criminal manner, cf. Article 161 of Customs Law. Also, Customs, according to Article 156 of the act, is authorised to examine and investigate all products transported to this country, whether products on a cargo manifest, mail transport, passenger transport or anything else.

Customs harbours number 23 according to the regulation on the custody and custom clearance of goods no. 1100/2006. They are to be found in the following locations: Reykjavík, Grundartangi, Akranesi, Grundarfjörður, Ísafjörður, Skagaströnd, Sauðárkrókur, Siglufjörður, Akureyri, Húsavík, Vopnafjörður, Seyðisfjörður, Neskaupstaður, Eskifjörður, Reyðarfjörður, Egilsstaðir, Höfn at Hornafjörður, Vestmannaeyjar, Þorlákshöfn, Keflavík, Keflavíkurflugvöllur, Hafnarfjörður and Kópavogur. The main cargo harbours are Reykjavík harbour, Grundartangi, Reyðarfjörður, Seyðisfjörður and Þorlákshöfn, where most of the cargo enters and leaves the country. Finally, many harbours in the countryside are used for significant fish exports.

In the past few years, there has been a great increase in tourism, if one discounts the years from 2020 to 2022 when the Covid-19 pandemic was at its zenith. Also, there has been a great increase in the number of fugitives and immigrants who come here to settle down or to work for longer or shorter durations.

INFORMATION FROM CUSTOMS ICELAND
Table 4

	2016	2017	2018	2019	2020	2021	2022	Total
Reports to customs regarding cash in the amount of 10,000 euros or more	2	14	8	13	7	16	23	83
Number of customs cases where the party is detained with cash in excess of 10,000 euros	0	0	0	4	2	0	4	10
Cash in excess of 10,000 euros found in shipment of mail, express delivery or cargo	0	0	0	0	3	*	*	3

* Information was not available for the number of cases for 2021 and 2022

Most tourists arriving in Iceland go through the Keflavik Airport. In addition to Keflavik Airport, there are three other international airports in the country, i.e. Reykjavik Airport, Akureyri Airport and Egilsstaðir Airport. There are also some arrivals, mainly privately owned aircraft, at other smaller airports. Part of the year, a passenger ferry comes and goes at Seydisfjörður. In addition, it is worth mentioning that a great number of luxury liners come to Iceland each year, mostly in the summer, and their passengers number hundreds of thousands.

It is extremely rare for the customs authorities to be informed of a person coming to Iceland or departing from the country who is carrying cash exceeding the limit for mandatory reporting. Also, no notifications of remittances in the amount of 10,000 euros or more have been received by the Customs post office. Similarly, very few cases have arisen with customs in recent years where cash is being transported over the border, although there has been an increase in the months already passed in 2023. From 2016 to 2022, ten cases have arisen where a party has been stopped with cash exceeding 10,000 euros without having notified Customs. Additionally, three cases arose from 2016 to 2020 where, without notice, cash exceeding 10,000 euros was found in a postal delivery, expedited delivery, or cargo shipment. Figures from Customs Iceland for the time period from 2016 to 2022 may be seen in Table 4.

THREATS

The main threat of the transport of cash is that it is easy and inexpensive to transport cash over the Icelandic border. One can fit a great amount of cash in a relatively small space, especially in the case of high denomination banknotes. There is a risk that offenders and parties affiliated with organised crime will transport money between countries to launder illegitimate gains or finance further criminal activity. On the international stage, offenders are known to use so-called mules, who transport cash on their own person, but it is also common for cash to be transported via cargo or mail.⁶⁰

⁶⁰ FATF Report. *Money Laundering Through the Physical Transportation of Cash*. FATF, Paris 2015.

Each year, a large number of people arrives in this country and departs from this country, both by air and by sea. Considering the natural defences regarding the transport of cash to and from Iceland, it may be pointed out that Iceland does not border any other countries and, therefore, the opportunities to transport cash may be fewer than elsewhere. Furthermore, the Icelandic króna is a small currency which is not in high demand worldwide. This renders the method of perpetration and/or possibility of money laundering dependent on foreign exchange transactions.

Finally, cases have been investigated by the police where illegitimate gains have been exchanged for foreign currency, which has been transported out of the country. Also, reports to the FIU regarding foreign exchange transactions are common and there are indications that they may be related to criminal activity, often drug offences, but it is also suspected that parties receive their wages in cash. There is a further discussion of foreign exchange transactions in the financial markets section of the risk assessment.

WEAKNESSES AND MITIGATING FACTORS

Disclosure regarding the transport of cash is tied to the duty of the party in possession of the money to give notice or the surveillance of Customs. There are very few notices upon arrival to or departure from the country of cash that exceeds the permitted limit and customs cases where the smuggling of cash is discovered on the persons of passengers, in cargo holds and shipments are very few. There is, however, an increase in cases such as these in the months already passed in 2023, which is traceable, amongst other things, to the implementation of more efficient monitoring of arriving and departing passengers on the basis of risk-based analysis. Also, there is active surveillance of passengers who have been reported to travel with money. Specialised surveillance of postal deliveries or expedited deliveries is limited and the training of the Customs' dogs to search for money is still ongoing. Considering the number of cases which Customs has been responsible for investigating and information regarding surveillance, it may be concluded that surveillance of the transport of cash and other valuables to and from this country are deficient.

Risk awareness regarding the transport of cash over borders is good and Customs and police are aware of the methods of perpetration which are thought to be used. The number of money laundering reports from Customs to the FIU depends on the number of reports regarding cash at arrival to or departure from the country. Furthermore, it's common that suspicious foreign exchange transactions be reported to the FIU, as it is a known form of money laundering to exchange the gains of criminal activities for foreign currency and transport it out of the country.

The surveillance authorisations of Customs are limited, as legal authority to

search the checked baggage of departing passengers without the person being present, or being given the opportunity to be present, during the examination, is not in place. It may also be concluded that the deterrent effect of the penalties are limited. Currently, for instance, the penalty is set at the amount of fees from any secreted product but there are no penalties on cash transported to the country or out of it. Also, there are more requirements for degrees of culpability in offences related to the import or export of cash than in the case of other customs violations.

RISK CLASSIFICATION

VERY HIGH

In light of the above, the risk in this area of assessment is deemed high.

4.2.2. CASH TRANSACTIONS

RISK CLASSIFICATION



GENERAL

In Iceland, there are no legal limits on cash transactions, whether by legal entities or individuals. Also, there are no constraints on cash withdrawals in commercial banks and savings banks. There is a development evident in this area, regarding cash transaction controls within the banks, with regard to both deposits and withdrawals, as a limit has been imposed on how much can be withdrawn from an Automatic Teller Machine (ATM) within 24 hours. Also, this country has ATM's owned by foreign parties not under direct surveillance by the CBI. It should be noted that in Europe, the countries who have imposed limits on the use of cash is growing⁶¹ and the proposal for the most recent anti-money laundering directive from the EU from 20 July 2021 includes a recommendation that a limit on the receipt of cash in business transactions be placed at 10,000 euros.⁶²

The AML Act imposes obligations on those who receive cash in business transactions in the amount equivalent to 10,000 euros. The act stipulates that parties who, in a business capacity, receive cash over that limit, in one payment or more which appear to be linked, shall be considered subject to mandatory reporting. In such cases, they are obligated to carry out due diligence with regard to their business partners. Finally, these parties are obligated to report to the FIU any suspicious transactions and finances which are suspected to be traceable to criminal activity. The Directorate of Internal Revenue has, since the beginning of the year 2019, surveilled those who are subject to this provision.

On the purchase of goods and services, the following laws may apply: the Act on the sale of goods no. 50/2000, the Industrial Act no. 42/2000, the Act on Consumer Goods Purchases No. 48/2003 and the Act respecting Professional Commerce no. 28/1998.

Generally, access to banking is good in Iceland and access to cash as well. However, there is little use of cash in this country when compared to other countries and there has been an increase in the use of electronic means of payment. It is estimated that the use of cash in cash transactions amounted to about 7,5% in the year 2022, compared with 8% in the year 2020 and just under 13% in the year 2018. In a Gallup poll for the CBI in the spring of 2022, a question was posed

⁶¹ *Supra-National Risk Assessment Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.* SWD(2022)/554. EU, Brussels 2022, pg. 14.

⁶² *Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing.* COM(2021)/420. EU, Brussels, 2021.

regarding the use of cash to pay for goods and services in retail locations and the result was that one third of respondents said that they used cash and the number had fallen by 6.5% from a comparable poll in 2020. A large majority said that they used it for presents and to pay other individuals.⁶³ In this context it should be noted that the various forms of the Covid-19 pandemic and the resulting downturn lead to less use of cash for transactions, such as increased internet shopping, an increase in touch free payment options and a reduction in the number of tourists.

Following the economic collapse in 2008, the use of cash increased from less than 1% of GNP to more than 2%. Generally, cash use as a percentage of gross national product has been estimated at 2%–2.5%. At the end of 2022, the cash in circulation was ISK 80.7 billion which amounts to 2.5% of GDP and that is a rather low percentage when compared with other countries.^{64,65} This development is not unique to Iceland and it has been noted within EU states, that is, demand for euros has increased, but at the same time cash has been used ever less in retail business. In the EU risk assessment it states that the development of an increase in the cash in circulation despite less use of cash has been dubbed the paradox of banknotes.⁶⁶

There exist various explanations for the continuing demand for cash despite the reduction in the use of cash as a means of payment at retail locations. In times of economic uncertainty, people seem to react by transferring their assets to a more secure form. Therefore, it may be that a significant amount of cash stays unused by its owners and is used for savings outside banks.⁶⁷ On the other hand, there are no indications that the group of individuals who keep cash outside banks has grown larger. Also, the demand for the largest bills has not increased and the amount of cash withdrawals in ATM's and with tellers has not increased.⁶⁸ Finally, the explanation that the increase in the number of tourists is related to the increase in cash in circulation is unlikely, as the amount of cash withdrawals by tourists has decreased.⁶⁹ It may be argued that since cash is anonymous, that means that part of it is utilised for criminal activities such as money laundering, purchase of illegal goods and services, payments of wages in cash and tax-fraud.⁷⁰

Accessibility to cash for purchasing products and services is good, and in most transactions, where the purchase of products and services goes on, it is possible to pay with cash. It may also be pointed out that it is possible to use cash for other kinds of transactions that are not deemed to be purchases and sales of goods and services, such as for the purchase of real estate and auction sales.

In general, rather little is known about the use of cash in Iceland by industry. However, the analysis of the FIU indicates that retail trade comprises over half of all cash within the banking system. Also, there is a great cash turnover in

⁶³ *Financial stability, 2022(2)*. CBI, Reykjavik, Volume 31. 28 September 2022, pg. 45.

⁶⁴ *Financial stability, 2022(2)*. CBI, Reykjavik, Volume 31. 28 September 2022, pg. 46.

⁶⁵ [Bills and coins in circulation](#) (sedlabanki.is)

⁶⁶ *Supra-National Risk Assessment Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*. SWD(2022)/554. EU, Brussels 2022, pg. 22.

⁶⁷ *Financial infrastructure*. CBI, Reykjavik, Volume 7. 24 June 2019, pg. 35.

⁶⁸ *Financial stability, 2022(2)*. CBI, Reykjavik, Volume 31. 28 September 2022, pg. 46.

⁶⁹ [Veltan – Trends and policies in Icelandic retail and services](#)

⁷⁰ *Financial stability, 2022(2)*. CBI, Reykjavik, Volume 31. 28 September 2022, pg. 46.

hardware stores compared with other industries, which substantiates the conclusion of the task force regarding tax evasion in Iceland that tax fraud is rather common among contractors and in the construction industry.^{71, 72}

THREATS

Although cash is not the main means of payment of consumers, it is still the means of payment which most often occurs in money laundering.⁷³ In markets where cash transactions are common the danger is that offenders and individuals affiliated with organised crime will try to launder the gains of their criminal activity by establishing operations or making use of relations in the field of commerce and services and funnelling such funds into legal operations. Also, there is a danger that offenders use ill gotten money to buy products or services in the market in the sole aim of laundering the gains of illegal operations, whether the merchant is unaware or complicit in the money laundering.

The main threats with cash transactions are that it is therefore easy to put unlawful gain from criminal activities quickly into circulation. Cash is hard to trace and this method is therefore a desirable and safe way for offenders to disguise their gains from unlawful activities. In this regard, all operations engaging in cash transactions are in a risk group. It requires no special knowledge to get unlawful gain into circulation and conceal a trail of money in other lawful economic activity.

In the analysis of Iceland Revenue of cash withdrawals in the years 2019-2021 it was revealed that the scope of cash withdrawals by legal entities and individuals which might possibly be considered inordinate withdrawals, amounted to just over 13 billion ISK per year. The research was limited to the withdrawals of legal entities over 3 million ISK each year and the withdrawals of individuals over 5 million ISK each year, from bank accounts via ATM's and bank tellers. The analysis reveals that cash withdrawals above and beyond that which can be considered reasonable are substantial and indicate that the withdrawals may be related to criminal activities. Finally, it must be considered especially inordinate when payments between two parties who are in business together (Business to Business, B2B) are rendered in cash.⁷⁴

There are also examples in police cases where there are ties between organised criminal activities and the use of cash. This is considered in the context that access to foreign currency is good, and it is easy to exchange Icelandic krónur for it and get unlawful gains out of the country. Finally, it's very common for reports to the FIU to be related to cash. These reports are related to both deposits and withdrawals of cash and inordinate withdrawals by legal entities. On the other hand, very rarely does the FIU receive reports for receipt of cash over 10,000 euros which indicates a lack of awareness of risk within companies in the field of commerce and services.

⁷¹ *Scope of tax evasion and proposals for actions. Report of task force.* The Ministry of Finance and Economic Affairs, Reykjavík 2017.

⁷² *Issuance of Bogus Invoices - The Nature of the Behaviour and Possible Scope - Proposals for Actions.* The Ministry of Finance and Economic Affairs, Reykjavík 2023.

⁷³ *Supra-National Risk Assessment Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.* SWD(2019)/650. EU, Brussels 2019.

⁷⁴ *Issuance of Bogus Invoices - The Nature of the Behaviour and Possible Scope - Proposals for Actions.* The Ministry of Finance and Economic Affairs, Reykjavík 2023.

WEAKNESSES AND MITIGATING FACTORS

There are no constraints or restrictions on the use of cash, and rather little is known about the ultimate use of cash by individuals and companies. It has been pointed out that reducing the use of cash in circulation, for example, by discontinuing the issue of ISK 10,000 and ISK 5000 banknotes, would make “the black economy difficult to use, along with reducing money laundering and tax evasion”.⁷⁵ Finally, it has been pointed out that by restricting the use of cash in business, the misuse of the operations by companies, for example, with the issuance of bogus invoices and money laundering related thereto, may be countered.⁷⁶

There is almost no monitoring of the use of cash except by the CBI to ensure that there is enough cash in circulation for aspects of economic management. However, since the beginning of the year 2019, surveillance of anti-money laundering measures has been overseen by the money laundering division of the Directorate of Internal Revenue in the case of cash transactions, in one or more related payments, in the amount of 10,000 euros or more. Lack of information regarding operations where cash is common leads to such surveillance possibly pertaining to all parties engaged in business and its execution is therefore subject to difficulties. There is considered to be a risk that retailers and service providers, particularly smaller parties, do not conduct a risk assessment or due diligence or do not attend to their obligations with regard to the use of cash over 10,000 euros as the same obligations do not apply to them with regard to the use of cash under the same limit. In the estimation of the supervisors, the efficiency of the requirements to parties required to give notice is limited in this context, for instance the limit amount is high and related payments narrowly defined by the parties subject to mandatory reporting.

Awareness of risk related to the use of cash and knowledge of the AML Act by parties who conduct their business with cash appears to be deficient, which is reflected in few reports to the FIU regarding cash payments. The government and supervisors are aware of the risk which may stem from the use of cash in connection with money laundering and educational materials have been published which refers to operations where cash is used a lot, in addition to educational meetings for parties in the market. Another mitigating factor is that there is little use of cash in Iceland compared to many other European countries, including EU member states.

⁷⁵ *Scope of tax evasion and proposals for actions. Report of task force.* The Ministry of Finance and Economic Affairs, Reykjavík 2017, pg. 36.

⁷⁶ *Issuance of Bogus Invoices - The Nature of the Behaviour and Possible Scope - Proposals for Actions.* The Ministry of Finance and Economic Affairs, Reykjavík 2023, pg. 28.

RISK CLASSIFICATION
VERY HIGH

For these reasons, the risk of cash transactions is high.

4.2.3. CASH IN CIRCULATION, HIGH DENOMINATION BANKNOTES

RISK CLASSIFICATION



GENERALLY

The discussion of the use of high denomination banknotes intertwines with the previous discussion of cash. Five kinds of banknotes are circulating in this country. This arrangement has been in place since the latter part of 2013 when the ISK 10,000 banknote was released into circulation. The purpose of issuing the banknote was to make transfers of funds in Iceland easier and more efficient by, amongst other things, reducing the number of banknotes in circulation.⁷⁷

By the end of 2022, bank notes in circulation outside the CBI were arranged as may be seen in Table 5. The most numerous banknotes in circulation are ISK 1000 bills and the least numerous are ISK 2000 bills. About 55% of all banknotes in circulation are ISK 500 and ISK 1000 bills. About 44% are ISK 10,000 and ISK 5000 bills. Less than 90% of the circulating money in the form of cash is in ISK 10,000 and ISK 5000 bills.

The number of banknotes in circulation has increased significantly in recent years, despite an increase in the use of electronic means of payment and a decrease in the use of cash in business transactions.

Regarding cash transactions with foreign currency in this country, the following information is available from CBI on the purchase and sale of foreign currency

⁷⁷ [A new ten thousand krona bill set into circulation today \(sedlabanki.is\)](https://sedlabanki.is)

BANK NOTES IN CIRCULATION OUTSIDE THE CBI BY THE END OF 2022

Table 5

Size of bills	In circulation outside the CBI	%	Number of bills	%
ISK 10,000 bills	49,787,580,000	65.4	4,978,758	26.1
ISK 5000 bills	17,435,915,000	22.9	3,487,183	18.3
ISK 2000 bills	209,000,000	0.3	104,500	0.5
ISK 1000 bills	6,948,825,000	9.1	6,948,825	36.5
ISK 500 bills	1,767,425,500	2.3	3,534,851	18.6
Total	76,148,745,500	100	19,054,117	100

CASH TRANSACTIONS IN FOREIGN CURRENCY, ITEMISED BY CUSTOMERS

Table 6

Customers	2018	2019	2020	2021	2022
Domestic individuals	33.8	30.7	8.6	11.1	18.0
Foreign individuals	7.2	8.8	3.6	1.0	1.0
Domestic legal persons	32.3	40.0	9.8	1.7	2.3
Tourists	10.2	7.5	0.6	2.0	3.4
Total	83.6	87.1	22.6	15.8	24.6

Amounts are in billions of ISK

CASH TRANSACTIONS IN FOREIGN CURRENCY, ITEMISED BY CURRENCIES

Table 7

Itemised by currency	2018	2019	2020	2021	2022
EUR	45.1	49.1	12.6	9.0	14.5
USD	18.4	17.7	5.3	3.5	5.7
GBP	6.7	6.4	1.4	0.7	1.3
PLN	4.7	5.6	1.6	1.4	1.6

Amounts in ISK billions

in the time period from 2018 to 2022, as can be seen in Tables 6 and 7. The effect of the Covid-19 pandemic, and the travel restrictions which came with it, on foreign currencies is clearly evident, as the purchase and sale of foreign currencies reduced dramatically in the years 2020-2022. One can see that the most common purchase is that of euros.

Information is not available on further use of foreign currency in this country, nor is information regarding which particular banknotes are most in circulation. The European Central Bank stopped issuing 500 euro bills in April 2019. The reason for the decision is that the bills are thought to be mainly used in organised criminal activities. Although printing of the 500 euro bill has ceased, demand for the bill is still active. This exception is thought to be connected to criminal activities.⁷⁸ For example, one might note that with the use of large bank notes it is possible to transport considerable sums between countries. For example, one can put about €6 million in €500 bills into a regular briefcase, which is almost ISK 900 million. In comparison, the largest Icelandic banknote is ISK 10,000, which is the equivalent of 70 euros, given the exchange rate at the end of September 2023. Finally, it bears mentioning that there is practically no market for the Icelandic króna outside the country.

⁷⁸ *Supra-National Risk Assessment Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. SWD(2022)/554. EU, Brussels 2022, pg. 22.*

THREATS

With cash, one can conduct quick, anonymous, and almost untraceable transactions. It is rather easy to put the gains of criminal activities in the form of banknotes into circulation, as it is generally easy to use cash for payments and as it is not subject to great restrictions. It requires little preparation and organisation. Also, a large part of the cash in circulation, in sums, is in the form of high denomination banknotes, which makes it easy to store high amounts of money. In this way, it is rather easy to get large sums of money into circulation despite the use of cash generally being proportionally uncommon. However, the threat related to cash and money laundering is not limited to high denomination banknotes and large amounts of small denomination banknotes can be just as attractive for offenders. Also, there is a known form of money laundering in police cases involving money laundering, where unlawful gain is exchanged for foreign currency and transported out of the country. On the other hand, nothing indicates that high denomination banknotes are used more than other bills in criminal activities in this country.

WEAKNESSES AND MITIGATING FACTORS

The Central Bank of Iceland ensures that there is enough cash in circulation for aspects of economic management. Also, the Directorate of Internal Revenue surveils operations where parties engaged in business engage in cash transactions of over 10,000 euros. In other respects, surveillance of the use of cash is limited and therefore, it is not known where the business community most uses high denomination banknotes. Information is also lacking on the use of cash, regarding both Icelandic and foreign banknotes – if they are accessible and distinguishable. Statistical information regarding the seizure of cash in police cases is also deficient.

Awareness of risk among parties in markets which are not subject to the AML Act is a weakness. Few reports reach the FIU regarding cash from parties engaged in commerce and services, which indicates a lack of risk awareness, although police and other authorities are aware of the risk stemming from cash.

A mitigating factor worth mentioning is that the biggest issued bank note in Iceland is the ISK 10,000 bill. This is not a particularly high amount, compared to banknotes in other currencies. Also, the market for Icelandic cash on foreign soil is almost non-existent and the use of cash generally in this country is small, compared to other European countries.

RISK CLASSIFICATION

HIGH

The risk of the use of high denomination banknotes is deemed high.

4.2.4. CRYPTO-ASSETS

RISK CLASSIFICATION



GENERAL

In the AML Act, crypto-assets are defined as: *“Any valuables in digital form: a. which can be used for payment or investment and which can be shared, and b. which are not considered digital currency in the sense of the Act on the Issuance and Treatment of Electronic Money or currency issued by a central bank or other authorities.”* As crypto-assets are not issued by the CBĽ as banknotes and coins are, no responsibility is taken for their value. The value of many crypto-assets is entirely dependent on the price which the buyer is prepared to pay at each time, not underlying assets, and, therefore, their value can fluctuate significantly. Other crypto-assets link their value to a currency/currencies or standard, such as gold, but claims that they are insured by underlying assets are not inspected at all. The CBĽ has, as the European surveillance authorities in the financial market and financial surveillance authorities in the EEA have, repeatedly warned of the risk that comes with doing business with crypto-assets.⁷⁹

Service providers of crypto-assets are those who offer services related to crypto-asset transactions, such as exchanging currency and/or electronic money for crypto-assets and vice versa or exchanging one type of crypto-asset for another. A precise definition of the service providers of crypto-assets is available in the AML Act. According to Article 35 of the act, those who offer such services in this country must apply to be registered at the CBĽ and receive their registration to be able to begin operations. Registered parties are obligated to abide by the AML Act and the surveillance of the CBĽ is limited to that. Special financial requirements are not made of the service providers of crypto-assets or requirements which ensure consumer protection. In other words, these parties are not subject to surveillance according to other legislation like other parties in the financial market. In this country, four parties were registered at the CBĽ as crypto-assets service providers in September of 2023. The number of clients of operational companies in the middle of the year 2022 was about 13,400 in total and there has been an increase in their number in the past few years. There is a further discussion of domestic crypto-assets service providers in the financial markets section of the risk assessment.

⁷⁹ [Risk comes with crypto-asset transactions \(sedlabanki.is\)](https://www.sedlabanki.is/)

As crypto-assets transactions take place online, it's easy for consumers to utilise the services of foreign parties. Therefore, consumers must estimate for themselves the reliability and security of such services, as service providers are not always obligated to be registered or licenced in other states. Surveillance of them can, therefore, be limited or even non-existent.⁸⁰ Also, one can conduct transactions with crypto-assets between two parties without the involvement of service providers.

In the first years, crypto-assets were mainly used as so-called speculative investments. In the past few years, though, the development has been quick and the number of companies who accept crypto-assets for products and services has grown quickly in the past few years. Also, various foreign crypto-asset service providers have begun to offer a connection of crypto-assets with payment cards which can be used the same as other traditional payment cards in stores or other places who accept Visa or Mastercard. This means that it will become ever easier for common consumers to use crypto-assets for payment in the traditional economy.

It's hard to estimate the total scope of crypto-assets in Iceland. According to a survey conducted for the CBI in February of 2022 regarding the public's views on and knowledge regarding crypto-assets, 8.7% of respondents had invested in crypto-assets. Also, 13.4% of respondents considered themselves likely to purchase crypto-assets in the future. Of those who had invested in crypto-assets, about 74% took their business through foreign service providers, 17% through domestic service providers and just under 9% through both domestic and foreign service providers. One in every four who had invested in crypto-assets had used them for product transactions. The results of comparable surveys in the states of Europe indicate that individuals in this country are not slower than individuals of other nations to do business with crypto-assets, quite the contrary.⁸¹

The precise number of various types of crypto-assets in the world is hard to estimate. However, in 2023 they numbered at least 20 thousand and their total market value amounted to well over 1000 billion us dollars. Bitcoin and Ethereum are the largest and best known crypto-assets.⁸²

THREATS

As previously stated, the scope and economy of virtual assets has been growing in Iceland and worldwide. This applies both to the number of entries and number of customers, but also with regard to where and when crypto-assets can be used as a means of payment or investment. Transactions in crypto-assets are by their very nature international and flow freely across borders. It can also be difficult to figure out the origin of crypto-assets and an actual owner despite it generally being possible to trace the path of transfers in crypto-assets in block-

⁸⁰ [Risk comes with crypto-asset transactions \(sedlabanki.is\)](#)

⁸¹ *Financial Stability, 2022(1)*. CBI, Reykjavík, Volume 30. 16 March 2022, pg. 49.

⁸² [Different Types of Cryptocurrencies – Forbes Advisor](#)

chains up to a certain point, as it is not always possible to acquire information regarding the party who is involved in the transaction. No official register of the owners or address holders who store crypto-assets is available. Transactions with crypto-assets generally occur in telecommunications, online, or even between two parties without outside services, and great speed characterises these transactions. These features are all attractive for parties who seek to transfer the gains of unlawful operations from one state to another, operate outside traditional borders, disguise their beneficial ownership and launder money.

Europol's report on organised criminal activity states that crypto-assets are an important means of payment for offenders in transactions involving illegal products and services, such as drugs, weapons and prostitution and that money laundering is the offence category which is mostly related to crypto-assets. Also, crypto-assets are a common means of payment for products and services on the darkweb and in transactions with dangerous states with which parties do not wish to be identified.^{83, 84}

According to information from Europol, Bitcoin is the most common crypto-asset used by offenders. However, the agency presumes that offenders will increasingly turn to crypto-assets which are especially designed to disguise beneficial ownership (*piracy currency*) and complicate transfers with the aid of crypto-mixers.⁸⁵ Monero is the best known example of such a type of crypto-assets. However, such types are more difficult to obtain and use for transactions than the better known and more transparent types, such as Bitcoin. So far, crypto-asset service providers in this country haven't offered transactions with Monero to a significant degree.

Finally, new crypto-assets with new features keep appearing, as well as new products and services based on blockchain technology. In this context, one might mention NFTs (*non fungible tokens*) which is a sort of digital certificate of ownership for digital constructs which are unique and unchangeable. Therefore, subjective estimation can determine value as in the case of other works of art and, thus, transactions with NFTs can pave the way for offenders to get inordinate amounts of money from one party to another without further explanations.

In Iceland there are indications that offenders have begun allocating profits from criminal activities into purchasing crypto-assets in the aim of laundering money. There are also indications that crypto-assets are used as a method of perpetration to get money out of the country instead of previously better known ways which are even considered riskier and slower, for instance, cash smuggling.

So far, relatively few police cases have been related to crypto-assets. It is considered almost certain, though, that their use for money laundering will increase in parallel to their expanded use, and as offenders develop methods to

⁸³ *EU Serious and Organised Crime Threat Assessment (SOCTA) 2021 – A Corrupting Influence: The Infiltration and Undermining of Europe's Economy and Society by Organised Crime*. Europol, Luxembourg, 2021.

⁸⁴ *Cryptocurrencies Tracing the Evolution of Criminal Finances, Europol Spotlight*. Europol, Luxembourg, 2021.

⁸⁵ *Supra-National Risk Assessment Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*. SWD(2022)/554. EU, Brussels 2022, pg. 95.

utilise them. The crypto-asset economy is still young and risks related to money laundering and terrorist financing are still emerging.

WEAKNESSES AND MITIGATING FACTORS

Crypto-asset transactions take place through the internet and Icelanders have access to foreign crypto-asset service providers and digital banks who are not subject to mandatory reporting in Iceland and are not subject to money laundering surveillance by the CBI. The transactions of offenders and other Icelanders are therefore not limited to Icelandic service providers. Varying requirements are made regarding due diligence and surveillance of parties who offer crypto-asset services and countries are not all as advanced in their efforts to implement anti-money laundering and terrorist financing measures related to crypto-assets. Offenders abroad are known to have taken advantage of the differing status of countries regarding the implementation of the FATF on crypto-assets and laws and regulations on money laundering and terrorist financing.

So far, crypto-assets have been outside the law in Iceland, except for the AML Act. No coordinated consumer protection regulations apply to crypto-assets and their service providers within the EEA. In September 2020, the European Commission submitted a draft regulation on Markets in Crypto-Assets (often abbreviated as MiCA) which the European Parliament has passed. The regulation will be implemented by EU member states in the year 2024 but awaits entry into the EEA-agreement and Icelandic legislation.⁸⁶ The purpose of the regulation is to coordinate requirements within the EEA for the operations of crypto-asset service providers and services, bolster innovation, strengthen protections for investors and consumers and to ensure financial stability. This way, a comparable set of regulations is set to apply to crypto-assets as that which applies to securities trading and market manipulation. Furthermore, the EU has passed an amendment to a regulation regarding the information which is to follow the transfer of funds and certain crypto-assets.⁸⁷ The aim of the regulation is to reduce the likelihood of crypto-assets being utilised to contribute to, finance or conceal offences or money laundering. Crypto-asset service providers will then be obligated to gather and submit information regarding the originator and recipient of a payment as they conduct transfers on their behalf. This is in accordance with the recommendations of the FATF.⁸⁸ It's important for the new European regulatory environment to be implemented as quickly as possible in this country so that Iceland doesn't lag behind other states in this respect and, thus, becomes a forum for circumvention and various kinds of criminal activities.

So far, reports to the FIU from Icelandic crypto-asset service providers have been relatively few and no reports have been forthcoming from foreign partners regarding the crypto-asset transactions of Icelanders through the crypto-asset service providers whose operations are based in other countries. In

⁸⁶ *Opportunity and risk in the field of digital financial services based on a distributed transaction register. Report of task force.* The Prime Ministry, Reykjavik 2023.

⁸⁷ [Risk comes with crypto-asset transactions \(sedlabanki.is\)](https://www.sedlabanki.is)

⁸⁸ *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations.* FATF, Paris 2023. pg. 76.

the next few years, one may expect an increased number of reports from crypto-asset service providers, because of the added scope and activity as well as because of a more stringent regulatory environment in this issue category.

The main weakness related to the issue category when considering the future is the lack within the Financial Intelligence Unit (FIU,) police and other monitoring agencies of necessary equipment, protocols and specialisation to conduct analysis, trace transactions and investigate cases related to crypto-assets. The FIU and the police are provided with the assistance of foreign police departments and institutions in this respect. Nevertheless, this hampers reactivity and the possibility of seizing ill gotten funds in the form of crypto-assets. Also, tools of analysis in this field are expensive and it is not clear whether Iceland will be able to run such systems. Vigorous international cooperation is the precondition for success in this field. The increased spread and usage possibilities of crypto-assets, within and without the traditional economy, come with various challenges for the police and other supervisors.

As a mitigating factor, it should be noted that crypto-asset markets can be unstable and value can fluctuate dramatically and, therefore, it can be risky to tie up funds in crypto-assets for the long term. Also, opportunities for using crypto-assets as a means of payment are still limited, although rapid changes may be detected.

Finally, it bears mentioning that there are no special legal provisions regarding the taxation of crypto-assets and in such matters the general provisions of tax laws apply. It may be assumed that the reporting of income in the crypto-assets of domestic parties is significantly deficient.⁸⁹

RISK CLASSIFICATION

VERY HIGH

For these reasons, the risk of crypto-assets is high.

⁸⁹ *Opportunity and risk in the field of digital financial services based on a distributed transaction register. Report of task force. The Prime Ministry, Reykjavik 2023, pg. 17..*

4.3. FINANCIAL MARKET

This section discusses the assessment and analysis of the risk of money laundering and terrorist financing in the Icelandic financial market. The end of the section will be especially devoted to digital financial services which are accessible to Icelandic citizens but are subject to registration and/or surveillance in other countries.

The Central Bank of Iceland is the supervisory body responsible for following up on parties subject to mandatory reporting in the financial market under the AML Act, regulations, rules, and related criterial rules. The CBI is authorised to take appropriate measures during monitoring, if necessary, such as applying penalties and coercive remedies. In addition, FSA sees to instructing parties in this category subject to mandatory reporting and evaluating its implementation under the act.

The following table illustrates the number of parties subject to mandatory reporting in the Icelandic financial market who were subject to CBI surveillance, cf. the AML Act, in September 2023.

The business of the four commercial banks is extensive in the market and they offer, as the savings banks do, various financial products and services for individuals and companies. However, their operations abroad are limited. The Icelandic pension fund system is large and ever growing and many of the pension funds offer services unrelated to their core operations, such as home loans. Other entities offer more specialised financial services. In the following discussion an effort will be made to assess the risk of misuse of financial products and services for money laundering rather than the misuse of types of financial companies for money laundering.

Threats, weaknesses, and mitigating factors were assessed, considering the knowledge and experience of the relevant authorities and law enforcement agencies in the financial market. Also, the assessment is based on various statistical information regarding operations in the financial market. The following are the main threats and weaknesses and mitigating factors which pertain to the financial markets in Iceland as a whole. Risk related to certain financial products and services will be covered further in the following sections.

**NUMBER OF PARTIES SUBJECT TO MANDATORY REPORTING IN THE ICELANDIC FINANCIAL MARKET
IN SEPTEMBER 2023**
Table 8

Financial undertakings	Number
Commercial banks	4
Savings banks	5
Credit companies	4
Securities firms	8
Mutual funds management companies	6
Pension funds	21
Life insurance companies	4
Insurance agencies (when they broker life insurance or other risk- and collection based life insurance).	9
Electronic money companies	2
Payment institutions	1
Currency exchange offices	0
Crypto-asset service providers	4
Licensed Alternative Investment Fund Operators	5
Alternative Investment Fund Operators Obligated to be Registered	17
Lenders and credit intermediaries	8
Agencies of foreign payment institutions	1
Branches of foreign insurance companies	1
Branches of foreign insurance agencies	2
Branches of foreign securities companies	1

- A changed and more open financial landscape, globalisation and increased supply and access to financial instruments have led to customers no longer receiving all of their financial services in one place. It gets ever more complicated for entities in the financial market, supervisors, investigators and police agencies to acquire and overview and assess whether the scope of transactions is in accordance with the estimated financial standing of the customer and, thus, to ascertain whether certain behaviour or business seems suspicious. Customers seek the most beneficial and simple ways which are most convenient for their needs. This applies to offenders and organised criminal groups who seek to funnel ill gotten funds into the financial system and conceal their origins. Changes in the arrangement of financial services may effect the methods used to launder money in this country.

- A great deal of automation is taking place, both with regard to services at entities subject to mandatory reporting, but also with regard to anti-money laundering and terrorist financing measures and surveillance. New dangers and opportunities must be considered, generally speaking, which may arise with the arrival of financial technology services and means of increasing the automation of entities subject to mandatory reporting in anti-money laundering measures. The processes, which are often contracted solutions, are to a great extent based on trust of the customers – that they'll answer truthfully – for example when they produce identification and answer due diligence surveys. Finally, it should be noted that foreign citizens with a ID number for foreign citizens can engage in business with domestic financial institutions. Further discussion regarding ID numbers for foreign citizens will take place before the risk of certain financial products is assessed.
- Financial services and payment solutions keep becoming simpler for customers to use and the need for expertise, even for the execution of complex financial instruments, has lessened. At the same time, various offshoots of the financial industry are based on technology no less complex, e.g. blockchain technology. It can be difficult for supervisory bodies and the police, with their limited human resources, to retain specialists in all areas.
- The Central Bank of Iceland is the supervisory body responsible for following up on parties subject to mandatory reporting in the financial market. The CBI prepares its own risk assessment of the financial market and conducts risk-based surveillance by it. Parties subject to mandatory reporting annually respond to the questionnaire of the CBI⁹⁰ and the CBI regularly conducts interviews with guarantors and conducts surveys to investigate the legal and regulatory compliance of parties subject to mandatory reporting. Following surveys in the years 2020-2022 of the conducting of risk assessments, the CBI published, amongst other things, a lessons report in April 2022⁹¹ in the aim of imparting the lessons of the supervisory body from surveys and databases. Also, the government has published lots of educational materials especially tailor-made for parties in the financial market subject to mandatory reporting.⁹²
- Awareness of risk among parties subject to mandatory reporting varies and it can be seen, amongst other things, in surveillance of entities and in the number and quality of reports regarding suspicious transactions which are sent to the CBI. Despite the measures generally resorted to by parties subject to mandatory reporting, there are still weaknesses, including to the risk assessment of operations and customers' risk classification, due diligence of customers, especially additional due diligence and regular surveillance of business, including that related to registration and traceability of information.

⁹⁰ *Guidelines with the questionnaire of the Central Bank of Iceland regarding risk assessment of measures against money laundering and terrorist financing.* CBI, Reykjavik 2023.

⁹¹ *Execution of risk assessment relating to money laundering and terrorist financing. Academic report. First edition.* CBI, Reykjavik 2022.

⁹² [Laws, rules and guidelines related to monitoring of money laundering and terrorist financing – Central Bank of Iceland \(fme.is\)](https://www.fme.is/)

- One of the strengths of the financial system is that a few large parties subject to mandatory reporting are responsible for the majority of domestic payments. Communication channels between cbl, supervisory bodies and parties subject to mandatory reporting are, therefore, efficient and the cooperation of the parties has been successful. On the other hand, the arrival of foreign digital banks online, crypto-assets as means of payment and other novelties within companies subject to mandatory reporting do not bode well. The experience of other states has taught us that very rapid changes in this field have in some cases reduced the efficiency of anti-money laundering measures across the country. It is important to closely monitor this development in this country.
- There is a great supply of digital financial services from financial technology companies based abroad. Such companies are not subject to mandatory reporting in Iceland and, consequently, the cbl doesn't have the same surveillance responsibility with regard to anti-money laundering and terrorist financing as with Icelandic companies who conduct operations subject to official authorisation or registration. Offenders in Europe are known to have begun increasingly to use these money laundering solutions and there are indications that this is also the case in Iceland. On the other hand, the FIU has seldom received reports on Icelandic citizens from its sister institutes abroad regarding suspicious transactions related to services of that nature.
- Despite the need for anti-money laundering and terrorist financing measures, de-risking within the financial system must be considered. This refers to certain groups being systematically excluded from traditional banking based on money laundering risk. Financial de-risking is conducive to increasing the share of shadow-banking, informal or untraditional financial services such as crypto-assets, Hawala, the services of foreign digital banks, etc. The scope of this problem in the current Icelandic financial market is not known. However, the focus should be placed on countering risk with additional surveillance instead of by de-risking.
- It is almost exceptional for money to be retrieved in cases related to internet fraud and other internet offences where most often a significant time period has elapsed since the fraud took place, where they may have taken place for some time and people refrain from seeking the aid of the police. In some instances the police department has failed to react in such matters and it would be beneficial for the police, the FIU and financial companies or their organisations to implement a protocol or contingency system in support of individuals, companies and other stakeholders against whom internet offences are perpetrated. The focus of the system would be on the first response following internet fraud, explicitly so that the deposits of bank accounts of offenders

which contain criminal gains may be seized or frozen. A contingency such as this is, first and foremost, geared towards the possibility of the authorities to reclaim funds. In this context, a revision might be required regarding authorisations within the Icelandic justice system to freeze assets in order to use the financial system to reclaim funds and of the authorisation of police to obtain information from financial companies without a court order, as such things often take precious time.

- Finally, it bears mentioning that legislation in the financial market with regard to anti-money laundering and terrorist financing is mostly adequate and anonymous transactions, for instance, are not permitted. It's important for the all changes and the new EU legislation to be implemented as quickly as possible so that Iceland doesn't lag behind other states in this respect and, thus, becomes a forum for circumvention and various kinds of criminal activities.

4.3.1.1. ID NUMBERS FOR FOREIGN CITIZENS

All individuals living in Iceland are recorded in Registers Iceland and must have a 10-digit ID number. Because of special interests in Iceland, foreign citizens can get "ID numbers for foreign citizens." This involves an identifier issued for administrative use regarding individuals not requiring registration, or fulfilling conditions for registration, in Registers Iceland. The Act on the Registration of Individuals no. 140/2019 entered into force, and legalised, for the first time, ID numbers for foreign citizens and the application process for it on 1 January, 2020. The act included the innovation that only public parties could be intermediaries for registration of an ID no. for a foreign person. Previously, legal persons could also be intermediaries. Individuals requiring ID numbers for foreign citizens must turn to a public party and that party applies to Registers Iceland for registration. A photocopy of a passport or recognised travel documents shall accompany the application.

The difference in the issue of ID numbers for foreign citizens, on one hand, and a traditional National ID number, on the other hand, is that there are different identification requirements. Thus, an individual getting an ID no. for a foreign citizen does not need to identify himself and present a passport or other valid travel papers, but rather the party applying makes a copy of the individual's identity papers. It's evident that in some cases the individuals never reside in Iceland and may not even have visited the country.

Those utilising ID numbers for foreign citizens are, for example, foreign employees receiving wages in Iceland for temporary work, foreign students, employees of embassies, individuals sitting on boards of directors of Icelandic companies or individuals accepting payments of some kind from Iceland, e.g. because of pensions.

An issued ID number for a foreign citizen grants no official rights in Iceland, for

example, to reside longer than 3-6 months, payments from the Social Insurance system or any other such rights. On the other hand, an ID number for foreign citizens facilitates people's access to specified services like healthcare services and a person with such an ID can, amongst other things, start a bank account, receive electronic ID, start a company and purchase real estate. There are known instances where ID numbers for foreign citizens have been used to found and run private limited companies and ID numbers for foreign citizens were registered on just under 500 properties in this country in 2021.

According to information from the register of ID numbers for foreign citizens at Registers Iceland, the number of applications in the year 2021 was about 2500 and in the year 2022 the applications were about 4700. However, the number of applications has decreased since the entry into force of Act no. 140/2019. Most applications for ID numbers for foreign citizens are for citizens within the EEA, from countries in Eastern Europe. There are few applications regarding individuals from states deemed to be risky states. Most applications regard temporary employment, e.g. about 61% in 2021 and about 73% in 2022, while other reasons include, for instance, business or board membership. The biggest group of applicants comes through Iceland Revenue. The percentage of rejected applications was 3.5% in the years 2021 and 2022. Finally, there are instances where an ID number for foreign citizens has been applied for based on false identification papers. According to Registers Iceland, however, the number of these cases has decreased in recent years.

The risk is that an ID number for a foreign citizen, based on forged identity papers, will be created to conceal the origin of the person involved, or even to "create" an individual within the system that does not even exist. As soon as such a National ID number is established, a bank account based on it can be opened that, depending on circumstances, can be utilised to launder unlawful gains.

The application process entails weaknesses, i.e. intermediation and analysis of personal identity papers. There is little monitoring of ID numbers for foreign citizens, and the law has no instructions on this. Among mitigating factors one might note that the legal requirements for ID numbers for foreign citizens are more stringent now than before the introduction of Act no. 140/2019. The authorities have also realised the problem in greater measure and are, moreover, actively looking out for forged identity papers. The employees involved in services and registration with Registers Iceland have been educated and trained with regard to the examination of identity papers.

4.3.2. DEPOSIT OPERATIONS

RISK CLASSIFICATION



GENERAL

A credit institution is, in Act no. 161/2002 on Financial Undertakings, defined as “a company whose operation involves receiving deposits or other repayable assets from the public and provide loans from their own account”. A credit institution can receive an operating license as a commercial bank, a savings bank or a credit company. Commercial banks and savings banks are obligated to provide deposit services while credit companies are not permitted to receive deposits.

In September 2023, four banks and five savings banks had permits to receive deposits under the Act on Financial Undertakings. Total amounts of the banks' and savings banks' deposits were as follows:⁹³

- In 2020 – ISK 2,267 billion
- In 2021 – ISK 2,497 billion
- In 2022 – ISK 2,707 billion

Neither the commercial banks nor the savings banks have branches outside the country. The proportion of foreign customers with the bank varies depending on the credit company in question but generally speaking that percentage is rather low and the majority of foreign customers is from within the EEA and a very limited portion is from risky and uncooperative states.

THREATS

Deposit operations entail the receipt of great sums of money, where the origin of it becomes difficult to trace, particularly where cash is concerned. This involves one of the main activities of banks and savings banks that entails many entries regarding customers. From this can stem various degrees of threat. For example, because this involves individuals in a risk group due to political ties, parties residing in areas defined as risky or parties connected with risky activities. Accessibility to these services is easy, for most people can open deposit accounts in domestic banks and savings banks as deposit accounts are necessary in many respects in modern society. Also, it is easy to misuse

⁹³ [Figures \(sedlabanki.is\)](#)

these services since they do not require much organisation or specialised knowledge in the aim of laundering money.

Organised criminals and/or a criminal organisation can use deposits to launder unlawful gains. The main threat entails the opening of numerous deposit accounts, for legal entities, trusts and/or individuals where transfers, deposits, and withdrawals are frequent. They often involve low amounts that may have the purpose of escaping notice. The use of straw men is known in this context.

Money laundering through deposit accounts is one of the commonest methods known to the police and the FIU receives many reports each year related to deposit accounts. Criminals are both domestic and foreign and can involve either organised crime or individual criminals. The scope of money laundering with this method is substantial. In addition, the use of cash is considerable.

Deposit accounts are often important links in the chain of various predicate offences. This includes organised tax law violations and internet fraud or other fraud where unsuspecting citizens are duped into depositing funds in the accounts of offenders or affiliated parties who subsequently withdraw the sum quickly in cash.

WEAKNESSES AND MITIGATING FACTORS

Despite the defences of parties subject to mandatory notification having been strengthened in recent years, there are still weaknesses in compliance with the AML Act, including risk assessment of the operations, customers' risk classification, due diligence and monitoring of customers. Commercial banks and savings banks have transaction monitoring systems to monitor deposits, although surveys have suggested that the systems have a few weaknesses. Also, new technology and financial technology services can create new risks and opportunities which enhance the automation of parties subject to mandatory reporting, e.g. the use of automatic tech solutions at the initiating of contractual relationships and at monitoring of transactions.

On the other hand, one can mention that anonymous transactions are not permitted, and the legal framework is deemed to be adequate. Further mitigating factors include extensive risk-based monitoring of the financial market, active internal monitoring of financial undertakings, and the general risk awareness of obliged entities is acceptable, after considering the number of notices to FIU by commercial banks. The savings banks send relatively few reports, though. Also, neither the commercial banks nor the savings banks have branches in other countries, the operations of the commercial banks abroad are generally limited and they have few foreign customers, although their number has been increasing. Finally, the publication of educational material has increased.

RISK CLASSIFICATION

HIGH

Considering threats and weaknesses after taking into account mitigating factors, the risk of money laundering regarding deposit operations is deemed high.

4.3.3. LOAN OPERATIONS

RISK CLASSIFICATION



GENERAL

Loan operations entail granting loans to individuals, legal entities, trusts and comparable parties. In Iceland there are various types of parties subject to mandatory reporting who provide various kinds of loan services. Commercial banks make comprehensive loans to individuals, trusts and comparable parties. These include overdrafts, real estate loans, car loans, and general as well as specialised loans to small and big companies. Savings banks lend especially to individuals and smaller companies in their fields. The Institute of Regional Development provides legal entities and individuals with loans in the aim of keeping regions populated and contributing to employment within the country and the Local Authorities' Loan Fund ohf. lends only to municipal authorities and institutions owned by them. The pension funds are also extensive in scope in the housing loans market. Other parties subject to mandatory reporting who provide loans, albeit to a lesser degree or in lower sums and for shorter periods of time than the aforementioned parties, include lenders registered with the Consumer Agency.

The total sums loaned by credit institutions – commercial banks, savings banks and credit companies – at the end of each year amounted to:⁹⁴

- In 2020 – ISK 3,349 billion
- In 2021 – ISK 3,684 billion
- In 2022 – ISK 4,139 billion

Lending operations in Iceland do not usually grant loans without a preceding credit rating or payment assessment of the relevant individual or company unless the amounts involved are low. Such loans are, therefore, usually not on offer to individuals or companies that, for example, cannot provide acceptable security or, for individuals, income information. Regarding foreign operations, lending institutions in Iceland do not have foreign branches. In addition, they have few foreign customers although the number of them has increased.

⁹⁴ [Credit institutions | Financial Supervisory Authority \(fme.is\)](https://www.fme.is/)

THREATS

The main threat of money laundering besetting loan operations is the repayment of loans with proceeds from criminal activities. An example of the characteristics of such loans is when instalments are made in cash or if the repayment process is quicker than one might assume given the fiscal capacity of the individual according to the payment assessment or given the turnover and financial standing of the company. In Iceland there are examples and/or indications of offenders using this method to launder their unlawful gain, especially related to real estate trades. Such methods, however, generally require specialised knowledge of the real estate market and/or company operations so that significant sums of money may be laundered. This is, therefore, also to be considered in context with the assessment of risk related to experts such as real estate brokers.

WEAKNESSES AND MITIGATING FACTORS

Despite the defences of parties subject to mandatory notification having been strengthened in recent years, there are still weaknesses in compliance with the AML Act, including risk assessment of the operations, customers' risk classification, due diligence and monitoring of customers. Furthermore, the weaknesses of these operations show up in their considerable scope, regarding both the number and the amounts of loans.

In addition, the access to smaller loans is easy, e.g. overdraft loans on the Internet and through credit cards. In the year 2020, lenders became, according to Act no. 33/2013 on Consumer Loans, subject to mandatory reporting. These parties, who mostly provide quick loans in small amounts, apply for and receive registration as lenders at the Consumer Agency but are subject to CBI surveillance with regard to money laundering and terrorist financing. Compliance with the requirements of the AML Act are, however, not a precondition for registration at the Consumer Agency.

Internal control of loan services is generally considered acceptable as the regulatory scheme for money laundering and terrorist financing covers commercial banking operations, including lending. In addition, the Act on Financial Undertakings no. 161/2002, the Act on Consumer Loans no. 33/2013 and the Act on Mortgage Lending to Consumers no. 118/2016 provide for lending institutions having acceptable internal lending rules and processes. Furthermore, the loan operations of Icelandic lending institutions is to the greatest possible degree limited to the domestic market, and risk-based monitoring of the financial market is extensive. Also, risk awareness is generally deemed acceptable, although it varies by the type of party subject to mandatory reporting. Likewise, the number of reports to the FIU differs by the type of party subject to mandatory reporting. Generally, few reports are received regarding suspicions of money laundering related to loan operations, although their number has increased. Finally, the authorities have published educational materials related to the issue category.

RISK CLASSIFICATION**MEDIUM**

Considering the above, the risk of money laundering connected with lending is deemed to be medium.

4.3.3.1. SIMULATED CONTRACTS

There are examples of offenders buying bonds against individuals who are registered for collection among financial companies, so-called collection bonds. The bonds are often against the coworkers of the one who buys the bonds and in many cases it's believed that the bonds are entirely simulated. In some cases there are indications that the bonds are related to collection by way of extortion. In this way, the offender can demonstrate a "legitimate" stream of income as he receives repayment and use for legitimate loans or investments.

4.3.4. PAYMENT SERVICES

RISK CLASSIFICATION



GENERAL

In the year 2021, Iceland implemented PSD2 (*Payments services directive 2*) with Act no. 114/2021 on Payment Services Payment Services, according to Article 4 of the Act, means the following:

- A** Services enabling cash contributions into a payment account, along with other necessary measures for a payment account's operations.
- B** Services enabling cash withdrawals from a payment account, along with other necessary measures for the operations of a payment account.
- C** Execution of payments, including transfers of funds into and out of a payment account at a user's payment service provider or another payment service provider:
 1. execution of direct payments, including individual direct payments,
 2. execution of payments with a payment card or comparable device,
 3. execution of asset transfers, including payments by credit card.
- D** Execution of payments if funds are insured with a line of credit for a payment services user:
 1. execution of direct payments, including individual direct payments,
 2. execution of payments with a payment card or comparable device,
 3. execution of asset transfers, including payments by credit card.
- E** Issue of payment media and/or payment processing.
- F** Money remittance.
- G** Execution of payments.
- H** Account information services.

Discussion of risk related to payment services is closely related to discussion of deposits and cash and other sections of the risk assessment are referenced regarding the above points a and b. In September 2023, no party was licenced for

TURNOVER OF ICELANDIC PAYMENT CARDS AND FOREIGN PAYMENT CARDS IN ICELAND IN THE YEARS 2020-2022.

Table 9

	2020	2021	2022
Turnover of Icelandic payment cards [ISK billions]	997	1096	1270
Turnover of foreign payment cards [ISK billions]	64	130	254

payment execution or account information services. Also, the risk assessment has a special discussion of remittances. The discussion here, therefore, applies first and foremost to payment services according to above points c, d and e regarding the execution of payments and payment processing.

In September of 2023, 13 entities in Iceland were authorised to provide payment services: four commercial banks, five savings banks, one credit company, two electronic money companies and one paying agency. Two of the aforementioned entities who mostly conduct payment processing, provide their services worldwide and are owned by foreign parties.

In connection with analysing the risk of money laundering, information was gathered on the size of transfer of funds in Iceland, total payment card turnover, and international transfer of funds.⁹⁵ The following table shows the total turnover of Icelandic payment cards and the total turnover of foreign payment cards in Iceland during the past three years. It's clear that the coronavirus pandemic has had a significant effect during these years. However, the turnover of foreign payment cards in the year 2022 had become comparable to that of the years 2016–2018.

The combined total number of transactions through the interbank system of the cbi (the gross settlement system and the imprest funds system) in 2022 amounted to just over 44 billion. Total turnover in the interbank payment systems at the end of each year amounted to:

- In 2020 – ISK 29,363 billion
- In 2021 – ISK 30,646 billion
- In 2022 – ISK 35,244 billion

Finally, the following table gives an overview of the flow of funds over the border in the years 2021 and 2022, including the flow of funds to and from risky and uncooperative states. The figures are based on data from the cbi regarding transfers within the SWIFT and SEPA systems.

The main trading countries of Iceland are the United States, Britain, Germany, and Denmark and most of the payments are made in euros and us dollars. Payments to and from risky states are about 0.5% of the total payments to and from foreign states. It should be noted that the list of countries considered risky

⁹⁵ Figures (sedlabanki.is)

THE FLOW OF FUNDS TO AND FROM RISKY AND UNCOOPERATIVE STATES IN THE YEARS 2021 AND 2022 IN BILLIONS
Table 10

	2021	2022
Total outflows [ISK billions]	1761	2032
Total inflows [ISK billions]	1786	1945
Total outflows risky and uncooperative states [ISK billions]	8.3	10.3
Total inflows risky and uncooperative states [ISK billions]	5.4	7.3

and uncooperative is subject to changes.⁹⁶ Finally, it should be added that payments through offshore companies, low tax areas and offshore areas, have a great turnover.

THREATS

The main threats of these operations stem from the characteristics of payment services, no borders, great and variable accessibility and the considerable number of transactions that payment service providers execute. It's easy to conceal and complicate the trail of ill gotten funds with transfers within payment systems and through different payment service providers, i.e. by transferring funds between payment accounts and payment service providers, as the quality of surveillance varies, the speed is great and the degree of complication of payments varies. Such circumstances can create increased opportunities for anonymity and tracking transactions becomes more difficult. The speedy development of new electronic payment methods to do business can attract parties engaging in money laundering as the risks are not as well known and, therefore, surveillance of them is not as active. Considering the above, it must be deemed that the risk of money laundering will increase with the new payment methods and new technology which has arisen in the Icelandic financial market as elsewhere in the world and will continue to develop in the next few years.

The FIU receives a considerable number of notifications of money laundering regarding these operations.

WEAKNESSES AND MITIGATING FACTORS

Despite the strengthening of the defences of parties subject to mandatory reporting in recent years and seasons, there are still weaknesses in compliance with the AML Act, amongst other things regarding risk assessment of operations, risk classification of customers, due diligence and regular monitoring of transactions. Parties subject to mandatory reporting in this market have transaction monitoring systems to monitor payments. However, surveys have detected several weaknesses in transaction monitoring.

⁹⁶ [Risky and uncooperative states – Central Bank of Iceland \(fme.is\)](#)

The awareness of risk among payment service providers is generally acceptable. Due to the small size of the financial system, domestic financial institutions should be able to be knowledgeable regarding customers who are extensive in scope with regard to foreign payments. The scope of payments through low tax areas and offshore areas is significant in the Icelandic context and the analyses of the FIU indicate that the economy may be vulnerable to international money laundering and terrorist financing. This is in keeping with the experience of other states. For future reference, it's important to ensure that controls regarding payments across borders are in keeping with the risk of international money laundering and terrorist financing. In this context, it should be noted that the expected risk in this field has increased quickly in recent seasons regarding ongoing threats in the international arena. For instance, payments involving international sanctions and terrorism.

Two of the entities involved in payment processing services in this country also provide them abroad. This includes geographical risk being more with them than with other payment service providers and increases the exposure of the Icelandic payment service market to money laundering risk.

Finally, the legal framework is considered satisfactory and anonymous transactions are unauthorised. Supervisors carry out a detailed risk assessment of the operation and educational materials have been updated.

RISK CLASSIFICATION

HIGH

With reference to the existing threats and weaknesses and considering mitigating factors, the risk of money laundering from this operation is deemed high.

4.3.5. REMITTANCES

RISK CLASSIFICATION



GENERAL

Money remittances are defined as “a payment service where funds are received from a payer without opening payment accounts in the name of the payer or the recipient of the payment. This is done for the sole purpose of sending the corresponding amount to a payment recipient or another payment service recipient on behalf of the payment recipient and/or when funds are received on behalf of the recipient of the payment and delivered to him for disposition”, cf. Article 3 of the Act on Payment Services no. 114/2021.

In September of 2023, no Icelandic entities with the operating licence of a paying agency ran this type of operation. On the other hand, one agent of a foreign paying agency was authorised for remittances in this country and, according to the CBÍ, the total amount of money remittances in 2022 was just over ISK 1.5 billion, the number of customers was just over 20,000 and the number of customers just over 5000. The activity has suffered contractions since the publication of the preceding risk assessment as in the year 2020 two of the four agents of foreign paying agencies who were then authorised to engage in remittances were active and the total amount of money remittances was just under ISK 2.5 billion. Money transfer services which agents provide on behalf of foreign payment services generally operate in parallel with other different operations, e.g. postal operations.

THREATS

The threats facing these operations mean that business relations are often not engaged in for business purposes and only involve several individual transactions, where the customers do not need to have accounts with the payment service provider in order to engage in business. The service also allows for the use of cash and money laundering through this operation does not require specialised knowledge or organisation. These characteristics of the operations, along with possibly forged personal identity papers being used to confirm identity possibly contribute to the limited availability of information about customers and the purpose of a transfer. Offenders are also known to make use of straw men and use smurfing related to remittances, dividing the profits from criminal activities into small

amounts in the aim of avoiding suspicion and dodging further surveillance.

The service can be connected with high-risk states, and there are indications that the service in those states is used by customers that would otherwise be subject to strict systematic surveillance. This risk assessment is not based on statistics regarding the receipt location of remittances from Iceland. However, according to information from the CBÍ, the percentage of foreign customers is low and in a few instances they are from risky or uncooperative states.

There are indications that remittances have been used systematically to launder money and get it out of the country quickly. Also, the FIU receives several notices each year regarding the suspicion of money laundering through remittances. However, there are several indications that offenders have begun using more various ways to send money between countries, such as crypto-assets and new financial technology services. Also, the number of cases where individuals are arrested with cash on their person on their way out of the country has increased - see the discussion of cash in the risk assessment for further details.

WEAKNESSES AND MITIGATING FACTORS

The scope of remittances has decreased in the past few years. Remittances in this country are only engaged in by agents of a foreign payment agency. This, in and of itself, entails considerable risk, not least because it is generally difficult for paying agencies employing agents to control and monitor them. There is also a weakness inherent in operating financial services of this sort in parallel with other unrelated operations, as it may increase the risk of employees lacking the adequate know-how and/or time to conduct legal surveillance. In light of the inherent risk, the surveillance of CBÍ of the operations has been significant given its scope, including surveillance related to anonymous transactions, as well as additional cooperation with the domestic surveillance of the payment agency which has issued reports regarding agents in this country. Finally, the publication of educational materials has increased.

There are indications that the risk awareness of parties engaged in this business is limited and that there are still weaknesses with regard to the implementation of a risk-based approach, amongst other things with regard to the risk classification of customers and regular monitoring. It should be noted, however, that the FIU has received several notices regarding the suspicion of money laundering through remittances.

RISK CLASSIFICATION

HIGH

Considering the above discussion, the risk of money laundering in cash transfer operations is deemed high.

4.3.6. FOREIGN EXCHANGE TRANSACTIONS WITH CASH

RISK CLASSIFICATION



GENERAL

Foreign exchange transactions refer to the act of “*exchanging domestic currency for foreign currency, foreign currency for domestic currency or one foreign currency for another foreign currency, and to credit transactions which are analogous to such delivery or reception of currency.*” according to Article 2 of the Foreign Exchange Act no. 70/2021. This section will only discuss foreign exchange transactions with cash where the money is not stored in a payment account.

Credit agencies are authorised for foreign exchange transactions based on the Act on Financial Undertakings no. 161/2002. Also, the purchase and sale of foreign exchange occur at money exchange services that are subject to mandatory registration under Article 35 of the AML Act at the CBI. The definition of a money exchange service in item 8, Article 3 of the AML Act is as follows: “*a business activity which, in the way of business, engages in buying and selling domestic and foreign currency*”. Furthermore, rules regarding the registration of foreign exchange services and crypto-asset service providers no. 151/2023 apply.

In September of 2023, the commercial banks and savings banks were authorised to engage in money exchange transactions. From June of 2019 one foreign exchange service provider obliged to be registered operated in this country, a company which was, at its own request, removed from the register of the CBI in October of 2022.

According to CBI information, the turnover of cash transactions in foreign exchange in the country from 2018 to 2022 mostly took place in euros (55.5%) followed by us dollars (21.5%). The development of the total turnover of commercial banks and savings banks in foreign currency in this country during the past few years was as follows:

- In 2018 – ISK 83.6 billion
- In 2019 – ISK 87.1 billion
- In 2020 – ISK 23.3 billion

- In 2021 – ISK 15.8 billion
- In 2022 – ISK 24.7 billion

It's evident that the coronavirus pandemic has greatly affected the turnover, as the share of domestic entities in the turnover amounted to 82% in 2022.

THREATS

In Iceland, the need for purchases of foreign currency should be on the wane, in light of widespread use of payment cards and increased electronic payment means. There are, however, instances of what might be called reasonable foreign currency purchases, as most individuals purchase foreign currency, for example, for trips abroad, but even for those the need is decreasing with the increased use of cards and ATM's. It may also be noted that there is a rich tradition for the use of cash in certain parts of the world and Iceland is an increasingly open and international society with an increased number of tourists, refugees and immigrants who come to work for long or short periods of time. However, the scope of foreign exchange transactions in cash is far greater than one might assume to be necessary.

It's clear that parties affiliated with organised criminal activities exchange significant amounts of Icelandic króna for foreign currency. This may be read in the context of internationally known money laundering methods such as smuggling cash from the country.⁹⁷ This is also done to finance further criminal activities, such as drug imports, and the scope of such violations is deemed to be significant. In this context, offenders are known to do this in an organised fashion and use a network of straw men who have no documented relations with the beneficial owners of the money. The profit of the criminal activity is, thus, divided into many smaller portions, which may even be taken to many bases of operations in the aim of disguising the origins of the funds, avoiding suspicions and dodging surveillance. This method of perpetration is to be examined considering accessibility to remittances in this country and the ease of transporting cash over borders, cf. discussions in other sections of the risk assessment. Also, specialised skills or technological know-how is not required to launder money this way and access to foreign exchange services is fairly good. Finally, notices to FIU of suspicious foreign exchange transactions are rather common and their scope is great.

WEAKNESSES AND MITIGATING FACTORS

Usually, transactions in foreign currency are not anonymous. Nevertheless, through the years there has been a number of foreign exchange transactions with entities who have no ID number and present foreign identification and

⁹⁷ FATF Report. *Money Laundering Through the Physical Transportation of Cash*. FATF, Paris 2015.

it can prove difficult to acquire oversight and surveillance of such customers. There are indications that the commercial banks have added to their requirements related to foreign exchange transactions.

Despite the risk awareness of parties subject to mandatory reporting being deemed acceptable, there are still weaknesses, amongst other things regarding risk assessment of operations, risk classification of customers, due diligence and regular monitoring of transactions, including the registration and traceability of information. Parties subject to mandatory reporting in this market conduct surveillance of foreign exchange transactions, amongst other things, through branches and transaction monitoring systems. However, such monitoring has been found to have several weaknesses.

The legal framework for foreign exchange is deemed acceptable, and the monitoring of parties engaging in foreign exchange transactions is thorough. In this context, it may be noted that the CBI examined the operations of foreign exchange services in 2022 where there were found to be shortcomings in the implementation of anti-money laundering and terrorist financing measures and an agreement was reached to settle that case.⁹⁸ Also, educational materials regarding this issue category have been updated.

RISK CLASSIFICATION

HIGH

Considering the main threats and weaknesses, after taking into account mitigating factors, this risk component of foreign exchange transactions is deemed high.

⁹⁸ [FX_true_10082022.pdf](#)
(sedlabanki.is)

4.3.7. ISSUE OF ELECTRONIC MONEY

RISK CLASSIFICATION



GENERAL

Electronic money is defined in the Act on the Issuance and Treatment of Electronic Money no. 17/2013 as follows: *“Monetary value in the form of a claim against the issuer that is stored in an electronic medium, including in magnetic form, issued in exchange for funds, to execute payment in the meaning of the Act on Payment Services and approved as such by parties other than the issuer.”*

A key characteristic of electronic money is that it is prepaid. This means that assets must be paid into an account, card, or equipment for it to be deemed electronic money. Electronic money has many different characteristics, including the possibility of reloading electronic money into an appropriate medium. In addition, cards can be connected to other electronic money, e.g. accounts on the Internet. Some types of electronic money have throughout the years been registered to the owner of the electronic money while others are issued to the holder, such as gift cards. In this country, only those who have presented recognised identification receive electronic money.

In this country, the bigger commercial banks, savings banks, and credit companies have issued electronic money. Some of these parties issue prepaid payment cards, but only the banks and savings banks also issue “gift cards”. There are also instances of electronic money being issued to a blockchain and, on the other hand, an custodian wallet. The total turnover on the domestic foreign exchange market in the year 2022, according to information from the cbl, amounted to approximately ISK 31 billion. Of this amount, gift cards for just under ISK 5.2 billion were issued.

THREATS

The main threat regarding the use of electronic money is especially related to possibilities for misuse. Contrary to gift cards, prepaid payment cards can be reloaded. In most instances, it is possible to load more than ISK 500,000 into each such card. It can also be permitted to pay with the card an amount exceeding ISK 250,000 per entry, and in some instances, it is possible to load cash into such cards. Finally, in some instances, it is possible to withdraw cash from prepaid cards and in most

cases there are no limits to how many cards each party can purchase.

Transporting high amounts of money between countries in the form of electronic money is easy and the cards can be used everywhere in the world, including internet shops. Also, it is quite possible to conceal the trail of funds with gift cards, as their characteristics in this respect are similar in this regard.

Reports of suspicious electronic money transactions are very few and electronic money, issued by domestic issuers, very seldom comes up in police investigations related to money laundering. On the other hand, the prepaid payment cards of new, foreign financial companies have begun to appear more often in police investigations, which is in line with the development taking place in the surrounding countries. The purpose of the use of such cards is deemed to be the concealment of the trail of ill gotten funds and the evasion of further surveillance. The services of financial companies who are subject to mandatory reporting outside Iceland are discussed further in another section of the risk assessment.

WEAKNESSES AND MITIGATING FACTORS

Despite the defences of parties subject to mandatory notification being strengthened in recent years and seasons, there are weaknesses in compliance with the AML Act, including risk assessment of operations, customers' risk classification, due diligence and regular monitoring of transactions.

However, the legal framework is deemed satisfactory, and the monitoring considers risk. The few notices to FIU indicate that risk awareness in these operations is deficient.

A mitigating factor worth mentioning is that the surveillance of parties subject to mandatory reporting of payments into prepaid cards is similar to that of other payments. Therefore, it may be assumed that their monitoring system issue warnings in the case of inordinate, complex or extensive payments into prepaid cards, especially in the case of cash withdrawals. Surveys have suggested, though, that the monitoring systems have a few weaknesses.

Finally, it bears repeating that transactions with electronic money are not anonymous and amounts are restricted. Also, educational materials have been published regarding these operations.

RISK CLASSIFICATION

HIGH

Regarding the above threats, weaknesses, and mitigating factors, the risk of money laundering related to the issue of electronic money is high.

4.3.8. TRADE AND SERVICES WITH CRYPTO-ASSETS

RISK CLASSIFICATION



GENERAL

Act no. 62/2022 amended the AML Act. That which triggered the amendments may be traced to changes in the recommendations of the FATF related to crypto-assets, which were finalised in the year 2019. The amendments involve, amongst other things, the use of the word crypto-assets instead of cryptocurrencies. After the amendments, the following definitions related to crypto-asset services can be found in the act:

„Crypto-assets: Any valuables in digital form:

- A** *which can be used as payment or investment and which can be shared, and*
- B** *which are not considered digital currency in the sense of the Act on the Issuance and Treatment of Electronic Money or currency issued by a central bank or other authorities.*

Crypto-asset service provider: Customer, private or legal party who:

- A** *exchanges crypto-assets for currency or electronic money,*
- B** *exchanges currency or electronic money for crypto-assets,*
- C** *exchanges crypto-assets for other crypto-assets,*
- D** *preserves, endorses, or transfers crypto-assets on behalf of another individual or legal entity,*
- E** *provides services pertaining to the issuance, tender or sale of crypto-assets,*
- F** *is the service provider of custodian wallets, according to the definition in item 20, or*
- G** *otherwise oversees crypto-assets for business purposes.*

Custodian wallet service provider: A natural or legal person which offers services for the management of ‘private keys’ for virtual currency (cryptocur-

rencies,) whether this is done through software, systems or another means of managing, keeping and transferring virtual currency (cryptocurrencies.)”

Service providers of cryptocurrencies are obligated to register with the CBI, cf. Article 35 of the AML Act. CBI surveillance with the operations of these parties covers anti-money laundering and terrorist financing measures but not financial surveillance. The legislation covers only those providing services in connection with cryptocurrencies, e.g. parties converting cryptocurrencies into electronic money or currency (or vice versa) and exchanging one cryptocurrency for another cryptocurrency. In general, such parties can accept several payment media, such as cash, transfers from a bank, from a credit card or other cryptocurrencies. This could involve exchange pages on the Internet or so-called Automatic Teller Machines that exchange crypto-assets.

In this country, four parties were registered at the CBI as crypto-assets service providers in September of 2023, including one who was registered in the year 2023. These are entities which operate exchange markets between crypto-assets and one issuer of crypto-assets. No ATM in this country provides crypto-assets. The total amount of these transactions in the country has increased greatly in the past few years, amounting to somewhere from 2 to 4.3 billion each year in the years 2020-2022. The number of customers has also grown but the share of foreign customers is low.

THREATS

The scope and economy of crypto-assets has increased quickly in Iceland and world-wide, with respect to both the number of transactions and number of customers, but also with regard to where and how crypto-assets can be used as a means of payment and investment. Transactions in crypto-assets are by their very nature international and flow freely across borders. It can also be difficult to figure out the origin of crypto-assets and an actual owner despite it generally being possible to trace the path of transfers in crypto-assets in blockchains up to a certain point, as it is not always possible to acquire information regarding the party who is involved in the transaction. No official register of the owners or address holders who store crypto-assets is available. Also, transactions with crypto-assets generally occur in telecommunications and great speed characterises these transactions. These features are all attractive for parties who seek to transfer the gains of unlawful operations from one state to another, operate outside traditional borders, disguise their beneficial ownership and launder money.

There are indications that in Iceland, offenders have begun allocating profits from criminal activities into purchasing crypto-assets in the aim of laundering money. There are also indications that crypto-assets are used as a

method of perpetration to get money out of the country instead of previously better known ways which are even considered riskier and slower, for instance, cash smuggling.

Although the police has had to deal with relatively few cases related to crypto-assets, it is considered almost certain that their use for money laundering will increase in parallel to their expanded use, and as offenders develop methods to utilise them. The crypto-asset economy is still young and risks related to money laundering and terrorist financing are still emerging.

WEAKNESSES AND MITIGATING FACTORS

In Iceland, four service providers for transactions between crypto-assets are in operation. In order to engage in business through these parties, customers need to identify themselves with fully valid electronic ID and generally to link the transfer market account to bank accounts or credit cards. Also, Icelandic crypto-asset service providers don't accept cash as the business runs solely on the internet and they generally don't offer crypto-asset transactions which are expressly designed to conceal ownership. Furthermore, no ATM in this country provides crypto-assets. As a mitigating factor, it should be noted that crypto-asset markets can be unstable and value can fluctuate dramatically which may serve as a certain deterrent. It's important to note, though that Icelanders have access to foreign crypto-asset service providers and neobanks through the internet, which are not subject to mandatory reporting in Iceland and not subject to money laundering surveillance by the CBI and it is therefore clear that business by offenders and other Icelanders in crypto-assets are not limited to crypto-asset service providers, as further outlined in another section of the risk assessment.

There are indications that the risk awareness of some parties engaged in this business is limited and that there are still weaknesses with regard to risk assessment of operations, risk classification of customers and regular monitoring. There have been a few reports of suspicious transactions from crypto-asset service providers and the number of those reports has been on the rise, although they are still few.

Unlike other parties in the financial market, crypto-asset service providers are not subject to other legislation than the AML Act. In other words, these parties do not have to fulfill any other requirements other than those of anti-money laundering and terrorist financing measures, which increases risk within those operations. It's important for all EU regulations regarding crypto-assets and crypto-asset service providers to be legalised in Iceland as quickly as possible.

Finally, one should note the lack within the Financial Intelligence Unit (FIU) and the police of necessary equipment, protocols and specialisation to conduct analysis, trace transactions and investigate cases related to crypto-assets. The FIU and the police are provided with the assistance of foreign police depart-

ments and institutions in this respect. Nevertheless, this hampers reactivity and the possibility of seizing ill gotten funds in the form of crypto-assets. Also, tools of analysis in this field are expensive and it is not clear whether a country like Iceland will be able to run such systems. Vigorous international cooperation is the precondition for success in this field. The increased spread and usage possibilities of crypto-assets, within and without the traditional economy, come with various challenges for the police and other supervisors.

RISK CLASSIFICATION
HIGH

Regarding the above threats, weaknesses, and mitigating factors, the risk of money laundering related to crypto-asset services is deemed high.

4.3.9. TRADE AND SERVICES FOR FINANCIAL INSTRUMENTS

RISK CLASSIFICATION

GENERAL

Mandatory operating permits for transactions and services for financial instruments under Act no. 115/2021 on Securities Transactions in Iceland entail the following:

- C** Receipt and brokerage of directions from customers on one or more financial instruments.
- D** Execution of orders on behalf of customers.
- E** Dealing on own account.
- F** Asset management.

- G** Investment advice.
- H** Underwriting in connection with the issue of financial instruments and/or tenders of financial instruments.
- I** Supervising tenders of financial instruments without underwriting.
- J** Operation of a marketplace for financial instruments (MFI.)
- K** Operation of an organised marketplace.

Four banks, eight securities companies and one credit company are authorised to engage in transactions and services for financial instruments under Act no. 115/2021 in September 2023. These companies offer all of the aforementioned services except for the operation of a marketplace for financial instruments and the operation of an organised marketplace. The securities companies were also not authorised for dealing on their own account. It varies whether the aforementioned entities offer their services to individuals or focus on financially well-off entities and legal entities, ie. so-called professional investors. Several entities offer the purchase and sale of securities on foreign markets.

Asset management, or private banking service, as it is sometimes called, is offered by the four commercial banks and the credit company. Six out of eight securities companies engage in asset management. One of them, however, provides such services only to pension funds. According to information from the CBI, the total amount of assets being managed by banks and securities companies in the year 2022, aside from the assets of pension funds, was over ISK 1,392 billion, having risen slightly from one year to the next.

THREATS

The main threats related to securities services are receiving considerable assets from customers since they often involve financially strong individuals and legal persons. Customers involved in business with financial instruments are generally deemed more risk-seeking than, say, traditional commercial bank customers. High amounts go through parties offering securities services and often a certain degree of complication, connections across borders and speed characterise the transactions. Accessibility to these services is also relatively good, and investment in financial instruments generally does not require great expertise. However, the expertise of customers is one of the things which determine whether the party in question is considered a common investor or a professional investor. Also, operations across borders with the parties subject to mandatory reporting who operate in this field are not deemed extensive, the proportion of foreign customers is comparable to that which is usual in the commercial banks and there are few examples of customers who reside in risky or uncooperative states.

Few police cases have arisen where there is suspicion of financial instrument trades being used for money laundering.

WEAKNESSES AND MITIGATING FACTORS

There are indications that the risk-awareness of the parties involved in these operations is limited and that there are weaknesses, amongst other things regarding risk assessment of operations, customers' risk classification, due diligence and risk-based monitoring, amongst other things related to the registration and traceability of information. Most parties subject to mandatory reporting have transaction monitoring systems to monitor the operations. However, surveys have detected several weaknesses in such monitoring. Reports of suspicion of money laundering in this operation are few, which may indicate that mandatory reporting is not conducted sufficiently.

On the other hand, it serves as a mitigating effect on the operation that the obligation of parties to gather information on customers is based on two pieces of legislation. On the one hand, the AML Act and on the other hand, the Act on Markets in Financial Instruments no. 115/2021. Thus, these parties are in reality subject to more requirements to know their customers than parties in other markets. Finally, anonymity is not allowed, neither are bearer bonds and there are almost no cash transactions.

RISK CLASSIFICATION

MEDIUM

Considering the above, transactions and services for financial instruments entail medium risk regarding money laundering.

4.3.10. OPERATION OF FUNDS

RISK CLASSIFICATION



GENERAL

The operations entail the operation of funds and sale of share certificates to the public and, depending on circumstances, to professional investors. The underlying assets of the funds can be shares, bonds, certificates and other funds and other assets, such as real estate and deposits. Investors usually buy into funds through their commercial banks or brokers.

Six operating companies of securities funds have operating permits in Iceland, under the Mutual Funds Act no. 116/2021 in September 2023. These operating companies are also authorised to be operators of specialised funds, cf. the Act on Operators of Specialised Funds no. 45/2020. Also, there are five operators of specialised funds who require licences and 17 operators of specialised funds obligated to register, cf. Act no. 45/2020 and their number has greatly increased in the past two years.

The total assets of securities funds, investment funds, and professional investor funds (specialised funds other than investment funds) were as follows:⁹⁹

- In 2020 – ISK 936 billion
- In 2021 – ISK 1.193 billion
- In 2022 – ISK 1.151 billion

The share of total assets of the GDP was about 30% in 2022. The main owners were pension funds and insurance companies (35%) and homes (29%) while only about 1% is owned by foreign entities.

THREATS

The main threat of the operations of management companies of securities funds regarding money laundering is that the amount of investments in funds is considerable. It is generally easy to engage in transactions with units in funds and access to them is considerable, especially to the funds always open to redemption. Also, the operations are tied to the domestic market and investment

⁹⁹ [Figures \(sedlabanki.is\)](https://sedlabanki.is)

by foreign entities is not extensive. Customers need a good working knowledge of the financial market to be able to launder unlawful gains through funds. However, offenders are able to seek the assistance of specialists like everyone else. Few police cases have arisen where there is suspicion of funds being used to launder unlawful gains.

WEAKNESSES AND MITIGATING FACTORS

Commercial banks that usually handle second-tier monitoring for management companies are generally sufficiently aware of the risk of money laundering. On the other hand, surveillance indicates that there are deficiencies in risk assessment of operations, customers' risk classification, due diligence and regular monitoring by the commercial banks.

Risk awareness of operating parties and the operating companies of funds is generally deemed acceptable. There are few examples of notices related to money laundering in fund operations, which may indicate that regulatory measures are not sufficiently executed.

A mitigating factor worth mentioning is that the operating companies and operating parties have no branches in other countries and rarely operate across borders. The number of foreign customers of these companies is negligible and their total ownership share is about 1%. Also, there are generally no cash transactions in this area and anonymous transactions are not allowed

RISK CLASSIFICATION

MEDIUM

Considering all this, the risk related to money laundering in the operation of funds is deemed medium.

4.3.11. OPERATION OF PENSION FUNDS

RISK CLASSIFICATION



GENERAL

Coinsurance: In Iceland there is a mandatory coinsurance system and according to it, all wage earners and independent operators from the age of 16 to the age of 70 are to contribute to a pension fund. Under the provisions of Act no. 129/1997 on Mandatory Insurance of Pension Fund Rights and the Operations of Pension Funds, a pension fund premium for minimum insurance protection and supplemental insurance protection shall be paid monthly, and pension funds must report to the tax authorities what annual premium has been paid to them for each entitled person. The main rule is that payments from coinsurance pension funds ensure entitled persons lifetime payments under the rights that fund members have acquired with their premiums. This, therefore, generally does not involve proper rights that are redeemable or assignable to other parties.

Private Pension savings: Under the provisions of Act no. 129/1997, commercial banks, savings banks, securities companies, life insurance companies and pension funds may accept private pension savings whether they are for minimum insurance coverage or supplemental insurance coverage. Payments into a private pension savings account always build on an agreement between an employer and an employee and are a certain percentage of wages. Legal persons cannot pay into a private pension savings fund, and individuals cannot pay into such funds independently. That is, payments into these funds are always linked to wages, and the wage payer sees to deducting the payment from the employee's wages and turning it over, along with its matching contribution, to private pension savings funds.

A pension fund premium for minimum insurance coverage and supplemental insurance coverage for private savings shall be paid monthly, and depositories, which are all subject to mandatory reporting, must report the annual premium paid for each entitled person to the tax authorities, for the accrual of pension rights. In addition, Act no. 129/1997 forbids withdrawing the balance until two years after the first premium payment, provided that specified conditions are fulfilled. That is, the person involved has reached the age of 60 or is a confirmed disabled person, or the death of the entitled person is involved. How-

ever, foreign citizens may get pension payments after they have moved away from the country. Pension fund payments are taxed as income when paid. Twenty-one pension funds are operating in Iceland and their total net assets in the year 2022 amounted to ISK 6,620 billion, which is 180% of GDP.¹⁰⁰ In addition, the commercial banks and savings banks and two foreign entities are authorised to provide contracts for additional insurance cover in this country. Pension funds are one of Icelanders' most important savings options.

Also, most pension funds in this country offer loans to fund members, although there are limits on lending to them. Money laundering risk related to lending operations is covered in another section of the risk assessment.

THREATS

There are no examples of pension funds having been used in Iceland to launder money. Such would require expertise and organisation. The main risk involves paid premiums having been acquired with criminal activities.

WEAKNESSES AND MITIGATING FACTORS

Although the amount of money in pension funds is substantial, the following mitigating factors in the operation must be kept in mind. Pension funds must report to the tax authorities all premiums paid to them that year for each entitled person. Common funds do not entail rights to redemption or assignment. Payments into private property funds are always linked to an employee's wages and it is forbidden to pay lump sums into private property funds. It is not possible to redeem rights in private property funds except under specific conditions, based on age, disability, or death and when foreign citizens move away from the country. Finally, the payments go through accounts at financial companies and, therefore, there is no use of cash.

Given the operation, risk assessment is deemed acceptable, as well as the legal framework and monitoring, after considering the risk. Also, there are no examples of money laundering through pension funds in the country and the FIU has received no reports of suspicious behaviour.

RISK CLASSIFICATION

LOW

Considering the above, the risk of the pension funds' system being used to launder illegitimate gains and the risk of money laundering in pension funds' operations is deemed low.

¹⁰⁰ [1. Assets | Lifeyrismál.is \(lifeyrismal.is\)](https://lifeyrismal.is)

4.3.12. LIFE INSURANCE OPERATION

RISK CLASSIFICATION



GENERAL

Life insurance companies and insurance agencies, when they broker life insurance or other risk- and collection based life insurance, are subject to mandatory reporting, according to the AML Act. The brokerage of life insurance means presenting, offering, or otherwise preparing agreements on such products, closing such agreements, or assisting with their execution.

Four life insurance companies have operating permits for life and health insurance under Article 21 of Act no. 100/2016 on Insurance Operations. Also, nine insurance brokers are authorised to broker life and health insurance for insurance companies under Act no. 62/2019 on the Brokerage of Insurance, and all except one of them do so. Also, one branch of a foreign life insurance company is operating in the country and two branches of foreign insurance agencies.

Life insurance companies and life insurance agents offer various investment products, including risk and cash-component life insurance. It is possible to set up the products so that they are collection-related, indexed or are or are not with a life insurance component from the life insurance company (also called life insurance-related investment products.) The risk can therefore lie with the insured or the life insurance company.

According to information from the CBI, only one of the four life insurance companies offered collection-related health- and life insurance for sale in September of 2023 and the total amount of premiums for these insurance policies in 2022 was only a small portion of the total scope of premiums for health insurance and life insurance. The total amount of premiums for life insurance products which were paid to insurance agencies and branches, which provided collection-related health insurance and life insurance from foreign life insurance companies in 2022 was around ISK 20 billion.

THREATS

The main threat of money laundering related to life insurance entails risk- and cash-component life insurance, where parties use the product as an investment and can deposit money with a life insurance company and withdraw such funds

as needed. There are no indications or examples of money laundering through life insurance operations in this country, as the complex arrangement of the operation, through which great expertise is required to launder money, indicates that this way is not a feasible option in such matters. The FIU has received no notices of money laundering connected with life insurance.

WEAKNESSES AND MITIGATING FACTORS

Accessibility to life insurance services is high. However, the threat is limited because of the low percentage of risk and cash-component life insurance products, compared to the total scope of life insurance. Anonymous transactions are forbidden, and the annual amount paid into cash-component insurance is low. Risk awareness is deemed acceptable, as well as the legal framework and monitoring, after considering the risk.

RISK CLASSIFICATION
LOW

The risk of money laundering through life insurance operations is deemed low.

4.3.13. DIGITAL FINANCIAL SERVICES MONITORED BY OTHER STATES

RISK CLASSIFICATION

GENERAL

So far, the financial services available in the Icelandic financial market subject to CBI surveillance have been covered. In this section the risk of digital financial services accessible in Iceland while subject to monitoring by other states is assessed.

In this context, one should mention digital banks who do not have actual branches and financial technology services (*fintech*) and most of which are only accessible online, through apps or a web-based interface. These banks and tech solutions can have differ-

ing licenses in their home country and can, thus, be categorised in various ways, e.g. as financial institutions, electronic money companies or payment agencies. In many cases, therefore, the services in question are the same and/or comparable to those offered by the commercial banks and other, more traditional entities on the financial market. From providing deposit accounts, payment tech and payment cards to transactions with financial instruments. However, here we refer only to ATM's in Iceland, the many electronic money tech on offer, as well as various kinds of services for crypto-assets. Also, services of this type may be related to financial systems which exist within computer games and social media platforms. The selection of products and services in question is wide and, therefore, it's hard to speak of a certain market. The common feature of these companies is that they offer some sort of digital financial services in this country without being subject to monitoring.

Reports of service across borders (*passporting*) enable companies subject to mandatory monitoring registered within the EEA to conduct their business in any other EEA-state without requiring further authorisation from the country in question.¹⁰¹ This way is especially important for financial companies located within the eurozone who operate across borders. Icelandic citizens can, thus, become customers of foreign entities in the financial market if they have reported to supervisors in their own homeland of the provision of services in this country and if the supervisor has sent a report to the CBI to that effect.

Basically, the same risk of money laundering arises with this tech as in other comparable tech from financial companies which are subject to mandatory reporting and monitoring in Iceland, and which have been covered in other sections of the financial market portion. As many different tech solutions fall under this assessment factor, their risk varies and each of them will not be precisely analysed here. Therefore, an attempt will only be made to cover in general the additional threats and weaknesses which present themselves in digital financial services by companies subject to monitoring by other states. It should be noted that as this is not Icelandic monitoring, it's difficult to acquire information, for instance, about the scope and, therefore, it is more difficult to precisely assess the risk. That, in and of itself, causes certain risks.

THREATS

Fintech is usually user-friendly and quick and business can easily be set up. An efficient institutional process may negatively effect the quality of due diligence, however. The services are irrespective of boundaries, and so the user need not reside in the same country as their headquarters in order to utilise the services. Communication is also usually digital from beginning to end, i.e. the customer never needs to meet or speak with an employee of the company. The aim is usually to simplify matters for customers and thus to bypass the often more gruelling and complex processes of more traditional financial institutions. Therefore, this service is often less expensive than comparable services.

The supply of fintech has increased significantly in recent years. According to in-

¹⁰¹ [Passporting and supervision of branches | European Banking Authority \(europa.eu\)](#)

formation from the website of the data- and statistics company Statista, fintech-companies world-wide in August 2023 numbered more than 26,000.¹⁰² At the same time there were 272 neo banks or digital banks operating in the world, whereof 99 were in Europe, according to the website NeoBanks.app.¹⁰³ There is no formal or legal definition of the word neobank, but it usually refers to a financial company with a commercial banking licence which offers only digital services. Sometimes, these banks are referred to as challenger banks, as the founders of many of these companies have decided to challenge well-established commercial banks to a competition for customers by offering digital, user-friendly and inexpensive services. In some cases, these are small fintech-companies who have then later had to apply for a commercial banking licence when they decided to offer services for which a commercial banking licence is required, for instance, taking deposits.

In a poll conducted by Gallup for the cbi in the spring of 2022, individuals were asked whether they use foreign mediums of exchange such as Paypal, Alipay and Revolut. Almost half of the respondents said that they had at some point used such tech solutions.¹⁰⁴ Although the scope of it is unknown, it's clear that the supply of fintech belonging to this assessment factor is substantial and that there are indications that Icelanders are increasingly using them to a significant degree.

The business model of various fintech companies provide offenders with the opportunity to operate in certain secrecy and are often built on atypical means of payment. Exchanges can be made between currency and crypto-assets and transactions can revolve around the transport of money across borders, which more often than not work faster than similar transactions by more traditional means which are often more stringently monitored. In the Nordic Countries, offenders are known to utilise foreign digital banks in order to launder money acquired by criminal activities.^{105,106} There are also indications that Icelandic offenders have begun utilising fintech to launder money, amongst other things to get money out of the country.

It is considered likely that the operation and scope of digital banks and other fintech will continue to grow and that offenders will increasingly use these means to launder money, and that the associated threat goes hand in hand with the increasing technological development of the financial world.

WEAKNESSES AND MITIGATING FACTORS

In the public arena there have been discussions of large entities in this market finding it difficult to fulfil requirements regarding anti-money laundering and terrorist financing defences and that there are examples of high fines against these companies.¹⁰⁷ While the companies promise redress, new ones pop up at the same time and it is imprudent to assume that comparable issues won't arise with them.

The digital fintech companies discussed under this assessment factor have operating licences abroad and are therefore not subject to mandatory reporting in Iceland. Consequently, the cbi doesn't have the same surveillance responsibility with regard to an-

¹⁰² [Number of fintech startups globally by region 2023 | Statista](#)

¹⁰³ [The list of neobanks and digital banks in the world in 2023 | NeoBanks.app](#)

¹⁰⁴ *Financial Stability, 2022(2)*. cbi, Reykjavik, Volume 31. 28 September 2022, pg. 45.

¹⁰⁵ *Neobanker – En rapport om neobanker och deras risker relaterade till penningtvätt och finansiering av terrorism*. Polismyndigheten, Stockholm 2022.

¹⁰⁶ *Den nationale risikovurdering af hvidvask*. Hvidvasksekretariatet 2022. Danmarks finansielle efterretningsenhed (FIU), Kaupmannahöfn 2023, pg. 133.

¹⁰⁷ [German watchdog BaFin orders N26 to pay \\$5 million fine | Reuters, Sanctions on Revolut group companies | Bank of Lithuania \(lb.lt\)](#)

ti-money laundering and terrorist financing as with companies who conduct operations subject to official authorisation or registration. Reports of suspicious transactions are to be sent to the FIU in the country where the company is listed, irrespective of the citizenship of the business person. This means that the quality and scope of the surveillance depends on the abilities of foreign supervisors. This also creates a need for increased cooperation and dissemination of information between the FIU in different countries. Shortcomings in the international cooperation of authorities regarding reports of suspicious transactions can lead to states being in danger of having limited knowledge of the financial standing of their citizens.

It is rare for the FIU to receive information regarding suspicious transactions from foreign sister institutions regarding business between Icelanders and foreign fintech companies. When examined in the context of the number of tech solutions and the fractures regarding money laundering which have been discussed in the public arena related to large, international fintech companies, it may be considered likely that the low number of reports are attributable to lackluster monitoring and/or risk awareness rather than the service being rid of all risk.

Different markets are largely subject to similar risk but they can also differ greatly from one country to the next. It is not certain that fintech companies with customers in many countries are made aware of local circumstances outside their homeland and their risk assessment of customers in other countries may be limited. Therefore, this can create a situation which offenders can abuse.

Financial services and payment solutions keep becoming simpler for customers to use and the need for a great deal of expertise, even for the execution of complex financial instruments, has lessened. At the same time, various offshoots of the financial industry are based on technology no less complex, e.g. blockchain-technology. In some instances, it may be that the service, implementation or tech in question is not offered by fintech companies with an operating licence in Iceland. It can be difficult for supervisory bodies and the police, with their limited human resources, to retain specialists and analytical tools in all areas. From a research standpoint, the use of digital financial services with headquarters in different countries means, furthermore, that there is a risk of relatively simple transactions becoming complex to investigate.

Finally, it should be noted that one may assume that there are significant deficiencies in reporting to the tax authorities of finances which are stored with digital financial service companies subject to monitoring by other states.

RISK CLASSIFICATION

HIGH

Considering all this, the risk of digital banks and other digital financial services subject to monitoring by other states being misused to launder money in this country is high.

4.4. SPECIALISTS

The following sections discuss specialists. Specifically included are attorneys, accountants, bookkeepers, estate agents, ship brokers, and car salesmen, jewellers and gold buyers and art sellers and dealers. These are specialists who are subject to mandatory reporting according to the AML Act. The aforementioned parties provide assistance related to business and operations in their area of expertise. As the case may be, such services can be the precondition for, or an item of, various types of payments, settlements and transactions with financial companies. In this context, specialists are sometimes described as gate-keepers. This report will examine whether there is risk that criminals or organised crime will utilise the services of such specialists, e.g. by getting them to handle transactions on their behalf, found companies or assist with book-keeping and accountancy for the purpose of laundering unlawful gains or concealing the beneficial ownership of companies and assets resulting from unlawful operations.

It may be that such specialists are unwitting participants in the money laundering of customers as there are no clear warning signs of money laundering or if the customer provides seemingly reasonable explanations of their business and the origins of their money. In other cases, clear warning signs may arise but such warning signs go undetected due to lack of knowledge of money laundering methods. A situation may also arise where a specialist detects warning signs but refrains from further examining the matter and does not employ sufficient defences or that the specialist is a willing participant in the money laundering and takes fees for it. Examples from abroad demonstrate that specialists offer special money laundering services to offenders.¹⁰⁸

According to the AML, the Directorate of Internal Revenue maintains surveillance of the aforementioned specialists. The Directorate of Internal Revenue is authorised to take appropriate measures during monitoring, if necessary, such as applying penalties and coercive remedies. The Money Laundering Division of the Directorate of Internal Revenue provides specialists subject to mandatory reporting with education and examines their compliance with the AML Act.

¹⁰⁸ *EU Serious and Organised Crime Threat Assessment (SOCTA) 2021 – A Corrupting Influence: The Infiltration and Undermining of Europe's Economy and Society by Organised Crime*. Europol, Luxembourg 2021, pg. 11 and 15.

ESTIMATED NUMBER OF ACTIVE SPECIALISTS ACCORDING TO INFORMATION FROM THE DIRECTORATE OF INTERNAL REVENUE 2023

Table 11

Profession of specialists	Estimated number
Attorneys	733
Accountants	315
Bookkeepers	~1300
Estate agents	636
Ship brokers	~10
Car dealers	~350
Jewellers and gold-buyers	~80
Art sellers and art dealers	~30

The following table shows the estimated number of active specialists in each trade, according to the information of the Directorate of Internal Revenue in the autumn of 2023.

As threats, weaknesses and mitigating factors were assessed, the supporting information was from various supervisors, the police, the FIU, the Directorate of Tax Investigations, representative organisations of various professions and the pertinent legislation.

The following are the main threats and weaknesses and mitigating factors which pertain to specialists operating in Iceland under the surveillance of Iceland Revenue. Risk related to each type of specialist will be covered further in the following sections:

- Information from the police indicates that certain parties involved in organised criminal activities in this country have, by dint of their financial strength and activity, easy access to specialists prepared to assist them in money laundering, for instance, regarding book keeping, real estate transactions and business with financial institutions. It must be assumed that such operations have the ability and expertise to employ advanced and complex money laundering methods.
- The Money Laundering Division of the Directorate of Internal Revenue is the supervisor of compliance to the AML Act by specialists subject to mandatory reporting. The surveillance is risk-based but due to its scope it has certain weaknesses. The group in question consists of specialists belonging to different professions who each number numerous parties.

- In many instances, the representative organisations of specialists operate according to their own conditions of qualifications and codes of ethics. On the other hand, in many cases, membership in these organisations is not mandatory. The representative organisations have proven beneficial, amongst other things when it comes to the dissemination of information, education and restraint of their members.
- Supervisors and various representative organisations have conducted lectures for parties subject to mandatory reporting, on matters related to money laundering and terrorist financing. The authorities have also been involved in publishing educational materials for experts.¹⁰⁹
- According to the Money Laundering Division of the Directorate of Internal Revenue, the risk awareness of specialists has, in general, increased since the AML Act was entered into force. However, the risk awareness differed greatly between professions. The FIU rarely receives notices of suspicious transactions from these professions, which is noteworthy due to the scope and inherent risk of their professions. Lack of reporting may indicate that there is still a lack of risk awareness among specialists.

4.4.1. ATTORNEYS

RISK CLASSIFICATION



GENERAL

Law firms, attorneys and other specialists are parties subject to mandatory reporting in the meaning of the AML Act when they:

- See to or represent their clients in any kind of financial or real estate transactions.

¹⁰⁹ [Parties subject to mandatory reporting who are subject to surveillance by the Directorate of Internal Revenue | Parties subject to mandatory reporting | Iceland Revenue – taxes and fees](#)

- Assist with organising or executing transactions on behalf of their client regarding the purchase and sale of real estate or companies.
- See to handling clients' money, securities or other assets.
- Open or supervise bank accounts, savings bank accounts or securities accounts for clients.
- Assist in procuring capital, organising or managing funds to found, operate or direct companies.
- Assist with the founding, operating or managing of companies, funds and similar parties.

“Attorney” means a party who has completed law school and has obtained litigation rights. The professional title “lawyer” is not protected by law. However, it is generally used for someone who has completed law school but has not obtained litigation rights. Only attorneys are authorised to operate and own law firms.

According to the Icelandic Bar Association (LMFI) attorneys in Iceland numbered about 1060 by the end of September 2023. Some of these attorneys work in private companies or governmental administration and do not, therefore, see to the projects described above. The number of attorneys practising law is 733, and the number of law firms is 219. The size of law firms can vary considerably, from ones where one attorney works, or one where that attorney runs a practice under their own name, to large law firms where tens of attorneys work.

Attorneys are obligated to belong to the Icelandic Bar Association, which sets a code of ethics for its members and monitors that attorneys always fulfil the conditions for attorney certification. These include:

- Fulfilling statutory qualifications.
- Having a separate fiduciary account.
- Having valid professional liability insurance.

An attorney is obligated to provide the Icelandic Bar Association or an accountant that the association designates for this purpose, all information necessary to assess whether he fulfils the obligations directed in Article 12 of the Act on Attorneys no. 77/1998, which deals, amongst other things, with a fiduciary account and professional liability insurance. In addition, the Icelandic Bar Association can order an investigation of attorneys' finances if there is cause to do so. Cases regarding alleged violations of Act no. 77/1998 or the association's Code of Ethics are handled by a complaints board appointed by the association.

THREATS

The greatest threat from attorneys' operations is that parties will misuse their services to lend unlawful transactions or operations a lawful appearance, e.g. by getting attorneys to see to various transactions on their behalf or provide services falling under the AML Act. There is also a risk that with the involvement of these parties, the plan is to conceal the beneficial ownership of companies and/or unlawful gain, e.g. assets connected with tax evasion. In such instances the case may be that the attorney is aware that their services are being misused or that they are unaware of the fact. The tasks entailing increased risk are mainly:

- Transactions with parties with complex ownership or organisation.
- The founding of companies and bank accounts in states where there is strong banking secrecy.
- Transactions on behalf of clients with foreign financial instruments.
- Management or representation on behalf of companies owned by clients.
- Lack of information on the source of assets.
- Transactions on behalf of clients that are in a risk group.
- Transactions where the transparency of actual ownership is lacking.
- Receipt and transfer of funds on behalf of clients through the fiduciary account of the attorney.
- Transactions where the attorney never meets their client and all communication takes place online.

There are indications that attorneys have been related to cases which have been under investigation by the authorities, both the police and the DTI because of various types of aid which could be related to assistance in criminal activity. There have been very few notices of suspicion regarding attorneys sent to the FIU in recent years. This is noteworthy because of the scope of this operation.

WEAKNESSES AND MITIGATING FACTORS

Within the profession, there is an inherent risk regarding the tasks that attorneys are generally entrusted to do. On the other hand, there are mitigating factors like governmental monitoring, ample qualifications, the Icelandic Bar Association's monitoring of finances and the Code of Ethics, and the risk of disbarment.

The Money Laundering Division of the Directorate of Internal Revenue maintains surveillance by checking that attorneys fulfil their duties under the AML Act. Since the entry into force of the act, there have been several checks of attorneys

and law firms. The most recent checks indicate that attorneys generally understand their obligations under the AML Act. However, there are still indications that some attorneys do not fulfil the conditions of the act. There are examples of law firms, attorneys, and other specialists not sufficiently executing due diligence on customers, not conducting risk-based monitoring, not adequately monitoring the political affiliations of customers and related parties and whether they are subject to international sanctions and overlooking reputation while analysing transactions to assess whether they are suspicious. The above practices enable the analysis of suspicious transactions and control of risk under the aforementioned act.

The few notices of suspicion of money laundering sent by attorneys indicate that risk awareness is still lacking to some degree and/or that the financial benefits of transactions are prioritised over the risk of transactions. There are indications that some attorneys choose to be of the opinion that the work of attorneys in the commercial arena falls outside the field of application of the AML Act rather than within it. On the other hand, attorneys' risk awareness has generally been increasing with the advent of active monitoring, the issuance of educational materials and informative lectures under the auspices of the LMFÍ, supervisors and other authorities. Finally, education regarding the obligations of attorneys under the AML Act is part of a course for litigation rights before district courts.

RISK CLASSIFICATION

HIGH

Considering existing threats, weaknesses, and mitigating factors, the risk related to money laundering in attorneys' work is deemed high.

4.4.2. ACCOUNTANTS

RISK CLASSIFICATION



GENERAL

Accounting firms, accountants, tax advisors, and persons who provide book-keeping services for third parties in exchange for a remuneration are parties subject to mandatory reporting in the meaning of the AML Act. The discussion below is solely about accountants and accounting firms.

Under the Act on Auditors and Auditing no. 94/2019, all parties except accountants and accounting firms are forbidden to use the words accountant and accounting in their titles or business name, cf. Paragraph 1 Article 6 of the Act Item 4 Paragraph 1 of Article 2 of the act defines an accountant as one who has the knowledge to provide impartial and reliable opinions on financial statements and other financial information, is chartered to work in accounting, is on the Register of Accountants, and otherwise satisfies conditions of the act.

To become licensed, the person involved must fulfil the following conditions under Paragraph 1 of Article 3 of Act No. 94/2019.

- Be domiciled in Iceland or be a citizen of a member state of the European Economic Area, a member state of the Articles of Association of the Economic Free Trade Association or the Faeroe Islands.
- Have legal capacity and control over his finances and not have had his estate declared bankrupt.
- Have a good reputation and be mentally fit to work as an accountant.
- Have no judgement against him for a criminal act where punishment was at least four months' imprisonment without parole or protective custody if he had reached the age of 18 when the offence was perpetrated unless five years have passed since the punishment was fully completed.
- Have completed a master's degree in auditing and accounting that is recognised by the Accountants' Council.
- Have passed a special examination, cf. Article 7.

- Have worked at least three years under the tutelage of an accountant with auditing annual financial statements and doing other accounting at a licensed accounting firm.
- Have professional liability insurance., cf. Article 8

Accounting firms shall have a work permit and be on the Register of Accountants, under Article 4 of the Act. The conditions for an operating permit of an accounting firm are that the majority of voting rights resides in the accountants or accounting firms that are recognised in the European Economic Area or member states of the Articles of Association of the European Free Trade Association, that a majority of directors is accountants or a representative of an accounting firm, that the accounting firm has a formal quality control system, and that it is ensured that the names and addresses of the firm's owners are accessible to the public. If an accounting firm does not fulfil the above conditions, the Accountants' Council must be informed immediately, and the certification certificate turned in.

The Accountants' Council is an independent administrative committee which is financed by monitoring fees paid by accountants. The Accountants' Council sees to monitoring that accountants and accounting firms work under Act no. 94/2019 on Auditors and Auditing, the code of ethics of accountants and other regulations which pertain to the work of accountants.

According to information from the Accountants' Council, accountants in Iceland numbered 315 in September of 2023 and listed accounting firms numbered 39. All those certified for work as auditors are permitted to work in accounting. On the other hand, accountants who endorse annual financial statements must work in an accounting firm. No information is available on how many of certified accountants work in the field.

THREATS

The main threats in the operations of accountants are that parties may misuse their services to lend unlawful transactions or operations a lawful appearance, e.g. by getting accountants to attend to various transactions on their behalf or provide services falling under the AML Act. There is also a risk that with the involvement of these parties, the plan is to conceal the beneficial ownership of companies and unlawful gain, particularly assets connected with tax evasion. In such instances, the accountant may not realise that his services are being misused. In addition, there is always a risk that an accountant will be too dependent on his client and identified with his interests. The tasks entailing increased risk are mainly:

- Transactions with parties in a risk group.

- Involvement in risky transactions, for example, across borders.
- Difficulties in discerning foreign beneficial ownership.
- Services with related companies/parties with complex ownership which may even operate across borders.
- Assistance with the founding, purchasing or sale of companies, even offshore companies.
- Assistance with bookkeeping and tax returns.
- Customers having operations engaging heavily in cash transactions.
- Assistance with increasing share capital, possibly involving high sums.
- Fund management for funds.
- Endorsements of companies' accounts.

There are indications that accountants have been related to cases which have been under investigation by the authorities, both the police and the DTI because of various types of aid which could be related to assistance in criminal activity such as money laundry resulting from tax law violations. However, the FIU has received few notices from accountants in recent years.

WEAKNESSES AND MITIGATING FACTORS

There is an inherent risk within the profession that strong defences cannot fully prevent. In this regard, one must keep in mind the interests of accountants' operations – i.e. the auditing of financial statements – because nearly all companies have a financial purpose. Accountants and accounting firms may also provide other types of services and, therefore, the variety of projects and customers can be great. On the other hand, there are mitigating factors like active monitoring, a code of ethics and an adequate regulatory environment, for example ample qualification requirements, quality control among accounting firms and the risk of losing their accountants' licence.

The Money Laundering Division of the Directorate of Internal Revenue maintains surveillance by checking that accountants comply with the AML Act. In addition, the Accountants' Council sees to quality control, for example, where details regarding anti-money laundering and antiterrorist financing are checked. Overall, this monitoring indicates insufficient adherence to the aforementioned Act. There are indications that accountants are not sufficiently cautious when endorsing accounts and doing due diligence, that they do not adequately check whether customers are at risk due to political connections or are subject to international sanctions and overlook reputation during analysis of whether the transactions in question are suspicious. The fact that few notifications are received regarding suspicion of money launder-

ing from accountants indicates that risk-awareness among accountants is still lacking. However, supervisors believe that the occupation's risk awareness has been increasing with additional educational materials and active monitoring. Authorities have organised the publication of educational materials related to the operations and have also held informative meetings for accountants to augment their understanding of the issue area.

RISK CLASSIFICATION

HIGH

After taking into account threats, weaknesses, and mitigating factors, the risk related to money laundering in the work of accountants is deemed high.

4.4.3. BOOKKEEPERS

RISK CLASSIFICATION



GENERAL

Accounting firms, accountants, tax advisors, and persons who provide bookkeeping services for third parties in exchange for a remuneration are parties subject to mandatory reporting in the meaning of the AML Act. The following discussion pertains only to parties keeping books or performing accounting services.

Accountants work in fairly diverse ways. Many of them work independently, but certified bookkeepers also work in bookkeeping offices, within companies and associations, in auditing offices, or other ways. Until April of 2021, only those who fulfilled the conditions set out in Article 43 of Act no. 145/1994 on Accounting could call themselves certified bookkeepers and a register of those parties was kept by the Ministry of Culture and Business

Affairs. Among the conditions were being domiciled in Iceland, within the EEA Area, within a member state of the Free Trade Association of Europe, be legally competent and in possession of his estate, and have passed an examination to be certified as a bookkeeper, which was further outlined in a regulation. Act no. 27/2021, on amendments to various laws to simplify the regulatory environment abolished the aforementioned provision and, therefore, certified bookkeeper can no longer be a protected job title. A report issued along with the bill stated that the purpose of the amendment was to simplify the working environment of the economy and to eliminate outdated legal provisions and unnecessary authorisations. The Ministry, therefore, no longer has a register of those who have received bookkeeping rights and the number of those who operate in bookkeeping is no longer known.

The interest group for those having rights as certified bookkeepers is The Association of Certified Bookkeepers. In the autumn of 2023, their members numbered 450 and it has decreased after the aforementioned legal amendment. The purposes of the association include maintaining and increasing the members' knowledge and working on coordinating their methods, cf. Article 4 of the association's Articles of Association. The association has requirements on continuing education and organises courses and the publication of guidelines regarding bookkeeping, accounting and tax returns. Finally, the association sets certain rules regarding communication and discipline in the aim of, amongst other things, to promote honest and sincere communication between its members and contribute to making their efforts professional, diligent and scrupulous. Membership in the association is not mandatory. Finally, there is also an Association of Accounting Offices, which is the interest group of accounting offices.

THREATS

The main threat in the operations of bookkeepers is that those who handle bookkeeping or provide bookkeeping services for a fee can become witting or unwitting participants in providing unlawful transactions or operations with a veneer of legitimacy and the involvement of a bookkeeper could be requested in order to disguise the trail of finances or unlawful gains and to hide assets. The tasks entailing increased risk are mainly:

- Transactions with parties in a risk group.
- Involvement in risky transactions, for example, across borders.
- Services with related companies/parties.
- Customers having operations engaging heavily in cash transactions.

There are indications that bookkeepers have been related to cases which have been under investigation by the authorities, both the police and the DTI. In these matters it is more common for the services of accountants to be misused than for them to participate in criminal activity themselves. However, the FIU has received few notices from bookkeepers regarding suspicious transactions in recent years.

WEAKNESSES AND MITIGATING FACTORS

There is an inherent risk in the field regarding existing threats, and, in many instances, precautions against them are not sufficiently strong. However, the inherent risk in the field is not considered as great as in the case of accountants who often bear more responsibility for the finances and tax returns of companies and are often involved in more diverse, extensive, or complex tasks.

The Money Laundering Division of the Directorate of Internal Revenue monitors persons who keep books and provide bookkeeping services for third parties in exchange for remuneration and checks that they comply with the provisions of the AML Act. Overall, this monitoring indicates that a number of bookkeepers has become compliant with the AML Act. There are indications that bookkeepers do not satisfactorily carry out a risk assessment of their operations, do unsatisfactory due diligence, do not check beneficial ownership in a satisfactory manner and ignore parties in risk groups regarding political ties and reputation when analysing whether suspicious transactions are involved and do not make sufficient arrangements to assess whether customers are subject to international sanctions.

Very few notices have been received regarding suspicious transactions from bookkeepers which indicates, to some degree, that they still lack risk awareness. On the other hand, supervisors believe that the occupation's risk awareness has been increasing with additional educational materials and active monitoring. A supervisor has, for example, gave a lecture on the knowledge day of the bookkeeper under the auspices of the Association of Certified Bookkeepers and at the annual meeting of the Association of Accounting Offices. The authorities have also been involved in publishing educational materials to improve knowledge of the issue category. Finally the monitoring of supervisors is active and certain requirements are made of members who are registered in the Association of Certified Bookkeepers.

RISK CLASSIFICATION

MEDIUM

Concerning threats, weaknesses, and mitigating factors, the risk of money laundering in bookkeepers' work is deemed to be medium.

4.4.4. ESTATE AGENTS AND REAL ESTATE TRANSACTIONS

RISK CLASSIFICATION



GENERAL

Estate agencies and estate agents are subject to mandatory reporting under the AML Act. In Iceland, a licence for estate agency operations is mandatory and only estate agents certified by a district commissioner may represent others in purchasing, selling, or exchanging real estate, cf. Article 2 of the Act on the Sale of Real Estate and Ships no. 70/2015. An exception to this is that people can sell their real estate without the involvement of an estate agent. Also, the beneficial ownership of a real estate property can change by other means, for instance, by assignment of a private limited company which owns, or may even be founded around, a real estate property. If an attorney or another specialist provides assistance in the organisation or execution of such transactions for their client, they are also subject to mandatory reporting according to the AML Act. This section covers real estate transactions with a focus on the involvement of estate agents.

There are strict conditions for granting a licence, such as that the person involved has completed a specified curriculum, acquired work experience, has legal capacity and control over his finances, and has not been sentenced to punishment for violations of specified chapters of the General Penal Code. The licensor is the District Commissioner of Greater Reykjavík, who checks that the fulfilment of the conditions of certification are met, in both the granting of the licence, its surrender and its reissue. The law allows the licensor to close an office if the operations entail the sale of real estate by an unlicensed party. Finally, it bears mentioning that a portion of the number of estate agents is also attorneys. However, they also must apply for a licence and fulfil the legal conditions like everyone else. Before the entry into force of Act no. 70/2015, however, attorneys were exempt from the condition of having to pass a test for certification as an estate agent and, therefore, a number of attorneys were granted the licence with fewer conditions than those who are made today.

The Estate Agents Surveillance Committee is an independent administrative committee which operates on the basis of chapter III of Act no. 70/2015 and the Regulation on the Estate Agents Surveillance Committee no. 931/2016. The

Estate Agents Surveillance Committee monitors estate agents' work procedures to ensure that they operate in accordance with the provisions of the act and best practices in the real estate market. The monitoring of the committee involves, amongst other things, the examination of bookkeeping data, including trust accounts, on-location inspections, examination of document processing, along with surveillance of ownership and work responsibility insurance. In part, the monitoring of the committee also involves an overlap with the responsibilities of supervisors regarding money laundering, for example, when documents regarding mediation in the sale of real estate properties and ownership are examined. Under the law, the Directorate of Internal Revenue checks that estate agents comply with the provisions of the AML Act.

The Estate Agents' Association. Membership in this association is not mandatory, unlike what applies to the comparable associations of attorneys and accountants. Of the 636 estate agents who were certified as of September 2023, 335 belong to the association. The association sees to its members' education, including on money laundering, and sets a code of ethics.

According to information from the website of the Housing and Construction Authority¹¹⁰ the total turnover of real estate properties in the entire country in 2022 amounted to about ISK 830 billion in 12,500 contracts of sale. In the previous year, just over 16,500 contracts of sale were officially registered and the sum of the transactions amounted to about ISK 880 billion. The situation in the housing market in Iceland has been tight as a result of unrelenting inflation since the beginning of the year 2022. It is deemed that inflation, along with rising food prices and interest rates, caused the scope of real estate transactions to decrease between years. Figures on the number of real estate transactions without the involvement of an estate agent are not available.

THREATS

There are possibilities to launder unlawful gains through real estate transactions, including where the cost is low and the scope of real estate transactions is great regarding both the number of them and the amounts. Among other threats, one might mention that:

- It is possible to conceal ownership when real estate is transferred into a company founded for the sole purpose of holding the real estate involved. Offenders are also known to have employed straw men in real estate transactions, especially when a real estate property is sold through a company. Finally, foreign persons who do not reside in Iceland can receive an ID number for a foreign citizen and purchase real estate and/or companies in Iceland, as detailed in the section on ID numbers for foreign citizens.

¹¹⁰ [Monthly turnover | Real property data base \(fasteignaskra.is\)](#)

- Payment of the purchase price can take place in part with cash or liquid assets, for example, automobiles which may have been acquired unlawfully.
- It's possible to sell real estate properties where the purchase price is specified significantly under or over the market value and part of the purchase price may be concealed and paid with ill gotten money.
- The law does not require that loan documents be prepared by estate agents and/or lenders.

The police have strong indications that Icelandic offenders launder the gains from their criminal activity through real estate transactions, including real estate projects, and by their very nature, each case revolves around significant amounts of money.

There are indications that estate agents have been related to cases which have been under investigation by the police. In those cases there are indications that the services of estate agents have been misused by offenders.

In some instances, the offender purchases a real estate property in part or in whole with a loan from a financial institution, a commercial bank or a pension fund and pays instalments on the loan with the unlawful gains of criminal activity. In these instances, estate agents are, therefore, not the only parties subject to mandatory reporting who have an opportunity to identify suspicious real estate transactions, as financial institutions are also required to conduct due diligence regarding the origins of funds. Also, financial institutions can identify unusual instalments on loans. Even with the same transaction, estate agents and financial institutions may have different information regarding the transaction and, therefore, it is important for each party to report independently of suspicions in such cases.

Few notices have been received regarding suspicious transactions by estate agents in 2021 and 2022. In comparison, the FIU regularly receives notifications from commercial banks or pension funds related to suspicious real estate transactions.

WEAKNESSES AND MITIGATING FACTORS

The exclusive right to sell real estate for others is legalised and the operation is subject to a licence. The trail of real estate transactions can be traced to a great extent as the main documents during the sale of real estate properties are officially registered, such as deeds and mortgage loans. The field entails considerable inherent risk. In addition, real estate transactions involve threats and weaknesses. Also, criminals require little expertise to launder unlawful gains through real estate transactions.

Three independent entities are involved in legal monitoring of the oper-

ation of estate agents, and the Estate Agents' Association also sets a code of ethics for its members. The District Commissioner of the Greater Reykjavík Area tends to the conditions of the certification and the Estate Agents' Surveillance Committee is legally obligated to conduct regular on-location inspections with every real estate agency. Also, monitoring of the compliance of estate agents is handled by the Money Laundering Division of the Directorate of the Internal Revenue and it has been active since the entry into force of the AML Act. Considering the surveys conducted by the Money Laundering Division of the Directorate of the Internal Revenue, there are indications that the risk awareness of estate agents has increased among estate agents. They tend to be aware of their basic legal obligations as parties subject to mandatory reporting. They conduct due diligence and risk assessment of their own operations and are aware of the risk that comes with accepting cash as payment of the purchase price. On the other hand, there are instances where obligations have not been sufficiently fulfilled, particularly in instances where the law requires that additional due diligence be executed, when it is to be investigated whether the customer is in a risk group for political affiliations or when legal entities participate in transactions. Lack of reporting from estate agents may also indicate that there is still a lack of risk awareness within the profession. When there is less activity in the real estate market and the competition is fierce, as was the case in 2022, it may be a priority issue to acquire assets on the sales catalogue at the expense of claims according to the AML Act. Measures have been taken to increase estate agents' risk awareness, with active monitoring and the publication of educational materials. Also, informative meetings on the issue category have been held, specifically intended for estate agents.

There is a lack of monitoring and oversight when ownership transfers of real estate properties take place with the sale of companies. There is no official register of company brokers and no qualification requirements are made of those whose profession is the selling of companies, as those who are made of real estate agents. Therefore, anyone can start such an operation.

RISK CLASSIFICATION

HIGH

Considering threats, weaknesses and mitigating factors, the risk of money laundering in real estate transactions is deemed to be high.

4.4.5. SHIP BROKERS

RISK CLASSIFICATION



GENERAL

All who have an official and published licence to sell real estate properties are also licenced to sell ships which are subject to mandatory registration in this country. The same rules apply to ship brokers as apply to estate agents, and reference is made to the discussion of estate agents regarding certification, qualifications, permits, and monitoring.

Few ship brokers are operating in Iceland, and most of them are solo brokers. In Iceland, ship brokers usually become involved only where the sale of fishing vessels is called for. There are few instances where ship brokers see to the sale of pleasure boats that do not fish for business purposes even though registration is mandatory for such vessels.

The sales market for ships may be divided into two. On one hand, there are smaller fishing boats, small motorboats and small boats, which usually all have fishing permits/catch authorisation and are located in Iceland. On the other hand, there are sales of bigger vessels in the country, which usually also have fishing permits/catch authorisations, or larger ships that are located abroad. The sale of large fishing ships mostly goes on abroad, and the involvement of Icelandic ship brokers varies for such transactions. However, this involves consultation or intermediation between a buyer and seller.

Payments regarding ship brokerage do not usually go through a ship broker's custodial account, but rather parties pay directly to each other through banking institutions. However, ship brokers may need to intervene to keep part of the purchase price secure in their custodial account, i.e. security of up to 10% of the purchase price, until the examination and purchase are completed. This pertains specially to selling ships between countries. This occurs with the assistance of banking institutions, and payments are traceable.

The Icelandic Transport Authority publishes the Icelandic International Ship Register, which contains the registration of ships subject to mandatory registration, including initial registrations, reregistrations, de-registrations, etc. For this reason, the Icelandic Transport Authority also monitors ownership, including a legal person's purchase of a ship owned by foreign parties. In all instances, its

ownership ought to be traceable. The existence of foreign customers is confirmed by information from the Business Registry and an agent of the relevant party, certified by a district commissioner as a notary public.

THREATS

In many ways the opportunities to launder unlawful gains through ship brokering and real estate transactions are the same and most threats are related to the payment of purchase price with cash or liquid assets or with transactions where a company is a buyer or seller. On the other hand, few parties are seeing to ship brokerage in this country, and the number of transactions is small, only a miniscule part of the scope of real estate transactions. There are no known examples of brokers being used to launder money in this country. Threats in the operations are, therefore, not very high, given the current environment.

WEAKNESSES AND MITIGATING FACTORS

The main weaknesses related to ship brokerage are the lack of ship brokers' risk awareness and the risk that conditions of the AML Act will not be fulfilled, particularly regarding satisfactory due diligence.

RISK CLASSIFICATION

LOW

After taking into account the discussion on threats and weaknesses, the risk related to ship brokerage is low.

4.4.6. CAR DEALERSHIPS, CAR DEALERS AND VEHICLE TRANSACTIONS

RISK CLASSIFICATION



GENERAL

With the Act on Amendments to Various Acts Regarding Licensing no. 19/2020, various acts regarding the issuance of permits were amended. One of the amendments involved Act no. 28/1998 on Retail Work. It revoked the certification of car dealers. Everyone is now free to engage in transactions with cars. Notwithstanding the above, Act no. 28/1998 applies to the sale of used vehicles with mandatory registration for business purposes. The general law on the purchase of liquid assets applies to transactions without intermediaries, cf. Act no. 50/2000. The duty to inform in transactions with used vehicles is covered in Regulation no. 44/2003, which contains detailed information on the requirements for minimum information to be provided in transactions with used vehicles going through car dealers or for business purposes. From the above, it follows that the requirements for those employed in selling vehicles are minor, considering the requirements for those seeing to the sale of, e.g. real estate and ships.

Alongside act no. 96/2020, the AML Act was amended to include the operations of car dealerships and car dealers. Control of compliance with the act is in the hands of the Directorate of Internal Revenue.

The operation of the automotive trade is extensive. There is an interest group of employers selling vehicles, products, and services related to them: the Icelandic Federation for Motor Trades and Repairs. Their purpose is to advocate for members of the federation regarding the interests of the motor trades in respect of public law bodies, associations, manufacturers, other customers, and the public. Membership in the federation is not mandatory. In the autumn of the year 2023 there were over 100 members, and they spanned a broader area than just car dealerships and car dealers. Involved here are car repair shops, tire repair shops, painting and body shops, car workshops, service stations, and spare parts sales.

THREATS

There are possibilities to launder unlawful gains through car transactions, including where the cost is low and the number of vehicle transactions is great

regarding both the number of them and the sums of money involved. Car transactions go on both between individuals and through intermediaries and little expertise is required to launder unlawful gains through car transactions.

Known ways to launder money where cars are the object of transactions, include acquiring cars to offset debts and other transactions where the car is part of the payment or transactions where the purchase price of a car is paid with cash. There is an additional threat related to car transactions where the buyer and/or seller is a company.

Often, traces of the extravagant lifestyle of offenders in this country are evident, where significant money appears to have been spent on expensive cars or liquid assets far exceeding that which can be considered reasonable according to reported income and legitimate means of earning money. On the other hand, few cases have been investigated in this country where car transactions have aroused suspicion. Also, there are still relatively few notices of suspected money laundering with car transactions.

WEAKNESSES AND MITIGATING FACTORS

The field is thought to entail considerable inherent risk. In addition, threats and weaknesses are inherent in the car trade.

Considering the surveillance of the Money Laundering Division of the Directorate of Internal revenue, there are indications that car dealers are still not sufficiently aware of their duties regarding measures against money laundering and, therefore, do not go far enough in their efforts to introduce them into their operations. Also, the surveillance results indicate that anti-money laundering measures are imprecise and, therefore, it may be argued that risk awareness within the field is still lacking. As a mitigating factor, it bears mentioning that educational materials for car dealers and car dealerships regarding risk factors in their operation and reporting duties have been published.

RISK CLASSIFICATION

HIGH

After taking into account the threats and weaknesses connected with the car trade, the risk is deemed to be high.

4.4.7. JEWELLERS AND GOLD-BUYERS, PRECIOUS METALS AND GEMS

RISK CLASSIFICATION



GENERAL

In Iceland, the retail, wholesale and design of imported precious metals and gems occur as such goods are not mined in this country. It is forbidden to import uncut diamonds to Iceland from conflict areas according to regulation no. 361/2016 on the Control of Services and Items that may have Strategic Significance.

The making gold and silver are protected trades, cf. Article 1 of the Regulation on Protected Trades no. 940/1999, cf. Paragraph 1 of Article 8 of Act no. 42/1978 on Manual Trades, and, therefore, only those having completed a journeyman's or master's certificate are authorised to work in the trade. Products processed from precious metals must be stamped, according to Act no. 77/2002 on products processed from precious metals and the Consumer Agency monitors the compliance of those laws. According to the aforementioned Act no. 77/2022, precious metals are defined as follows:

"[G]old containing 375 parts per thousand or more of pure gold, silver containing 800 parts per thousand or more of pure silver, platinum containing 850 parts per thousand or more of pure platinum, and palladium containing 500 parts per thousand or more of pure palladium." No special law has been set on the handling of precious gems. In addition, precious gems are defined as "natural stones like diamonds, rubies, emeralds, sapphires, opals, and pearls".

The market in Iceland, regarding sales of precious metals and precious gems and other products sold in jewellery stores, is deemed small in international comparisons, relative to the gross domestic product.

THREATS

When assessing a threat, it is necessary to look to the smallness of the market in Iceland for precious metals and gemstones, keeping in mind their percentage of the national product. The main threats lie in precious metals and precious gems being used to launder unlawful gain because of their characteristics. That is, they are easy to transport, store and smuggle across borders because of their size. The value of precious metals and gems is generally high and they maintain

their value for longer, which makes it easy to use them for transactions whenever and wherever in the world. Finally, it should be mentioned that, as is the case with most other liquid assets, information regarding ownership and transactions is usually not officially registered.

Precious metals and precious gems are imported and therefore go through customs, and the imports into the country are recorded. According to customs authorities, the confiscation of precious metals and precious gems is relatively rare, and the value of the seized items is very low.

Often, traces of the extravagant lifestyle of offenders in this country are evident, where significant money appears to have been spent on expensive cars or liquid assets, such as jewels, far exceeding that which can be considered reasonable according to reported income and legitimate means of earning money. On the other hand, very few notices have been received from jewellers or gold buyers, and the police have generally not been involved much in cases related to this product category.

WEAKNESSES AND MITIGATING FACTORS

Iceland does not have restrictions on the use of cash or restrictions on the purchase of precious metals, gemstones or other jewelry. Therefore, there may also be a risk that sellers and buyers will be conscious or unconscious participants in money laundering if such goods are bought and sold for cash.

Jewellers and gold buyers only fall within the scope of the AML Act when transactions take place in one payment or more which seem to be interlinked, in the amount of 10,000 euros or more. The Money Laundering Division of the Directorate of Internal Revenue of entities in the market is complex and limited as parties may fall within the scope of the Act on Measures against Money Laundering and Terrorist Financing in one transaction, but usually not. In addition, dealers are often small operations and may find it difficult to fulfil their duties under the AML Act and do not even have sufficient knowledge in that field. The above can lead to due diligence not being executed under the aforementioned Act or the executions being unsatisfactory. This will make the traceability of purchases of precious metals and precious gems for amounts above the amount limit more difficult than ever. Risk awareness within the field is deemed low.

Despite weaknesses, these operations are rather uniform, the scope of them most often small, and the market small by international comparison. Mitigating factors also worth mentioning include the publication of educational materials on the risk factors in operations where a great deal of cash is used, and a risk assessment, due diligence, and measures against money laundering. In addition to this, informative meetings have been held to review the duties of mandatory-notice parties where jewellers have been invited to take part. Most of the weaknesses in national defence and customs control which pertain

to the smuggling of cash to and from Iceland also pertain to the smuggling of precious metals and gems and are discussed in that respect in the section Cash, transport to and from Iceland. Finally, it bears mentioning that registration of confiscation of jewels in police systems is deficient and, therefore, it's difficult to process statistical information regarding confiscation of precious metals and gems.

RISK CLASSIFICATION
MEDIUM

Considering the aforementioned, the risk of money laundering in the market of precious metals, gems and other jewelry is deemed medium.

4.4.8. ART DEALERS AND ART BROKERS, ART OBJECTS MARKET

RISK CLASSIFICATION

GENERAL

In this country, the sale and auctioning of art objects takes place with the involvement of third parties through art galleries and auction houses. Art seller and art dealer are not protected job titles and everyone is permitted to inter-mediate in the sale of art objects. Also, there is no operational interest group for art sellers or art dealers.

Art sellers and dealers, including art galleries and auction houses are subject to mandatory reporting with regard to transactions in the amount of 10,000 euros or more, whether in one payment or more which seem interrelated. The Directorate of Internal Revenue monitors the compliance of art sellers and dealers with the provisions of the law.

As it is common for transactions or assignment of art objects to take place without the intercession of a third party and even for art objects to be bought

directly from the artist themselves, the total scope of the art object business in Iceland is not known. Considering gross domestic product, the market of art objects through third parties in Iceland is insubstantial in scope.

THREATS

Art object transactions take place both between individuals and through third parties and there may be a risk of buyers, sellers and/or intermediaries becoming witting or unwitting participants in money laundering. Additional money laundering risk related to the art object business especially applies when art objects are paid for in cash or the buyer and/or seller is a company.

Generally speaking, only one of each art object exists and their value can be great. Also, they generally maintain their value for longer and a long time can elapse between the purchase and sale of individual works of art. Finally, it should be mentioned that, as is the case with most other liquid assets, information regarding ownership and transactions is usually not officially registered.

The main threat involves offenders buying artworks for unlawfully gotten money or using art object transactions to transfer money, even across borders. The subjective valuation of art objects renders it difficult to assess whether a certain price for a work of art is truly commensurate with its real value, which makes it easier for offenders to move money between parties, for instance, with underpricing or overpricing. This inherent risk with art objects especially applies when works of art are being sold for the first time, even directly from the artist. The same work of art can be endorsed many times for this purpose as the requisitioning of art objects to offset debts or the use of art objects as currency in transactions outside the traditional market are also known money laundering methods.

Often, traces of the extravagant lifestyle of offenders in this country are evident, where significant money appears to have been spent on expensive cars or liquid assets, such as art objects, far exceeding that which can be considered reasonable according to reported income and legitimate means of earning money. On the other hand, the police has had very few cases where art object transactions have been used directly for money laundering purposes and where the confiscation of customs of art objects is rare. Also, the FIU has never received notices from art sellers, art galleries or auction houses because of suspicious art object transactions.

WEAKNESSES AND MITIGATING FACTORS

Iceland does not have restrictions on the use of cash or restrictions on the purchase of art objects. Art sellers and dealers only fall under the scope of the AML Act when transactions take place in one payment or more which seem to be interlinked, in the amount of 10,000 euros or more. The surveillance of the Di-

rectorate of Internal Revenue of entities in the market is complex and limited as parties may fall within the scope of the Act in single transaction, but usually not. In addition, art sellers are often small operations with small operational units and may, therefore, find it difficult to fulfil their duties under the AML Act and/or do not even have sufficient knowledge in that field. The above can lead to due diligence not being executed under the aforementioned Act or the executions being unsatisfactory. This will make the traceability of purchases of art objects gems for amounts above the amount limit more difficult than ever. Risk awareness within the field is deemed low.

Despite weaknesses, these operations are rather uniform, the scope of them most often small. Mitigating factors also worth mentioning include the publication of educational materials on the risk factors in operations where a great deal of cash is used, and a risk assessment, due diligence, and measures against money laundering. Finally, informative meetings have been held to review the duties of mandatory-notice parties where art sellers have been invited to take part.

RISK CLASSIFICATION

MEDIUM

Considering the aforementioned, the risk of money laundering in the market of art objects is deemed medium.

4.5. GAMBLING

Under Article 183 of the GPC, anyone gambling or betting as a business or urging others to participate can be fined or imprisoned for up to 1 year. Despite this, there are in force various laws under which certain companies may be allowed to run operations having the characteristics of gambling and/or betting. There the main operations worth mentioning are lotto, lotteries, sweepstakes, and collection boxes. One of the main characteristics of the above operations is that all profit shall go to charities. The following table shows the number of operators by the type of gambling which were licenced to operate in 2022, as well as the turnover of those parties in that year.

The sections below will discuss these operations with respect to the assessed risk of their misuse to launder unlawful gains. The discussion considers the above classification. Furthermore, it will discuss gambling on the Internet through the websites and apps of foreign operators which are, thus, subject to surveillance by other states. During the analysis, information from operators, supervisors, police, FIU, other authorities and appropriate legislation especially provided support.

The following are the main threats and weaknesses and mitigating factors which pertain to gambling in Iceland. The risk related to each type of gambling will be covered further in the following sub-sections:

- Individuals or legal entities which have received an operating licence on the basis of laws regarding lotteries or the operation of money collectors and lotteries on the basis of special legislation are subject to mandatory reporting according to the AML Act. Operators are, therefore, obligated to comply with the provisions of the act, e.g. regarding its own risk assessment, mandatory reporting, due diligence, the preservation of data, organisation, and systems. However, it is considered a weakness that vendors of various gambling games and slot machines are not subject to mandatory reporting under the act.

THE NUMBER OF OPERATORS BY THE TYPE OF GAMBLING WHICH WERE LICENCED TO OPERATE IN ICELAND IN 2022, AS WELL AS THE TURNOVER IN THAT YEAR IN ISK BILLIONS

Table 12

Gambling	Number of operators	Turnover [ISK billions]
Lotto	1	6.6
Lotteries operating under a special act	3	4.1
Lotteries operating under the Law on Lotteries	33 (issued licences)	0.4-0.5
Sweepstakes/Bets	1	2.0
Gaming machines – slot machines and lottery machines	2	12.1

- Most reports which are received by the FIU because of suspicions of money laundering related to gambling in Iceland occur because of slot machines. The risk awareness of operators related to money laundering has increased in the past few years with additional monitoring, additional education and the publication of educational materials.
- Various methods to launder money through gambling are known. In most instances, offenders purchase a winning ticket or play/bet with limited risk for ill-gotten gains, even cash, in the aim of using winnings to account for the money in their keeping. There are indications that gambling has been used to launder money in Iceland and slot machines and online gambling is deemed to possess the most inherent risk.
- The amount of betting and other gambling online has been increasing in recent years and in the newest risk assessment of the EU, the risk of online gambling is assessed as very high.¹¹¹ Known ways are, for instance, the use of games such as poker to get funds between parties, even across borders, for example by losing intentionally without arousing suspicion. There are several indications that the turnover of Icelanders through websites which offer online gambling is substantial.

¹¹¹ *Supra-National Risk Assessment Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. SWD(2022)/554. EU, Brussels 2022, pg. 236.*

4.5.1. LOTTO

RISK CLASSIFICATION



GENERAL

Three kinds of lotto operated in Iceland in the autumn of 2023: Lottó, Víkingalottó, and Eurojackpot. Participants choose 5 figures (Lottó), 6 figures (Víkíngalottó) or 7 figures (Eurojackpot.) Participants can also buy “system tickets” where it is possible to considerably increase their chances of winning by buying additional numbers. The drawings are weekly in all the lotto games, and the numbers are random.

The operator of all the lotto games is Íslensk getsþá, which operates under the Act on Numbers Lotteries no. 26/1986. The National Olympic and Sports Association of Iceland owns 46.67% of Íslensk getsþá; the Organisation of Disabled People in Iceland owns 40%, and the Youth Association of Iceland owns 13.33%. The profits of Íslensk getsþá's operations shall be earmarked for the strengthening of sports organised by sports enthusiasts in the country in associations under the umbrella of the National Olympic and Sports Association of Iceland and the Youth Association of Iceland. The profits are also intended to pay the initial cost of residential housing for disabled people under the auspices of the Organisation of Disabled People in Iceland or to support other activities of the organisation for the benefit of disabled people, cf. Article 5 of the Act.

Tickets are sold at numerous sales locations throughout Iceland, such as kiosks, stores, petrol stations and other comparable locations, as well as on the Internet through the operator's homepage. Tickets can be purchased at sales locations whether with cash or a payment card. Prizes of up to ISK 25,000 are paid out at sales locations against the presentation of winning tickets, while higher winnings must be claimed from the operator. If tickets are purchased online, one must set up an account on a valid ID number and link a payment card to the account which belongs to the registered ID number. Winnings are also paid out to the party to whom the ID number in question belongs and withdrawals from the account can only take place via the transfer of funds into a bank account or payment card belonging to the ID number registered for the account.

The statistical probability of a first prize is low, cf. Article 13 of the Regulation on the Numbers Lotteries of Íslensk getsþá no. 1170/2012 as amended and

other winnings are generally low. The total turnover of lotto games in 2021 was ISK 6.1 billion and the market purchase value of winnings was ISK 3.4 billion. In the year 2022, the total turnover of lotto games was ISK 6.6 billion and the market purchase value of winnings was ISK 2.4 billion.

THREATS

Even though the accessibility is easy, tickets can be bought with cash and participating requires no special knowledge, the winnings ratio is so low and random that it is nearly impossible to launder money by participating. Furthermore, purchasing a winning ticket is nearly impossible as winnings higher than ISK 25,000 must be claimed from the operator and tickets belong to their bearer and, therefore, no information can be acquired about the winner before the person in question has come forward. Therefore, these operations seem to entail limited threats.

Also, FIU has received no notices of suspected money laundering through lotto, and no winning lotto tickets have been found during police investigations, nor has there been any suspicion of the misuse of lotto in connection with money laundering.

WEAKNESSES AND MITIGATING FACTORS

The weaknesses are limited as only one party is licenced to operate a lotto in Iceland and regulations govern the operation. Lotto falls within the scope of the AML Act and operators are, therefore, obligated to comply with the provisions of the act regarding mandatory reporting, due diligence, preservation of data, organisation and systems. However, one must deem that the current law on operators will considerably reduce the likelihood that criminals or organised crime will gain control or ownership of points of sale. Detailed annual evaluations also considerably reduce the risk of misuse. All prizes above a low amount are paid out by the operator and data on the winners are preserved. Finally, the authorities have commissioned the publication of educational materials regarding gambling, along with general educational materials regarding money laundering and educational meetings with the operator have taken place.

RISK CLASSIFICATION

LOW

The risk of money laundering related to lotto is low.

4.5.2. LOTTERIES

RISK CLASSIFICATION



GENERAL

Lotteries are a type of gambling where the holder of a winning ticket is selected in a random draw. The lotteries discussed here, are “ticket lotteries”, i.e. a participant buys a numbered lottery ticket, and if his number is drawn, he wins something. Laws govern lottery operations. On one hand, there is Act on Lotteries no. 38/2005. On the other hand, special laws cover lotteries, e.g. the Act on the Lotteries of the University of Iceland no. 13/1973, the Act on Elderly Fishermen's Home no. 16/1973 and the Act on Lotteries for the Association of Icelandic Tuberculosis and Thoracic Patients no. 18/1959. Ticket lotteries, to which the above legislation applies, may be split into two groups.

TICKET LOTTERIES OPERATING UNDER A SPECIAL ACT

Three lotteries fall into this group: Lotteries of the University of Iceland (UI), Lotteries of Elderly Fishermen (DAS,) and Lotteries for the Association of Icelandic Tuberculosis and Thoracic Patients (SIBS.) Winnings in these lotteries are cash prizes. As with other gambling allowed in Iceland, the operating profit of the lotteries goes to charity. Statutes determine the organisation of these lottery operators, and there is thorough monitoring of their drawings and finances. Finally, lotteries are required to keep accounts.

The total turnover in 2022 for the three lotteries was ISK 4.1 billion and about ISK 2.5 billion was paid in winnings. Lottery tickets in this category are sold only to named parties, i.e. ticket buyers must provide their name and National ID, and tickets are generally subscription tickets. Tickets can be purchased online and they are sold through the website of the operators. An account must be set up on a valid ID number and connected to a bank account or a payment card belonging to the ID number in question. Winnings are also paid out to the registered owner of the ticket via the transfer of funds into a bank account or payment card belonging to the ID number registered for the ticket.

TICKET LOTTERIES WHICH OPERATE UNDER THE LAW ON LOTTERIES

Such lotteries must apply to the District Commissioner of South Iceland for a permit. The permit may only be issued to a company, association or institution domiciled in the European Economic Area and only to raise money for the public good in Iceland as well as national, charitable, cultural, and sports concerns or charities, as well as international humanitarian work. In 2021, 35 permits were issued, and in 2022, 33 permits and these lotteries are obligated to submit reports or accounts about their operations to the District Commissioner.

Winnings in these lotteries are only products or services, such as automobiles, trips, household appliances or other more inexpensive products. According to information from the District Commissioner, the total turnover of these lotteries in recent years ranged from ISK 350–450 million and ISK 100–150 million was paid in winnings. Sales in this category generally take place in two ways. On the one hand through volunteers who go from door to door or busy places, such as shopping malls, and on the other hand with direct marketing where tickets are sent to people's homes without having been requested and an optional payment demand is set up in their online bank.

THREATS

The threats from this operation seem to be limited. Lotteries operating under a special act appear not to be a desirable way to launder money, amongst other things because of the protective measures in place, such as winnings being based on luck, all tickets being registered to a name, low winnings, detailed safeguards against cheating during drawings, and detailed rules on the operator's organisation and finances, amongst other things.

In the case of lotteries operating under the Law on Lotteries, winning is also based on luck, and the prizes are only products where the biggest prizes can be cars, but the value of other prizes is generally much lower. Tickets belong to their bearers and, therefore, the winner is unknown until they come forward.

There are no indications that the lotteries discussed here have been used to launder money, and no cases connected with money laundering have come under examination by FIU or the police.

WEAKNESSES AND MITIGATING FACTORS

There are limited weaknesses in these operations, as there is a regulatory framework and substantial organisation. Lotteries fall within the scope of the AML Act and operators are, therefore, obligated to comply with the provisions of the act regarding, amongst other things, mandatory reporting, due diligence, the preservation of data, organisation and systems. The District Commissioner of South Iceland is responsible for granting licences for lotteries who operate

under the Law on Lotteries and for providing surveillance. Also, the authorities have organised the publication of educational materials on the money laundering risk related to gambling. However, the knowledge regarding money laundering and terrorist financing of parties subject to mandatory reporting who operate under the Law on Lotteries is still considered a weakness.

RISK CLASSIFICATION

LOW

Considering the above, the risk regarding lotteries is deemed low.

4.5.3. SWEEPSTAKES

RISK CLASSIFICATION



GENERAL

Iceland basically offers two kinds of sweepstakes – Lengjan and 1x2. Both games are connected with sweepstakes/betting where people guess the outcome of sports events, e.g. the winner, number of goals or the scorers of goals etc., either before or during a game. The operator of both types is Íslenskar getraunir (Icelandic Sweepstakes,) which was founded based on the Act on Sweepstakes no. 59/1972. The company's operations aim to collect money to support the practice of sports organised by sports enthusiasts in Iceland in association with the Youth Association of Iceland or the Iceland Sports Federation. All proceeds go toward building up these activities.

People can buy tickets on the Internet, the operator's website, or at recognised sales agents, of which there were just over 200 in the autumn of 2023. Buying tickets on the Internet requires registering for access and connecting it with a payment card. Purchasing on the Internet is therefore only possible with

a recognised payment card. Purchase of tickets at a sales agent is possible with either a payment card or cash. Winnings of more than ISK 25,000 are only paid out by the operator which requires the person with a winning ticket to provide information on his name, National ID number, address, and bank account. Winnings are only paid into the winning ticket holder's bank account. Consequently, the operator can monitor whether the same individual is repeatedly claiming winnings. The total turnover at Icelandic Sweepstakes from the aforementioned games was about ISK 2 billion in 2021 and 2022 and paid winnings amounted to just under ISK 1.5 billion during each year.

Finally, the operator conducts a background check regarding the financial standing and criminal record of new retail operators before the resale permit is granted. Also, a new contract is made in the event of a change in ownership.

THREATS

The main threats regarding sweepstakes operations are the number of dealers and the high percentage of winnings. More to the point, there is considerable access to sweepstakes. It is relatively easy to learn their rules, and, for this reason, criminals do not require expertise. Also, people can use cash for transactions. On the other hand, to a considerable degree, they take place on the internet and, therefore, they are traceable.

It is also possible for offenders to directly or indirectly own a retail operator and their connections may grant them access to winning tickets which someone tries to redeem at a retail location. On the other hand, the amounts which can be redeemed at a retail location are low and, therefore, the threat is significantly limited.

The FIU has received very few notices regarding suspicion of money laundering connected with sweepstakes. The police have investigated few cases related to sweepstakes, and there have been no cases concerning tampering with results. On the other hand, there have been cases where footballers have been suspended by the disciplinary board of KSÍ (the Football Association of Iceland) for violating betting rules after having bet on games played by their own teams.

WEAKNESSES AND MITIGATING FACTORS

There are limited weaknesses, as the operation is simple and only available to Icelandic Sweepstakes, cf. Act no. 59/1972. The operation of the operators fall within the scope of the AML Act and operators are, therefore, obligated to comply with the provisions of the act regarding, amongst other things, mandatory reporting, due diligence, the preservation of data, organisation and systems. On the other hand, it is deemed a weakness that the purveyors are not subject to mandatory reporting under the AML Act. However, one must deem that the current law on operators will considerably reduce the likelihood that criminals

or organised crime will gain control or ownership of points of sale. Detailed annual evaluations also considerably reduce the risk of misuse. All prizes above a low amount are paid out by the operator and data on the winners are preserved. The above arrangement consequently enables an operator to systematically monitor the payment of winnings. All operations in the Icelandic Sweepstakes' systems are recorded, and if irregularities come to light, it is easy to trace and examine them more closely. Finally, the authorities have commissioned the publication of educational materials regarding gambling, along with general educational materials regarding money laundering and, thus, risk awareness has been increased.

RISK CLASSIFICATION

MEDIUM

Considering threats, weaknesses, and mitigating factors, the risk related to sweepstakes is deemed to be medium.

4.5.4. GAMING MACHINES – SLOT MACHINES AND LOTTERY MACHINES

RISK CLASSIFICATION



GENERAL

The operators of gaming machines are Íslandsspil ehf. and the University of Iceland Lottery (UL). Their operations build on statutory authorisation, cf. Act no. 73/1994 on Slot Machines and Act no. 13/1973 on the University of Iceland's Lottery. Íslandsspil is owned by The Icelandic Red Cross and The Life Saving Association Landsbjörg. It is statutorily determined how the profits from the income produced from the collection box operations shall be allocated. No others are authorised to operate slot machines or lotteries in Iceland.

It is only possible to play for cash in the gaming machines or for winning

tickets. It is possible to load a maximum of ISK 100,000 at a time in a single gaming machines. However, it is possible to repeat this as often as wanted. It is also possible to print out winning tickets without playing, or if few games have been played.

The ULL and Íslandsspil conduct due diligence of the operators of gaming sites. They have internal requirements regarding good reputation and investigate items related thereto. There are instances where agreements with operators of gaming sites have been revoked due to reputation issues. Operators of gaming sites pay out winnings with money transfers and in the case of one of the operators, there is a limit on the amount which the gaming sites can pay out in cash. Due diligence is done on winners when a gaming site pays out winnings by bank transfer and in some cases their gaming history is traced. On the other hand, a minority of prizes is paid out via bank transfers, although that ratio has been increasing in recent years. Finally, there is a requirement that the operators of gaming sites conduct due diligence on winners in certain instances where a specified limit amount has been reached.

There were 23 gaming sites for the University of Iceland (UI) lotto machines in the autumn of 2023, mainly either bars, kiosks, or special casinos. There were 486 lottery machines in use. Íslandsspil ehf. had 51 gaming locations with collection boxes. They were mainly in the Reykjavik Metropolitan Area and were either bars, kiosks, or special casinos. There were 329 slot machines in use in the autumn of 2023.

The total turnover in 2022 of gaming machines was about ISK 12.1 billion, and the winnings paid out the same year were about ISK 8.4 billion

THREATS

There is a high risk that gaming machines can be utilised for money laundering, and there are indications of such. The accessibility to gaming machines is considerable and the extent of the risk regarding both the number of collection boxes and their turnover is great. Among other threats is the fact that the only way to pay is with cash and the ID of the gamer is registered nowhere before the gaming takes place. It's possible to load cash into a gaming machine and then print out lottery tickets without playing or after playing a few games. On the other hand, the operators are able to some extent to identify such behaviour by analysing gaming patterns. It is also possible for offenders to be connected with the operation of gaming sites, as access to gaming sites can enable them to purchase winning tickets. Finally, money laundering through gaming machines does not require expertise, special preparation, or cost outlays.

Most notices to the FIU regarding gambling are connected with gaming machines and their number has increased in recent years. There are also indications that collection boxes have been used for money laundering and offenders have

accounted for significant amounts of money in their keeping as winnings from gaming machines.

WEAKNESSES AND MITIGATING FACTORS

The operators of gaming machines fall within the scope of the AML Act and comply with the provisions of the act regarding, amongst other things, mandatory reporting, due diligence, the preservation of data, organisation, and systems. On the other hand, it is deemed a weakness that monitoring established for these operations covers only those authorised to operate the data libraries but not authorised dealers, i.e. those who host the gaming machines. However, there are indications that risk awareness has increased, given the increase in notices to the FIU in recent years and the strengthening of the defences of the operators. Also, surveillance of and within the operations has been enhanced. Finally, the authorities have commissioned the publication of educational materials regarding gambling, along with general educational materials regarding money laundering.

In July 2023, plans were published in the consultation portal of the authorities regarding amendments to the Act on Slot Machines no. 17/1994, and the Act on the University of Iceland's Lottery no. 13/1973.¹¹² The purpose of the amendments is to respond to discussions in the most recent iteration of the risk assessment and thus to decrease the risk of money laundering and terrorist financing in the operations covered by these acts. Amongst other things, it may be assumed that there be more stringent legal requirements regarding the identification of gamers, for example, with the implementation of gaming cards. The intended amendments are focused on mitigating risk related to the operation, to the extent that they are implemented.

RISK CLASSIFICATION

HIGH

According to the above, the risk of money laundering in connection with the operations of slot machines and lottery machines is now deemed high.

¹¹² [Consultation portal | Consultation portal – Plans for amendments to laws regarding collection boxes and the Act on the Lotteries of the University of Iceland \(anti-money laundering and terrorist financing measures\) \(island.is\)](#)

4.5.5. GAMBLING ON THE INTERNET – FOREIGN OPERATORS

RISK CLASSIFICATION



GENERAL

Icelanders have ready access to foreign websites and apps which offer gambling and are able to set up gaming accounts and engage in all kinds of gambling on the internet. This refers to both gambling comparable to that which is accessible through Icelandic websites like sweepstakes, lotto, lotteries, and slot machines, where the service provider is bet against, and also games like poker where participants play against each other and the service provider takes a certain fee.

Gambling is not allowed in Iceland except under a special act, and the companies who offer gambling on foreign websites are not authorised to operate in Iceland. There is no domestic surveillance of gambling on foreign betting sites, as they are hosted in other states and operated from there.

Precise information regarding the scope of participation of parties domiciled in this country in gambling on foreign websites is not available and it is difficult to estimate. However, in December of 2022, a report was issued by the chief of a task force, which was established by the current Minister of Justice in March of 2021 and was meant to examine possible judicial improvements in the field of lotteries.¹¹³ The report states that it may be roughly estimated, according to information which the task force received from financial companies and supervisors, that parties residing in this country spend from ISK 10.5 to 12 billion on gambling on foreign betting sites in a year.

THREATS

The access of consumers in Iceland to foreign gambling on the internet is not subject to restrictions and the supply is considerable. Many service providers accept and execute payments in the form of electronic money, crypto-assets, and by other means of payment which are harder to trace than ones in which the gaming account is linked to a traditional bank account or payment card. Various methods to launder money through gambling online, gaming for ill-gotten funds and concealing the trail are known. Many of these methods require little planning, expertise or cost outlays. Among common methods one might mention:

¹¹³ *Judicial improvements in the field of lotteries - reports and proposals*. Chairman of a task force which was meant to investigate possible judicial improvements in the field of lotteries, Reykjavik 2022, pg. 22.

- Depositing funds into a gaming account and quickly withdrawing it or gaming/betting with limited risk of losing, for example, by using various gaming accounts or service providers and betting on “all possible results”. The aim of this, amongst other things, is to use winnings to account for funds in the keeping of offenders.
- For several collaborators to use the interface of the service provider as a sort of payment service to move funds quickly between parties and even across borders. For example, coworkers can play “against each other” and lose on purpose without arousing the suspicion of service providers.
- Also, gaming accounts are bought and sold and offenders use straw-men or fake ID to disguise the origins and hide the trail of funds from criminal activity.

A considerable amount of business and transactions go through foreign betting sites. Those who gamble can have many accounts and with various service providers and as service providers don't coordinate, it can be difficult to spot unusually prolific or suspicious gaming habits.

In the EU risk assessment from 2022 on the risk of money laundering and terrorist financing, the money laundering risk of gambling on the internet is assessed as very high, which is a greater risk level than in the previous EU risk assessment.¹¹⁴ The case is similar in the surrounding countries, such as in Denmark, where gambling is legal.¹¹⁵

The police has discovered indications that Icelandic offenders use gambling on foreign websites to launder money. Also, the FIU has received notices from foreign sister institutions regarding suspicions that foreign websites which provide gambling services have been misused for money laundering by parties registered as Icelandic citizens.

WEAKNESSES AND MITIGATING FACTORS

As previously stated, there are no restrictions on gaming on foreign websites or gambling apps by parties who reside in Iceland. In many countries, attempts are made to shut down such sites and/or prevent payments thereto. The proposals and summaries of the representatives of lottery companies in a task force focused on judicial reform in the field of lotteries included a summary of the measures taken by other countries to curb gaming on gambling websites.¹¹⁶ Norway has a state-run betting operation which is based on an exclusive licence and Norway restricts access to foreign gambling sites and forbids payment services thereto. In Sweden, betting operations on the internet are allowed but subject to a state licence. Since 2019, Sweden has restricted access to illegal betting sites. In Denmark, the operation of betting companies is subject to state authorisation. The authorities in that country restrict access

¹¹⁴ *Supra-National Risk Assessment Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. SWD(2022)/554. EU, Brussels 2022, pg. 236.*

¹¹⁵ *Den nationale risikovurdering af hvidvask. Hvidvasksekretariatet 2022. Danmarks finansielle efterretningsenhed (FIU.) Kaupmannahöfn 2023, pg. 222.*

¹¹⁶ *Proposals and summary of the representatives of lottery companies in a task force regarding judicial improvements in the field of lottery affairs to the Minister of Justice regarding amendments to jurisprudence regarding lotteries. Reykjavík 2022.*

to illegal gambling sites and keep a list of companies involved in illegal betting operations online.

The companies which run this operation are entities subject to mandatory reporting in other countries and there is no domestic surveillance of the operation, as the surveillance options of the Icelandic authorities in this context are limited. This means that the quality and scope of the surveillance depends on the abilities of foreign supervisors. This calls for additional cooperation and the sharing of information between the FIU and its sister institutions in other countries, some of whom have different requirements regarding anti-money laundering measures related to this activity.

Disclosure to the FIU from abroad regarding the betting of parties residing in Iceland is lacking. When examined in the context of the supply and estimated use in this country, it may be considered likely that this is attributable to lackluster monitoring and/or risk awareness rather than the service being free of all risk.

Finally, it bears mentioning that any profits acquired on these websites by a party with a tax domicile in this country are taxable in Iceland. It may be estimated that tax reporting of winnings is severely deficient and there is no particular monitoring of the taxation of such winnings.

RISK CLASSIFICATION

VERY HIGH

After taking into account the discussion on threats and weaknesses, the risk related to gambling on the internet is low.

4.6. COMPANY OPERATIONS

This section will examine company operations and whether there is risk in this country that criminals or organised crime will utilise companies for the purpose of laundering unlawful gains or concealing the beneficial ownership of assets resulting from unlawful operations. In this context, it will be examined whether certain forms of companies are more susceptible to risk and more likely to be misused than other ones.

Iceland has many companies and organisations, and their forms vary. There is no comprehensive legislation on companies, but laws have been enacted regarding different company forms, such as limited companies, private limited companies, and partnerships. The Business Registry of Iceland Revenue receives and maintains the registration of companies.

In differentiating company forms, they may be split into companies with a financial or non-financial purpose. In practice, companies with a financial purpose have somewhat more stringent requirements. For example, regarding the competence of board members and finances. Companies with a financial purpose may be classified according to the responsibility of its members for the company's obligations, i.e. whether members have unlimited or limited responsibility for the company's obligations. The discussion below considers three kinds of companies with a financial purpose. First, there are private limited companies. Second, there are limited companies, limited partnerships and self-governing institutions engaging in business operations. Third, there are other companies with a financial purpose. Then there is a discussion of general associations and non-governmental organisations (NGOs) having no financial purpose. Finally, non-profit organisations are covered.

The following table shows the number of registered companies which will be discussed by form of company at the end of the year 2022, according to information from the Business Registry. Other forms of association, such as homeowner associations, state institutions and one-person operations will not be especially covered.

THE NUMBER OF LISTED COMPANIES BY FORM OF COMPANY AT THE END OF THE YEAR 2022
Table 13

Companies with a financial purpose	Number
Private limited company (ehf.)	45,097
Limited company, general (hf)	556
Limited companies - public	18
Partnership limited by shares	86
Partnership limited by shares, general (slf)	3458
A self-governing institution that is engaged in business activity (ses)	149
General partnership (sf)	1948
Partnership of official entities	2
Other partnerships (undefined)	18
Co-operative societies (svf)	30
Housing co-operative	8
Other companies	Number
Associations	11,172
Non-governmental organisation	443
Political organisation:	19
Registered religious/lifestyle association	51
Self-governing institution with a confirmed charter	684*
Other self-governing institutions	11
Non-profit organisation operating across borders	47
Non-profit organisation	30

* Information from the National Audit Office.

As threats, weaknesses and mitigating factors were assessed, the supporting information was from parties such as the Business Registry, the Registry of Annual Accounts, the police, the FIU, the Directorate of Tax Investigations, information and reports from other official entities and the pertinent legislation. The following are the main threats and weaknesses and mitigating factors which pertain to company operations in this country. The risk related to each type of company operations will be covered further in the following sub-sections:

- It's generally easy and relatively inexpensive to found companies in Iceland and legal requirements of owners, founders and spokespersons are often not very stringent. Also, one can found and own "dummy companies" where requirements of operations are not made. Thus, it is possible to found many companies and establish a network of companies which may then be used with the sole purpose of laundering money. This more often applies to private limited companies than other companies.
- Companies can be subject to obligations regarding registration, taxation, bookkeeping accounts, and drafting and submitting annual financial statements. However, this does not apply to all companies. It depends on the company form and/or activity. Therefore, a birds eye view of companies, as well as surveillance and legal framework of their operations, is lacking. Coordinated procedure and efficient surveillance is also lacking, in order to identify money laundering and the possible misuse of companies, e.g. by analysis of operating figures and qualifications of spokespersons. Additionally, more efficient means are needed to wind up companies which are not operating or are not tending to their responsibilities, as well as more efficient penalties if spokespersons have violated laws.
- Therefore, the number of companies in Iceland is very great and there are many ways to use companies for predicate offences or money laundering, which have been allowed to operate in Iceland screened, it would appear, by a certain culture and lack of monitoring, legal resources, and penalties. In this context one could mention ID number-hopping, the use of straw-men, illicit employment, self-dealing from the funds of a company, artificial transactions, organised tax fraud, misrepresentation in accounts and failure to submit annual financial statements or other reports which are due.
- However, one can see signs that risk awareness is increasing among the authorities, which is best demonstrated by the number of new laws and amendments in recent years related to companies and anti-money laundering and terrorist financing measures. This includes provisions regarding an operational ban which is meant to curb ID number hopping and new laws on forms of companies, e.g. non-profit organisations, which are known to have been utilised for terrorist financing in other states. However, the most extensive amendment is the Act on the Registration of Beneficial Owners of companies, which will be discussed before the risk of particular forms of companies will be assessed. One must bear in mind, however, that many of these laws or amendments are new and, therefore, there hasn't been enough experience regarding their implementation and deterrent effect.

4.6.1.1. BENEFICIAL OWNER

6 July 2019 saw the entry into force of the Act on the Registration of Beneficial Owners no. 82/2019. This was the first legislation on this matter in this country and a great piece of judicial reform, as up until that point the arrangement of the registration of beneficial owners differed from legal person to legal person. The purpose of the act is to ensure that correct and reliable information on beneficial owners of legal persons within the scope of the act is available at all times to analyse and prevent money laundering and terrorist financing, cf. Paragraph 1 of Article 1 of the Act.

Beneficial owner (BO) is defined in the AML Act as natural persons, one or more, who ultimately own or control the customer, legal entity or natural person on whose behalf a transaction or activity is being conducted or carried out. The Act on the Registration of Beneficial Owners no. 82/2019 builds on the above definition. In this context, one differentiates between legal owners and BOs. A legal owner is a person registered as an owner of money, assets, or companies. However, he need not necessarily be the BO. Parties can see that it is to their advantage to conceal their ownership. For example, by getting other parties to act as a legal owner through founding a complex network of companies or asset-holding companies (dummy companies) or in another manner. BO is always an individual and is the one who can make decisions on the disposition of funds, management of parties or the party benefiting from the assets involved.

The act covers legal persons engaging in business operations in Iceland or that are registered in the Business Registry, including foreign branches of limited companies and private limited companies. The act also applies to foreign trust funds or comparable parties engaging in business in the country. However, the act does not apply to institutions and companies owned by the State or municipalities, nor does it apply to legal persons registered on a regulated market as defined by the Act on Stock Exchanges. In case of doubt, the Directorate of Internal Revenue will determine whether a party or category of parties falls under the act. Finally, information about BOs of a legal person shall be on record in the Business Registry operated by the Directorate of Internal Revenue. Registration agents must provide notice of all changes in registration

Section III of Act no. 82/2019 prescribes penalties. The act provides two kinds of penalties, i.e. daily fines on entities subject to registration, and administrative fines on individuals or legal entities. The act also contains the authority to terminate and deregister entities subject to registration. In October of 2022, an interim provision was added to the act, which was meant to provide the Directorate of Internal Revenue with simpler and more efficient remedies than previ-

ously provided for in the act, to initiate exchanges or windups of parties with a duty to register which had neglected their duties.¹¹⁷

Since the entry into force of Act no. 82/2019, much effort has been put into finalising the registration of beneficial owners of the 62,855 parties with a duty to register which were listed on the Business Registry at the time of entry into force of the act. Most of the penalties provided for in the act have been employed which has, amongst other things, led to the deregistration of many companies. According to the Business Registry, only six companies had yet to register beneficial ownership in November of 2023.

No new company receives an ID number unless it adequately registers the beneficial owners. After new registration it is the responsibility of the companies to update the registration. The main threats regarding the registration of BOs are that the registration will not be correct and that someone other than BO is registered for the sole purpose of concealing actual ownership and, at the same time, a possible trail of money. There have been instances where the registration of beneficial owners has proved wrong or outdated, e.g. with regard to a request from a bank for a certificate of beneficial owner registration when the company wants to initiate a business relationship. Also, the initiative surveillance of the Business Registry has revealed, from a random sample, that the registration is not always adequate. Finally, the police and tax authorities confirm that despite the legal obligation, there are still numerous examples of attempts to conceal beneficial ownership. It's clear that it will be an ongoing task for the Business Registry to maintain the quality of registrations with surveillance measures, education and comments to companies and that with the aid of financial companies and other parties subject to mandatory reporting who play an important part in authenticating the reliability of information. It is also considered a weakness that the Business Registry lacks remedies to authenticate beneficial ownership and deregister legal entities more simply and efficiently due to incorrect or misleading registration of the beneficial owner.

¹¹⁷ <https://www.althingi.is/altext/stjt/2022.139.html>

4.6.2. PRIVATE LIMITED COMPANIES

RISK CLASSIFICATION



GENERAL

Private limited companies are companies where no member is personally responsible for the total debts of the company and they are subject to Act no. 138/1994. It is by far the most common company form and the number of private limited companies by the end of the year 2022 was just over 45,000. In the years 2021 and 2022, just over 3000 new private limited companies were founded each year. More private limited companies by far are founded each year than are wound up and the total number of registered private limited companies has increased each year by just over 1500 companies on average each year in recent years.¹¹⁸ The Business Registry receives and keeps track of the registration of companies.

Founding private limited companies requires the following information and/or conditions to be met:

- There shall be share capital of at least ISK 500,000, but there is no condition that this involves cash.
- There must be articles of association (a charter,) stating, for example, information on the founders. The founders can be individuals, the Icelandic State and its institutions, municipalities and their institutions, registered limited companies, registered co-operatives, other registered companies with limited liability, registered partnerships, registered limited partnerships, registered organisations, pension funds and self-governing institutions that are subject to governmental monitoring. Furthermore, the above companies and institutions that are domiciled in the European Economic Area (EEA) or member states of the European Free Trade Association can also be founders.
- Proposed by-laws stating, amongst other things, what the company's purpose is.
- The minutes of the inaugural meeting, where, for example, a memorandum of association shall be presented. However, notice of the company's registration shall be made within two months from the date of the memorandum of association.

¹¹⁸ [Number of listed corporations and companies by their legal form 2005-2022. PxWeb \(hagstofa.is\)](#)

The following qualifications are set for the founders of a private limited company:

- A founder may neither have requested nor be in a payment moratorium, nor may his estate be in bankruptcy proceedings.
- If he is an individual, he shall have legal capacity.

Also, spokespersons of a private limited company, i.e. members of the board of directors and managing directors, shall fulfil the following qualifications:

- Being of legal age.
- Control of own assets.
- In the last three years, in connection with business operations, may not have been convicted of a punishable act under the GPC or acts on limited companies, private limited companies, accounting, annual financial statements, bankruptcy or governmental fees.

There are no qualifications for owners of private limited companies who are not also founders or spokespersons.

It is easy to found a private limited company, and forms are accessible on the homepage of Iceland Revenue. There is no condition for a private limited company to be in operation or in business. Information on the number of registered private limited companies in operation is not available. Their operations can be diverse, but they most often involve overall management of the operations of a specified economic activity. Act no. 138/1994 has various instructions on the handling of a private limited company's assets, such as the distribution of dividends and lending. These involve rather stringent conditions. In previous years, for example, judgments have ruled that payments from a private limited company's funds cannot be connected with shareholders' finances except insofar as they involve interests regarding shareholding. Also, dispositions shall respect lenders' interests, and shareholders shall not be enriched inappropriately at the company's cost.

Private limited companies are obligated to pay taxes and, like other companies engaging in economic activities, are required to keep accounts in accordance with Accounting Act no. 145/1994. They must, amongst other things, preserve the accounting and ensure that it is possible to base an annual financial statement on it.

Private limited companies are obligated to prepare and submit annual financial statements in accordance with the Act on Annual Accounts no. 3/2006, and are obligated to employ an examiner or accountant. After fulfilling certain conditions, a private limited company can be deemed a "micro-company," as defined in Act no. 3/2006, and is thereby exempt from the obligation to submit annual financial statements. Surveillance of submissions is the responsibility of the Directorate of

Internal Revenue which operates the Register of Annual Accounts registry and Act no. 3/2006 includes penalties for not submitting an annual financial statement. The penalties are a governmental fine of ISK 600,000 and a demand for corrective action. However, the fine can decrease if a company submits an annual financial statement before a certain amount of time has passed from the notification of the decision to levy the fine. There is also a clause in the act which provides for requiring liquidation if the nonperformance is severe. The Register of Annual Accounts has fined over 4000 companies on average each year and liquidation was first required in 2022. The submission of annual financial statements has gradually improved in previous years. In 2021, the submission of annual financial statements by all companies subject to surrender requirements was close to 91.5%. On the other hand, almost half of the companies submitted annual financial statements after the legal deadline on 31 August 2022.

Generally, a private limited company can cease to exist in three ways, i.e. by merger, winding-up or bankruptcy. Act no. 138/1994 covers windups of companies and mergers. The Act on Bankruptcy etc. no. 21/1991 contains rules on a company's bankruptcy. Stringent rules apply to the disposition of a company's assets in the lead-up to bankruptcy and after the proceedings have begun. However, such conduct may be punishable under the General Penal Code. In practice, such criminal liability can be a considerable test.

THREATS

One risk is that the private limited company's form will be misused in various ways. The main threats are as follows:

- It is easy, inexpensive and quick to found a private limited company. Because of their number and the frequency of their founding, it is simple and easy to establish a network of companies that can be used to launder money by various means. It is also possible to have companies with no operations, i.e. "dummy companies," since there are no requirements regarding operations or activities and there are examples of attorneys and accountants being stocked with such companies.. Dummy companies can be founded for the sole purpose of laundering money and they can be resorted to when the need arises.
- There are no legal requirements for private limited companies' owners. In addition, the requirements for founders are limited. Finally, the remedies applicable to board members or managing directors of private limited companies are inefficient, and, in this respect, monitoring by the Business Registry is limited. For example, if a board member or managing director becomes unfit for his post, they shall inform the Business Registry of this. On the other hand, there are no examples of the Business Registry being informed of such instances.

- It is easy to extract money from a private limited company and make disbursements from its funds with self-dealing, e.g. by expensing owners' private consumption unlawfully cf., for example, Landsréttur Appeal Court judgment (Lrd.) 28 April 2023 in case no. 271/2022, Lrd. 18 November 2022 in case no. 633/2021, Lrd. 20 November 2020 in case no. 533/2019, The judgment of the Supreme Court (Hrd.) 3 November 2016 in case no. 738/2015, The judgment of the Supreme Court (Hrd.) 22 November 2016 in case no. 499/2015. Disbursements of such assets can entail money laundering. In recent years, several judgements have stated that a private limited company's owner cannot identify his private interests with the company's, cf., e.g. Hrd. 6 April 2017 in case no. 770/2015, and Hrd. 28 April 2016 in case no. 74/2015.
- Black operations thrive in Iceland. Amongst other things, reports about tax evasion have been written and made public.^{119, 120} Figures regarding this vary, but observers deem that the scope of hidden operations can range from 3% to 7% of gross domestic product and that it is especially common among contractors and in other professions. Various kinds of tax fraud fall under this heading, such as the evasion of value-added tax, evasion of income tax on wages and wage-related payments, unreported income tax on business operations because of over-reported costs or under-reported income and other unpaid taxes, including those related to income from offshore companies. The tax authorities and police have systematically tried to address this. Available information shows that, in parallel with the operations of private limited companies, there are sometimes instances of black operations.
- In Iceland, the failure to report assets and "ID number-hopping" are major problems in company operations, i.e. when companies petitioning for bankruptcy transfer their assets to a "new ID number" while leaving the company's debts behind under "the old ID number". Thus, the company's owner can continue to operate without paying its debts because creditors can only file claims against assets registered under the old ID number. In this way, a company can avoid paying off creditors, especially other private limited companies. The same can apply to other governmental fees and taxes. Judicial practice has numerous examples of evasion involving assets and taxes upon bankruptcy. Examples are also known of courts dealing with ID number-hopping, where the private limited company form has been misused, cf. e.g. Hrd. 6 April 2017 in case no. 770/2015.
- There are many examples of individuals being persuaded to found, or register as management of, a private limited company as a sort of a straw-man, in order to disguise who truly owns and operates it. In this sense, incorrect information regarding beneficial owners is wittingly conveyed to the Busi-

¹¹⁹ *Scope of tax evasion and proposals for actions. Report of task force.* The Ministry of Finance and Economic Affairs, Reykjavik, 2017.

¹²⁰ *Issuance of Bogus Invoices - The Nature of the Behaviour and Possible Scope - Proposals for Actions.* The Ministry of Finance and Economic Affairs, Reykjavik 2023.

ness Register of Iceland Revenue and other parties subject to mandatory reporting. In this way, beneficial owners and gains can be isolated from the predicate offence, which renders it difficult to elucidate and investigate alleged money laundering and seize gains. This can take place right at the beginning of operations and under the operation and it is especially common shortly before the bankruptcy of companies, in which cases straw men are called “funeral directors”. In such cases the aim is, amongst other things, to prevent those responsible for the losses from being implicated in the bankruptcy, e.g. to keep them from being put on the defaulters’ list and to make it less likely that a court-case be filed against them which would render them unqualified to be involved in a new limited liability company in the near future.

- There is no duty to wind up a private limited company which has stopped operating. There are instances of “empty” companies having been misused and their bank accounts used to conceal a trail of money.
- One form of criminal activities within otherwise lawful operations are various artificial transactions between related parties that, for example, can stretch across borders. One example of this is the issuance of unfounded invoices for services never rendered, the issuance of invoices for products not of the quality and/or quantity which might have been assumed, under-pricing and/or over-pricing or refunds of a simulated loan which did not take place in reality. This is done, amongst other things, in order to get funds and products between parties and/or countries, get funds into or out of off-shore companies in tax havens, sever the trail of funds or to avoid having to pay value added tax, as is covered in more detail in the section on tax fraud as a predicate offence of money laundering. There are numerous examples of the private limited company form having been misused in such a way.
- Finally, it is usually considered easy for offenders to circulate ill-gotten funds through various kinds of retail operations and services, e.g. with a private limited company founded around the operation which they own or to which they have access. In markets where cash transactions are common the danger is that offenders and individuals affiliated with organised crime will try to launder the gains of their criminal activity by funnelling such funds into legal operations which sell various products and services. There are few restrictions on cash transactions and the use of cash in this country, cf. the discussion in the section of the risk assessment on cash. Commercial and service operations make it easier for offenders to account for cash and anonymous transactions under 10,000 euros as there is seldom a requirement for transactions to be traceable. There are indications that retail trade comprises over half of all cash within the banking system.

The number of private limited companies and the frequency with which new companies are founded renders it more complex to keep track and monitor them and offenders try to take advantage of that. There are also many examples with the police and tax authorities of companies being misused to launder and/or cover the trail of funds and the private limited company form is the company form which is by far most commonly used for that purpose.

WEAKNESSES AND MITIGATING FACTORS

According to the above, various threats beset the operations of private limited companies, and various things have been lacking in laws and monitoring that could counteract money laundering or reduce its likelihood, such as regarding:

- the qualifications of founders, board members, and owners of private limited companies,
- checking up on board members' loss of eligibility in private limited companies,
- swapping the directors of private limited companies shortly before bankruptcy for “funeral directors”,
- more stringent penalties for deficiencies in submissions of annual financial statements, and
- de-registration and termination of companies when they are no longer in operation.

Governments also lack legal remedies enabling them to exchange information on company operations, regarding, for example, the loss of eligibility. For example, the Business Register, which is meant to monitor the eligibility of the directors of companies, does not have access to the criminal records of the state or another centralised, real-time database with information on punitive sentences which could effect the eligibility of directors and, therefore, the surveillance is inefficient.

In addition, there has also been a considerable lack of monitoring for money laundering, possible misuse of the private limited company form and various things connected with private limited companies' operations, e.g. regarding analysis of numerical information from companies' annual financial statements. Active surveillance of annual financial statements is limited and, for instance, not based on a focused analysis of *modus operandi*, e.g. regarding analysis of profits in the annual financial statements of companies within the same industry, operating expenditure and possible tax evasion.

Finally, there has been no instruction regarding money laundering for those founding companies and/or their directors. Also, it appears that risk awareness in that area is rather low.

Regarding mitigating factors, one can see signs that risk awareness is increasing in this country regarding private limited companies' operations and money laundering, as authorities' determination to address ID number-hopping shows.¹²¹ In this regard, it is also worth mentioning amendments of the General Penal Code, the Act on Limited Companies, the Act on Private Limited Companies, and the Act on Self-governing Institutions Engaging in Business Operations. They aim at clamping down on the misuse of the limited company form. ID number-hopping is the primary target there. More specifically, this involves amendments made in June of 2019 to Article 262 of the GPC regarding prohibited business activities.¹²² In judicial practice, the ban has been employed a few times. A parliamentary bill was also introduced to amend the Act on Bankruptcy etc., no. 21/1991 (ID number hopping) at the end of the year 2022. The purpose was to clamp down on the misuse of the limited company form and ID number-hopping in business activities.¹²³ Finally, the passage of the Act on the Registration of Beneficial Owners no. 82/2019, which requires information to be on file on the real ownership of companies, is a substantial improvement. The relevant authorities will therefore always have access to information on companies' beneficial ownership, as is covered in more detail in the risk assessment in the introduction on the operation of companies. All of these amendments are relatively new and, therefore, there hasn't been enough experience regarding their implementation and deterrent effect.

RISK CLASSIFICATION

VERY HIGH

There are major threats and weaknesses in the framework of private limited companies as mentioned above. For these reasons, the risk of founding, operating, and winding up private limited companies is deemed very high.

¹²¹ *Report of the task force of the Ministry of Social Affairs and Children against social underbidding and illegitimate operations in the labour market.* Ministry of Social Affairs, Reykjavik 2019.

¹²² <https://www.althingi.is/altext/stjt/2019.056.html>

¹²³ <https://www.althingi.is/altext/stjt/2022.133.html>

4.6.3. LIMITED COMPANIES, LIMITED PARTNERSHIPS AND SELF-GOVERNING INSTITUTIONS

RISK CLASSIFICATION



GENERAL

Act no. 2/1995 applies to limited liability companies and partnerships limited by shares. The main characteristic of limited companies is that shareholders are not responsible for the debts of the company in excess of the capital which they invested in the beginning. The shareholders' meeting is the highest authority in company matters, makes major decision regarding it and elects a board which can make other decisions. A partnership limited by shares is a type of partnership where one or more members bear direct and unlimited responsibility for the debts of the company while other members (shareholders), one or more, bear no personal responsibility in excess of the capital which they invested in the company. The minimum stock is ISK 4,000,000 and there must be at least two founders and the shares of the company must be held by two or more parties. In most respects, however, legal requirements for limited liability companies and partnerships limited by shares are comparable to those which apply to private limited liability companies.

No separate law applies to limited partnerships, but the Act on Commercial Registries, Firms and Proxies no. 42/1903 contains scattered provisions on such organisations. The limited partnership is a form of partnership based on an agreement of two or more parties on a common financial operation. The liability of certain members for the debts of the company is direct, joint and unlimited while others are only liable for the debts of the company in the amount of their capital contribution (partners.) Thus, their financial risk is limited in a similar way as that of members in limited liability companies, i.e. limited to a certain amount. The liability in partnerships limited by shares and limited partnerships is mixed.

Self-governing institutions engaged in business activity fall within the scope of Act no. 33/1999. A self-governing institution is not a company but a certain form of association. Such an institution's main characteristic is that it is self-owned, i.e. that no defined party lays claim to the assets of self-governing foundations. Self-governing institutions engaging in business operations shall be dealt with as organisations with limited liability, as applicable under Act no. 33/1999. A self-governing institution does not involve share capital but rather initialisation capital that shall not be less than ISK 1,000,000. No qualifications

are required for founders of a self-governing institution. However, the same qualifications are required for the board members and managing director as in limited liability companies and private limited liability companies.

At the end of the year 2022, the number of limited liability companies was just under 600, the number of self-governing institutions engaging in business operations was about 150, that of partnerships limited by shares was almost 100 and that of limited partnerships was just over 3450, as the number of the latter has increased in recent years.

THREATS

Many of the threats applying to private limited liability companies apply to limited liability companies, partnerships limited by shares, limited partnerships, and self-governing institutions that engage in business operations. On the other hand, these organisations are many times fewer than the private limited liability companies and fewer of them are founded per year. Nevertheless, it bears mentioning that the increase in the number of limited partnerships has been proportionally greater than that in the number of private limited liability companies in recent years.

Finally, the instances of their misuse are nowhere near the percentage for the private limited liability company form. It is also more difficult to use these company forms to launder unlawful gains. For further explanation, one might note that not as many individuals are involved in the founding of a private limited liability company as in that of a limited liability company and the requirements for auditing of accounts are more stringent in the case of large limited liability companies than in the case of private limited liability companies.

WEAKNESSES AND MITIGATING FACTORS

Many of the weaknesses applying to private limited liability companies apply to limited liability companies, partnerships limited by shares, limited partnerships and self-governing institutions that engage in business operations. However, there are somewhat more stringent requirements for founding a limited liability company than a private limited liability company – for example, the amount of the share capital contribution and the number of shareholders. On the other hand, there is a lack of formality in the articles of association of limited partnerships.

Most of the mitigating factors applying to private limited liability companies also apply to these company forms.

RISK CLASSIFICATION

MEDIUM

The risk related to the forms of association of limited liability companies, partnerships limited by shares, limited partnerships and self-governing institutions that engage in business operations is deemed to be medium.

4.6.4. OTHER COMPANIES WITH A FINANCIAL PURPOSE

RISK CLASSIFICATION



GENERAL

Hereunder are company forms other than those discussed above having a financial purpose. Most of these organisations are partnerships. There were about 1950 of them at the end of 2022 and their number has decreased somewhat in recent years. A partnership is a company form based on an agreement between two or more parties on a joint financial operation where liability for the debts of the partnership borne by all members of the company is direct, joint and unlimited. Act no. 50/2007 applies to partnerships.

Other company forms are, for example, cooperatives, European financial interest groups and European companies. Special acts apply to all of the above company forms.

THREATS

There are no known threats regarding these company forms and no examples of their misuse.

WEAKNESSES AND MITIGATING FACTORS

Few of the weaknesses discussed above apply to the company forms involved here, for example, regarding their number and examples of misuse. There are also no mitigating factors to consider.

RISK CLASSIFICATION

LOW

For the above reasons, the risk of money laundering misuse of company forms with a financial purpose other than those discussed in the previous sections is low.

4.6.5. NON-GOVERNMENTAL ORGANISATIONS AND ORGANISATIONS

RISK CLASSIFICATION



GENERAL

General associations and nongovernmental organisations (NGOs) are structured, permanent organisations of two or more parties that are founded with a private law instrument for a non-financial purpose. In other words, general associations are not operated for profit. No act provides for the structure of general organisations or associations, and the provisions of the articles of association are therefore very important in construing their legal status. In addition, the main rules of company law are also considered. As examples of general organisations and NGOs, one can mention political parties, sports associations, chess associations, professional associations, occupational associations, associations of employers, humanitarian associations, cultural associations, and non-profit organisations who are neither registered as NPOs according to Act no. 110/2021 nor Act no. 119/2019. It is possible to register general associations and NGOs in the Business Registry under the Act on the Business Registry no. 17/2003, but they have no duty to register, and a separate application must be made to do so. Furthermore, the Business Register contains information regarding the founding documents and articles of association of the registered companies.

General associations and NGOs are not intended to engage in business operations. However, if they engage in fund-raising or trust activities, they are legally required to keep accounts in accordance with Act no. 145/1994 and must prepare an annual financial statement. On the other hand, they have no duty to submit an annual financial statement under the Act on Annual Financial Statements no. 3/2006.

In recent years, the Business Register has deregistered many associations without assets which had not submitted information on the beneficial owners. At the end of the year 2022, the number of general associations and NGOs was 11,600 and their number has decreased by about 4500 from the entry into force of the Act on Registration of Beneficial Owners no. 82/2019.

THREATS

Founding general associations can be done easily, inexpensively and quickly and their operations can be affected and the number of registered associations and NGOs is considerable. It is also easy to launder money through their operations since such compa-

nies have no requirements regarding finances. Finally, misusing the company form requires no expertise.

The police have no examples of misuse of this company form. The DTI, however, has several such examples.

WEAKNESSES AND MITIGATING FACTORS

There is no monitoring of the operation of general associations and no institution or organisation is tasked with providing an overview of their operation. The operation is limited by the articles of association of each company but no general qualification requirements are made of their founders, owners or spokespersons or regarding their expertise to handle finances or accounting. Also, there is no information anywhere regarding the finances and accounting of general associations. Furthermore, there are no rules or instruction on the operations of general organisations except that their purpose must be legal. No other rules apply to the operations of such companies and clubs, other than those they set for themselves as articles of association. Finally, no instruction on the operations of general organisations have been issued on the management practices of such companies.

A mitigating factor is the duty to register BO of a general company or club. This is intended to detect and prevent money laundering, cf. the Act on the Registration of Beneficial Owners no. 82/2019.

RISK CLASSIFICATION

HIGH

Considering the foregoing threats and weaknesses, after taking into account mitigating factors, the risk of misuse of this company form must be deemed high.

4.6.6. NON-PROFIT ORGANISATIONS

The purpose of non-profit organisations is to serve the public good. The main reason for considering such associations is that FATF heavily emphasises company forms in FATF states where such companies have been misused, especially for terrorist financing. In preparing the risk assessment, FATF's definition of NPOs was kept in mind. The task force defines such organisations 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"."*¹²⁴ On this basis, the discussion was limited to registered religious and lifestyle associations, associations and funds that operate under a certified charter and other NPOs.

4.6.6.1. RELIGIOUS AND LIFESTYLE ASSOCIATIONS

RISK CLASSIFICATION



GENERAL

Religious and lifestyle associations operate under Act on Registered Religious and Lifestyle Associations no. 108/1999 and the regulation on the registration of such associations no. 106/2014. The act provides for people's right to found religious associations and practice their religion in accordance with their con-

¹²⁴ *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. FATF, Paris 2023.*

victions. At the end of 2022, there were 51 religious and lifestyle associations, according to information from the District Commissioner of North East Iceland. Of these, 44 are religious organisations, and seven are lifestyle associations. Registration entails certain statutory rights and duties for such associations, including the right to a share in levied income tax in the form of congregational fees. In 2022, this amount was ISK 13,284 per person per year. In 2022, about ISK 3.1 billion in congregational fees was paid from the State Treasury, of which just over ISK 2.4 billion went to the State Church.¹²⁵ The act sets several general conditions for the registration of such associations.

Spokespersons for registered religious and lifestyle associations must be at least 25 years old and fulfil general qualifications to work for the civil service, other than those regarding citizenship. Those requirements regard not having been convicted of a criminal deed while in public service. There are no other qualifications, such as a spotless criminal record or certificate of no bankruptcy proceedings. There are no requirements for founders or board members, and, for example, there is no requirement that they must reside in Iceland or have other connections with the country. Additionally, there is no requirement that board members shall be registered in the association or a requirement that they shall actually be involved in its operations.

The District Commissioner of North East Iceland oversees the registration of religious and lifestyle association and handles surveillance. The surveillance of the District Commissioner mostly pertains to the disposition of the funds going into such associations in the form of congregational fees and the status of the directors. If the association no longer fulfils the conditions for registration or neglects its statutory duties, the district commissioner can cancel its registration after a preceding warning and deadline for rectification. The act otherwise says little regarding the district commissioner's monitoring and authorisations in this regard. In addition, the act does not provide for penalty-related remedies.

There are no rules on the disposition of the funds of religious and lifestyle associations, except that these associations are obligated to send a district commissioner an annual report on their activities in the previous year and on changes to information which appeared at registration. Changes to the list of members and the disposition of the funds of the company are to be especially accounted for. Also, monitoring of the finances and accounts of these companies is limited and the remedies of the supervisor are limited. No qualifications are required for those seeing to the associations' finances.

In recent years, reporting of these religious and lifestyle associations on operations and, thereby, their finances, to the district commissioner has decreased. When the deadline for reporting the operation of the years 2021 and 2022 expired in March of the following years, only about half of religious and lifestyle associations had handed in a report.

¹²⁵ *Parochial dues 2022. Financial Management Authority, Reykjavik 2023, pg. 2.*

THREATS

The main threat from operations like these is that the company form will be misused to benefit criminal activities, including for laundering unlawful gains, as conditions for the founding of such companies aren't especially stringent and little requirements of qualifications are made of spokespersons. Monitoring of the finances of these associations is limited and, therefore, there is a possibility of allocating the congregational fees elsewhere than towards the operation of the associations. There is one known example of a religious association which was misused to engage in alleged criminal conduct and money laundering. That case is going through the criminal justice system.

Because of the nature of these associations, people of foreign origin or who have relations to other countries often have access to them and, depending on circumstances, possibilities to work across borders. This can entail a threat.

WEAKNESSES AND MITIGATING FACTORS

There are weaknesses in the framework, legislation, and monitoring of registered religious and lifestyle associations. The weaknesses especially regard the unsatisfactory provisions on the qualifications of these associations' spokespersons, accounting, and finances. Also, legal remedies to enable monitoring of these associations' activities are lacking, e.g. regarding report submissions. In July 2023, plans were published regarding a bill to amend the Act on Registered Religious and Lifestyle Associations no. 108/1999 in the consultation portal of the government. The aim of the amendments is, amongst other things, to respond to discussions in the most recent version of the risk assessment, which is mostly unchanged.¹²⁶

Few religious and lifestyle associations are registered, and cases related to the misuse of this company form are rare. There are also indications of increased risk awareness of the operations of NPOs. Finally, educational materials have been published regarding NPOs and courses and informative meetings have also been held for NPOs.

RISK CLASSIFICATION

HIGH

Considering the above, one must deem that there is still a high risk of misuse of this organisation form.

¹²⁶ [Consultation portal | Consultation portal – Plans for amendments to laws regarding registered religious and lifestyle associations and the Act respecting Foundations Engaging in Business Operations \(anti-money laundering and terrorist financing measures\). \(island.is\)](#)

4.6.6.2. FUNDS AND ORGANISATIONS OPERATING UNDER A CERTIFIED CHARTER

RISK CLASSIFICATION



GENERAL

Funds and Associations Operating under a Certified Charter are covered by Act no. 19/1988 and Regulation no. 140/2008 on the same subject. This involves funds and associations falling under the heading of self-governing foundations with no financial purpose that operate under a certified charter. Upon founding, money is paid into the fund or association by gifting, a will, or another private law instrument. These funds are intended to be utilised for one or more goals that can be of various kinds.

The charter shall specify the initialisation funding, its source, what the goals of the fund or association are, and how the funds shall be spent to achieve those goals. After taking into account changes in the credit terms index in 2023, a fund's minimum initialisation funding may be ISK 1,480,000.¹²⁷ The charter shall also report how the board of directors of a fund or association shall be appointed, and who shall be responsible for management of the assets. In addition, no later than 30 June each year, the party responsible for a fund or association shall send the Icelandic National Audit Office the fund's or association's accounts for the previous year along with a report on the disposition of funds that year. There are no qualifications for those managing such funds and associations.

The District Commissioner for Northwest Iceland is responsible for the implementation of Act no. 19/1988 and shall maintain a register of funds and associations in accordance with the act. In addition, the State Auditing Office shall keep a register of the total income, expenditures, assets, and liabilities of all registered funds and associations, as well as comments on submitted accounts. If a report and accounts of a fund or association have not been received for one year, or the accounting proves to be deficient, the district commissioner, after receiving recommendations from the Icelandic National Auditing Office, can entrust the chief of police to investigate the finances of the fund or association and seize documents and assets. The chief of police shall then be responsible for stewardship until the district commissioner has otherwise arranged matters.

The Icelandic National Audit Office annually publishes an abstract from the

¹²⁷ [Application for the confirmation of a charter for a new fund or self-governing institution | Island.is \(island.is\)](#)

annual financial statements of associations and funds operating under a certified charter. According to published abstracts for fiscal 2021, published in January 2023, there were 684 active associations and funds operating under a certified charter at the end of the year 2022. Also, five new charters were confirmed during the year, and 16 associations and funds, deemed unqualified, were closed down. In December of 2022, 403 funds and associations had submitted annual financial statements to the Icelandic National Audit Office for fiscal 2021, while the deadline was set at 30 June 2022. Altogether, 693 funds and associations were obligated to submit annual financial statements for that year, and therefore only 58% of the annual financial statements were received six months after the deadline. A total of 42 funds and associations have never submitted an annual financial statement despite having a legal obligation to do so.¹²⁸

According to the Icelandic National Audit Office's abstract, the associations and funds operating under a certified charter greatly vary in size. Thus, the value of assets of the 48 funds submitting an annual financial statement for 2021 were less than ISK 500,000. Of these, 13 funds had no assets at the end of 2021. Of the 403 associations and funds submitting annual financial statements, 193 of them had income in 2021. Of the 210 funds that had no income during the year, 97 of them had no expenditures. In addition, four funds had neither income nor expenditures, nor did they have assets at year-end 2021.

THREATS

The main threat from these operations is that criminals or a criminal organisation will misuse such funds and associations. Founding them is relatively simple, and it is easy to exercise control of them without any of the information being recorded. In addition, there are no stringent requirements for supervising assets. Statutory monitoring especially pertains to the submission of annual financial statements. However, such submissions are unsatisfactory. One must consider that more than 40% of more than 700 associations and funds do not submit annual financial statements or submit them too late and that ratio is higher than when the risk assessment was updated two years ago.

However, there are no known examples of a fund or association operating under a certified charter being misused for money laundering in this country.

WEAKNESSES AND MITIGATING FACTORS

Act no. 19/1988 is past its prime and must be thoroughly reviewed, considering that far too many funds and associations fail to submit annual financial statements and that monitoring of the operations is limited. There are no penalties for not submitting an annual financial statement and the remedies prescribed in the act are few and, seemingly, not as useful as they should be. There are also no qualifications in the act for those managing such funds and associations.

¹²⁸ *Self-owned organisations and funds that operate under an approved charter for the 2021 operating year. Excerpt from the annual accounts. National Audit Office, Reykjavík 2023, pg. 3.*

In July 2023, plans were published regarding a bill to amend the Act on Funds and Associations Operating Under a Certified Charter no. 19/1988 in the consultation portal of the government. The aim of the amendments is to respond to discussions in the most recent version of the risk assessment, which is mostly unchanged.¹²⁹

Despite a rather high number of institutions and funds, cases related to misuse of this company form are quite rare.

RISK CLASSIFICATION

HIGH

Considering the above, it must be deemed that the risk that such associations or funds will be used for laundering unlawful gains is still high.

4.6.6.3. OTHER NON-PROFIT ORGANISATIONS

RISK CLASSIFICATION



GENERAL

This category includes organisations and associations working in the public interest. Therefore, the consideration here is the organisation's purpose, not its form and the main purpose is usually to collect or distribute funds in the public interest, as for charitable institutions, religious issues, cultural issues, educational issues, social issues or other charities. These organisations may be subdivided into three categories. Organisations operating under the Act no, 119/2019 on the Obligation of Non-profit Organisations to Register, companies operating under the recent Act no. 110/2021 on NPOs and other general organisations and NGOs who are not run for profit but work towards the public interest. The final company form is also covered in the section on general organisations and NGOs previously mentioned in the risk assessment.

¹²⁹ [Consultation portal | Consultation portal – Plans for amendments to laws regarding registered religious and lifestyle associations and the Act respecting Foundations Engaging in Business Operations \(anti-money laundering and terrorist financing measures\) \(island.is\)](#)

Non-Profit Organisations operating across borders are obligated to register under the Act no. 119/2019. At the end of 2022, there were about 47 organisations and the scope of these organisations is not great. The act sets forth, amongst other things, conditions for management of a company, minimum qualification requirements for directors, accounting, and annual financial statements. According to Paragraph 2 of Article 38 of the AML Act., cf. the act amending Act no. 96/2020, Iceland Revenue monitors such organisations with regard to money laundering and terrorist financing.

NPOs working according to Act no. 110/2021 are also registered in the NPO-register of Iceland Revenue. These are organisations founded or operated for the purpose of promoting specific public interest issues according to their articles of association, and whose operation does not reach across borders. The registration of such organisations is optional and meant for organisations where the size, scope and nature of the operation involves the obligations and rights covered by the act. However, the state, municipalities, official institutions and other legal entities, the majority of which is publicly owned, may set the condition for grants, operational contracts and official licences for companies that they be registered in the NPO-register. By year-end 2022, the number of registered NPOs was only 30, when the act had been in force for over a year. The requirements for the above organisational form regarding management, accounting and annual financial statements is quite similar to those for NPOs operating across borders.

At the end of the year 2022, the number of general associations and NGOs was just over 11,600. The Business Register does not categorise organisations by their purpose and, therefore, information regarding the number of registered general organisations and NGOs working in the public interest is not available in the NPO-register. Therefore, the number of NPOs is not entirely clear, while the previous risk assessment estimated their number at 450 at most.

THREATS

The main threat from operations of companies working in the public interest regarding money laundering relates to organisations and voluntary associations, cf. the above discussion in the risk assessment. This stems from how simple and easy it is to launder money through their operations. However, there are no examples of misuse of this form of organisation to launder money in this country in recent years.

WEAKNESSES AND MITIGATING FACTORS

With the arrival of Act no. 119/2019, organisations operating across borders became subject to the obligation to register, while the registration of other NPOs is optional according to Act no. 110/2021 although it may be set as a condition for

a grant. The act sets forth, amongst other things, conditions for management of a company, minimum qualification requirements for directors, accounting, and annual financial statements. There has also been instruction for organisations operating across borders under Act no. 119/2019.

On the other hand, oversight of general organisations and NPOs working in the public interest, as well as surveillance and legal framework for their operations. There is no education on the operations of general associations and organisations, for example, on good management practices or instructions on finances and accounting. In fact, no other rules apply to the operations of such companies and organisations working in the public good, other than those they set for themselves as articles of association. However, one must consider that the percentage of the organisations working in the public interest, compared to the total number of general organisations and clubs, is low. Another mitigating factor is the duty to register BO of a general company or club. This is intended to detect and prevent money laundering, cf. the Act on the Registration of Beneficial Owners no. 82/2019.

RISK CLASSIFICATION

MEDIUM

Considering the above threats and weaknesses, after taking into account mitigating factors, it must be deemed that the risk that organisations having this purpose can be misused is medium.

5. TERRORIST FINANCING

Terrorism, by nature, is an offence deemed to be multiple crimes since either perpetrators or victims are a considerable number of people. Assessment of the risk from terrorist financing was done in cooperation with domestic law enforcement agencies, such as police authorities, tax and customs authorities and the FIU. Also, information was gathered from foreign sister agencies. The NCIP employs international collaboration with other law enforcement and security agencies that have the goal of preventing terrorist acts, investigating such acts, etc. Moreover, NCIP's National Security Unit has diverse information about terrorist operations. Since 2008, the unit has assessed and produced reports on the risk of terrorism.

GENERALLY ON THE RISK OF TERRORISM IN ICELAND

In Icelandic law, the provisions of Article 100 (a.-c.) of the GPC contain offences regarding terrorist acts. They involve punitive provisions on terrorism, terrorist financing, and abetting terrorist activities. Icelandic criminal law does not have a long tradition of penalty clauses on terrorism, for the above provisions went into force 31 May 2002 with Act no. 99/2002, cf. the previous discussion of the risk assessment regarding the reason that provisions on terrorism were legalised in this country.

A major factor in the battle against terrorism is the authorities' application of preventive measures of this kind, e.g. by disrupting or upsetting conduct possibly related to terrorism. There are also societal defences against such operations, e.g. strict legislation, collection, and registration of information on terrorist organisations and individuals related to terrorism, a robust and efficient monitoring system, cooperation with governments, and education on and strengthening of risk awareness regarding the issue category.

Under its role under Regulation on the National Security Unit of the National Commissioner of the Icelandic Police no. 404/2007 the unit assesses the risk

of terrorism in Iceland In a report from the NCIP, regarding an assessment of the threat of terrorism issued in February 2022, it was stated that the possibility of terrorism in Iceland cannot be eliminated and that it was hardly possible to prevent random attacks by individuals, although the likelihood of such attacks falling within the scope of the terrorism clause were deemed slight.¹³⁰

In September 2022, the police announced an investigation into alleged preparation of a terrorist offence in Iceland. A charge was filed for the case and the case is still before the courts. This is the first investigation and charge of terrorism in Iceland.

In December of 2022, a five-level scale was introduced to assess the risk of terrorism which is geared toward coordinating the use of risk levels in Iceland with that of neighboring countries. In Iceland, a four-level scale had been used until then and the risk level in Iceland had been assessed as level one of four. In December of 2022, the NCIP's National Security Unit announced that Iceland was at level three of five; additional threat, i.e. that there was intent and/or capability and possible organisation of terrorism.¹³¹

The assessment of terrorist financing in Iceland has until now drawn on the NCIP's assessment of the risk stemming from terrorism. Therefore, it may be assumed that the risk level of terrorism in this country can affect the risk assessment of terrorism. It may also be deemed likely that the solidarity displayed in this country with foreign groups which are located in conflict areas and have been defined as terrorist organizations can affect the risk assessment of terrorist financing.

RISK ASSESSMENT OF TERRORIST FINANCING

In parallel with assessing the risk of money laundering, an assessment was made of risk factors connected with terrorist financing. Even though there is no direct correlation between these two factors, they can have various things in common since the financing of terrorism can be the fruit of criminal activities, e.g. unlawful gains from the predicate offences of money laundering, such as drug offences and enrichment crimes. Also, both money laundering and terrorist financing can be connected with organised crime. Moreover, weaknesses connected with these two things can be the same or comparable.

Likewise, there are many differences between these two factors. Unlike what generally applies to money laundering, the sums regarding terrorist financing can be low, and the money used is obtained by any means whatsoever, lawful or unlawful. Also, terrorist financing can go on in a state other than the one planned as the site for terrorist acts, and it is therefore not possible to rate these two things as equal.

The NCIP's National Security Unit handles investigations of criminal cases related to terrorism under the provisions of the Regulation on the supervision

¹³⁰ *Terrorist threat in Iceland. Risk Assessment Report of the Department of Research and Analysis of the National Commissioner of the Icelandic Police.* National Commissioner of the Icelandic Police, Reykjavik 2022, pg. 8.

¹³¹ www.logreglan.is/vidbunadargeta-logreglu-aukin-timabundid/

of police investigations and cooperation of the district attorney and chief of police during the investigation of criminal cases no. 660/2017. For that reason, based on the AML Act, the unit receives FIU's analyses of notices of suspicious transactions on possible terrorist financing for processing. The above information was considered for the risk assessment, as well as the knowledge and know-how within the National Security Unit in addition to the above reports on terrorist threats.

In carrying out the risk assessment, known methods of terrorist financing, to which FATF has, amongst other things, called attention, were kept in mind. Examples include low contributions from private parties or companies to terrorist operations, the misuse of companies with no financial purpose and sending money to risky areas concerning terrorism, the use of profits from various criminal activities, or various kinds of intimidation, kidnapping, legal trade operations, and official contributions from a state. In addition, it is known that in transferring funds used for terrorist financing, methods are used like transfers from bank accounts, remittances, and transfer of cash between regions or countries.¹³²

The risk assessment also considered that Iceland is a homogeneous society with relatively few residents, where about 18% of them are of foreign origin.¹³³ The frequency of crime is low. The police are generally unarmed day-to-day, and Iceland has no military and no special ties to states regarded as risky concerning terrorism. As previously stated, the first charge for violations of the terrorist clause was filed in 2022 and it was for an alleged attempt to commit terrorism. No confirmed cases connected with terrorist financing have come up in the country. The same applies to support for such conduct terrorist offences.

The main premises for the evaluation of threat are as follows:

- The first investigation and charge for attempted terrorism in Iceland has appeared.
- It's possible that there are individuals in this country who subscribe to a violent and extreme ideology and develop the capability and intent to commit terrorism.
- There are no indications of terrorist groups operating in Iceland.
- There are no indications of Icelandic terrorist groups operating abroad.
- There is no confirmed information regarding a community of extreme religious or lifestyle groups having been formed in Iceland.
- There are no visible signs that leaders or influencers conduct or organise the indoctrination of extreme ideology or call for terrorism in Iceland.

¹³² FATF Report. *Emerging Terrorist Financing Risks*. FATF, Paris 2015.

¹³³ [Population in 2nd quarter 2023 – Statistics Iceland](#)

- There are no indications of the travels of foreign fighters from Iceland.
- Iceland is not deemed a target for terrorist organisations such as the Islamic State (ISIS) and Al-Qaeda, or for other violent extremist groups which support their cause.
- The number of received and sent requests based on international cooperation to share information regarding terrorist financing is very small.
- The percentage of reports to the FIU due to suspicious transactions related to terrorist financing is very low.

On the other hand, there are threats connected with possible terrorist financing. Those threats are known and are, furthermore, international threats that FATF and others have called attention to. They relate to the transfer of cash across borders, remittances to and from Iceland through the financial system and the operations of NPOs. These assessment factors will each be dealt with in the following sections.

In assessing risk, one must consider weaknesses, such as those regarding exposure to risk, risk awareness, the legal framework, and monitoring. Iceland's weaknesses in grappling with terrorist financing primarily regard discretionary legal powers to acquire information and data without offences having been committed, i.e. exercising preventive measures in the name of law enforcement, e.g. discretionary legal powers to acquire financial information from a third party. For example, the police have more stringent discretionary legal powers than FIU and DTI. However, it bears mentioning that there is a bill underway to amend the Act on the Police no. 90/1996, amongst other things, regarding crime prevention. Finally, it must be mentioned that although the general overview of associations' operations is better, amongst other things, for the obligation to register NPOs operating across borders, it is perhaps insufficient, given the number of associations, their divergent forms, and limited public monitoring of associations.

Regarding mitigating factors, the collaboration of authorities and institutions is very good and efficient in this area. Also, the work procedure is tightly constrained and documented, at both FIU and the police, regarding the processing of notices and clues regarding terrorist financing, as well as case investigations.

Risk assessment and risk assessment factors of terrorist financing consider this.

5.1.1. TRANSPORT OF CASH ACROSS BORDERS

RISK CLASSIFICATION



GENERAL

Transferring cash to and from the country can occur mainly in two ways. On one hand, an individual may transport assets across the border when leaving the country, e.g. in baggage or on his person. In this context, so-called 'money mules' are referred to. On the other hand, it's possible to send cash to or from the country without the sender accompanying the money, such as by mail or cargo service. Here, the transport of electronic money across borders, i.e. pre-paid cards, will be examined.

Ways in and out of the country take place by air or by ship. In Iceland, there are four international airports and about 70 ports, of which 10 accommodate cargo transport. Also, a passenger-ferry comes here regularly; Norræna. Finally, cash can be sent in shipments of mail or cargo. There has been much growth in the tourist industry in this country, discounting the period of the Covid-19 pandemic. The number of arriving and departing passengers, foreign and domestic, through international airports was about 2.2 million in the year 2021 and there has also been an increase in the number of arrivals of cruise ships.

There is an obligation to especially notify the customs authorities of money (cash or bearer bonds) which is transported to the country from abroad and abroad from the country in the amount of 10,000 euros or more. This applies whether the assets are transported to the country by plane, by ship or by shipment of mail or cargo.

THREATS

In the international context, there are known examples of terrorists transferring assets between areas, e.g. in travels from Europe to a third state. There are also known examples of 'aspiring' returning fighters transporting cash on their way from a homeland to a conflict area. No cases have come up where assets have been transported across borders for terrorist financing.

Transporting cash across borders is a known means to terrorist financing, as the amounts in question are often low. The cash amounts may even be under the limit amount one is obligated to report. For the sender, there is even less risk

in sending cash via mail or cargo shipments, for example with many shipments, each amount low. This is likely to make customs' monitoring difficult. Finally, there is the threat of the use of prepaid cards and their transport across borders, as prepaid cards are exempt from the duty to report.

WEAKNESSES AND MITIGATING FACTORS

The risk of the transport of cash across borders is related to the risk of high denomination banknotes, as by this method it's possible to transport high amounts of cash quickly and anonymously. This is to be considered in the context that access to foreign currency is good, and it is easy to exchange Icelandic krónur for it, cf. the discussion in the risk assessment on foreign exchange transactions. There are more stringent requirements of business men now regarding foreign exchange transactions than during the preparation of the previous risk assessment. Through the years it has proved difficult to maintain oversight and monitor individuals without ID numbers who present personal identification during foreign exchange transactions.

Surveillance of the transport of cash across borders during the arrival and departure of tourists has been enhanced related to a campaign, which involves more efficient surveillance from the standpoint of risk-based analysis, which also includes active surveillance of passengers who have reported that they are travelling with money. On the other hand, specialised surveillance of the transport of cash by mail shipments, express shipments, or cargo shipments is limited. Finally, it bears mentioning that the training of the Customs' dogs to search for money is still ongoing. Also, very few cases have arisen with customs in recent years where cash is being transported over the border in 2021 and 2022, although there has been an increase in the months already passed in 2023. No cases have arisen due to transport of cash by shipments of mail or cargo. Considering the number of cases which Customs has been responsible for investigating and information regarding surveillance, it may be concluded that surveillance of the transport of cash and other valuables to and from this country are deficient.

The legal framework regarding the duty to report the transport of cash also pertains to shipments of mail and cargo. On the other hand, the surveillance authorisations of Customs are lacking, as legal authority to search the checked baggage of departing passengers without the person being present, or being given the opportunity to be present, during the examination, is not in place. Also, one may deem that the deterrent value of penalties is limited and that there are more requirements for degrees of culpability in offences related to the import or export of cash than in the case of other customs violations.

As a mitigating factor, one may point to the geographical location of Iceland, far away from areas where the risk level of terrorism is deemed high. Risk

awareness has increased in this field, both within the administration and among parties subject to mandatory reporting, and the authorities have commissioned the publication of educational materials. However, reports to the FIU of suspicious transactions regarding terrorist financing are still very few.

RISK CLASSIFICATION

MEDIUM

Considering the threats and weaknesses, as well as mitigating factors, the risk of transport of cash across borders regarding terrorist financing is deemed medium.

5.1.2. TRANSPORT OF ASSETS TO AND FROM ICELAND THROUGH THE FINANCIAL SYSTEM

RISK CLASSIFICATION



GENERAL

Up for discussion here is the transport of assets across borders through the financial system, i.e. transfers of assets. Related to the risk of terrorist financing, additional risk is considered to be inherent in transfers to risky areas. The Icelandic banking system is to be examined here, i.e. financial institutions which are subject to mandatory reporting in this country.

In Iceland, access to banking services is good, cf. the discussion in the financial section of the risk assessment for money laundering. The Icelandic banks and payment service providers do not have branches abroad and the percentage of foreign customers is not very high. Also, banking business cannot be established unless the person in question has a domestic ID number. In the case of a foreign citizen who fails to meet the conditions for registration in Registers Iceland, the person in question must apply for an ID number for a foreign citizen with a public entity.

THREATS

In the international arena, there are known examples of the use of deposits and withdrawals of cash to finance terrorism. There are examples of terrorists, their relatives and friends placing lawful or ill-gotten funds into the financial system, that forged and stolen identification have been used to open bank accounts and that terrorists withdraw cash from ATMs located in conflict areas or their neighboring countries. Also, cash has been withdrawn from areas where the risk of terrorism isn't great in order to pay various expenses related to terrorist activity. No cases have come up where deposits or withdrawals of cash have been used for this purpose.

In Iceland, there is ready access to banking services. It's easy to start a bank account and transport cash between countries rapidly. This especially applies when the origin of assets is legitimate and, therefore, the opening of a bank account arouses no suspicions. This service is subject to risk exposure as misuse of it does not require great organisation or expertise. The main threat of terrorist financing involves often low amounts that may have the purpose of escaping notice.

WEAKNESSES AND MITIGATING FACTORS

With regard to weaknesses in this activity, the weaknesses covered in the chapter on deposits and payment services regarding money laundering also apply here, e.g. regarding weaknesses related to the risk classification of customers and regular monitoring of transactions. It's also important to note that new threats and opportunities may arise with new technology, e.g. with the use of automated tech solutions in initiating business relationships.

As a mitigating factor, one can mention that anonymous transactions are not permitted, and the legal framework seems adequate. Also, risk-based surveillance of the financial market is extensive. Finally, the four commercial banks do not have branches abroad and they have few foreign customers although the number of these is increasing

The risk awareness of parties subject to mandatory reporting is lacking when it comes to foreign payments. In addition, law enforcement authorities lack authorisations to gather information and data without an offence having been committed. Also, reports of suspicious transactions regarding terrorist financing are few and only one such report has been received by the FIU from a commercial bank during the last five years.

RISK CLASSIFICATION

MEDIUM

Considering the threats and weaknesses, as well as mitigating factors, the risk of terrorist financing from transport of assets across borders through the banking system is deemed medium.

5.1.3. TRANSPORT OF ASSETS TO AND FROM ICELAND BY MONEY REMITTANCES

RISK CLASSIFICATION



GENERAL

Assessment of the risk of terrorist financing from the transport of assets across borders by money remittances is covered here. The discussion of the assessment of the risk of money laundering in this operation applies here to a great degree.

Remittances are a service which involves handing funds over to a payment service provider who then forwards them to the recipient through another payment service provider. The recipient can then request the assets in cash, cf. clause 30, Paragraph 1 Article 3 of the Act on Payment Services no. 114/2021. Customers do not have to have accounts with the payment service provider to engage in these transactions. If transactions amount to 1000 euros or more, the parties are obligated to conduct due diligence of their customers in accordance with the AML Act. The supply of this service in this country has decreased and only one party handles this operation and that party is the commercial agent of a foreign paying agency. As the service has become less accessible, the use of these transactions has decreased. The percentage of foreign customers is low and in a few instances they are from risky or uncooperative states. No information is available of remittance services being operated without a licence, also known as Hawala.

THREATS

In many places abroad, the risk from money remittances has been assessed as very high, as there are known examples of this service being used to transport money for terrorist financing. In conflict areas, where there is limited access to banking services and terrorist organisations operate, money remittances are often the financial services used to transport assets.¹³⁴

One is able to move cash between countries rapidly by money remittances. Anonymous transactions are not permitted, but one can avoid disclosing the beneficial owner of finances by using forged or stolen identification or by using straw men. Due diligence surveys can also be avoided by transferring low amounts, which is common in the case of terrorist financing. Also, frequent use

¹³⁴ FATF Report. *Terrorist Financing Risk Assessment Guidance*. FATF, Paris 2019.

of cash and the occasionally informal structure of such services often creates an additional threat of terrorist financing. The percentage of foreign customers with the only entity engaging in money remittances in this country is low and in a few instances they are from risky or uncooperative states.

No cases have come up in this country where assets have been transported from Iceland by remittances for terrorist financing.

WEAKNESSES AND MITIGATING FACTORS

In this country, money remittances are conducted by the commercial agent of a foreign paying agency. This, in and of itself, entails considerable risk, not least because it is generally difficult for paying agencies employing agents to control and monitor them. Money remittance services are conducted alongside other, different services, e.g. postal services, and there are weaknesses regarding the implementation of a risk-based approach. Business relationships are usually not for the long-term, limited due diligence is conducted and, therefore, the likelihood of the use of forged or stolen identification is increased. The service is based on cash transactions, which involves a certain degree of risk. Misuse does not require specialised knowledge or organisation.

As a mitigating factor, one might mention that access to this service has decreased with a reduction in the number of commercial agents. One might also note that the legal framework and monitoring of money remittances is in good standing, and that the authorities are well aware of the threats from the operation. Risk awareness has also increased in this field, both within the administration and among parties subject to mandatory reporting, and the authorities have commissioned the publication of educational materials. Few notices have reached the FIU of suspicions of terrorist financing, but a majority of those received comes from the service providers of money remittances. Nevertheless, risk awareness within the operation is limited.

RISK CLASSIFICATION

MEDIUM

Considering the threats and weaknesses, as well as mitigating factors, the risk of terrorist financing from the transport of assets across borders by money remittances is deemed medium.

5.1.4. TERRORIST FINANCING, OPERATION OF NON-PROFIT ORGANISATIONS ACROSS BORDERS

RISK CLASSIFICATION



GENERAL

The preparation of the risk assessment included a special examination of NPOs with operations across borders. The main reason why such organisations are considered is that there are examples within the states of the FATF of organisations without a financial purpose, working in the public interest, being misused, particularly for terrorist financing purposes.¹³⁵ In preparing the risk assessment, FATF's definition of NPOs was kept in mind. The task force defines such organisations 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"."¹³⁶ On this basis, the discussion was limited to registered NPOs who operate across borders, religious and lifestyle associations, associations and funds that operate under a certified charter.

With regard to organisations considered general organisations and NPOs operating across borders the Act on the obligation of non profit organisations who operate across borders to register no. 119/2019. The act entered into force on 11 October 2019 but until that time the obligation to register was not in place with regard to this company form. At the end of the year 2022, registered organisations numbered 47. Requirements of the company form in question are reasonable, considering their number. The act sets forth, amongst other things, conditions for management of a company, accounting and annual financial statements and minimum qualification requirements for directors. The scope of these organisations is not great in terms of financial activity. According to Paragraph 2 of Article 38 of the AML Act., cf. the act amending Act no. 96/2020, the Money Laundering Division of the Directorate of Internal Revenue monitors such companies.

Religious and lifestyle companies work in the public interest and are NPOs according to the definition of the FATF. They operate under Act on Registered Religious and Lifestyle Associations no. 108/1999 and the regulation on the registration of such associations no. 106/2014. The act provides for people's right to found religious associations and practice their religion in accordance with their convictions. The legal framework of the company form is such that the director of the organisation must pay church-taxes

¹³⁵ FATF Report. *Risk of Terrorist Abuse in Non-Profit Organisations*. FATF, Paris 2014. pg. 36–48.

¹³⁶ *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations*. FATF, Paris 2023. pg. 63.

in this country, which means that they must be taxable in this country and, therefore, reside here for most of the year. There are no such requirements for the directors of the organisations, they can reside in other states, even without having any connection with Iceland. There are examples of Icelandic religious and lifestyle associations being involved in international operations, especially related to the Nordic countries, and of the directors of organisations residing abroad. To that extent, the operation of such organisations can reach across borders.

Public surveillance of this company form is the responsibility of the District Commissioner of North East Iceland and mostly pertains to the disposition of the funds going into such associations in the form of congregational fees and the status of the directors. The district commissioner can also deregister an organisation if it no longer fulfils the conditions for registration or neglects its statutory duties, the district commissioner can cancel its registration after a preceding warning and deadline for rectification. There were 51 registered religious and lifestyle organisations at the end of the year 2022. Of these, 44 were religious organisations, and seven were lifestyle associations. In 2022, about ISK 3.1 billion in congregational fees was paid from the State Treasury, of which just over ISK 700 billion went to congregations outside the State Church in this country.¹³⁷

Finally, funds and associations operating under a certified charter may, according to Act no. 19/1988 and Regulation no. 140/2008 belong to the category of NPOs according to the definition of the FATF. This involves funds and associations falling under the heading of self-governing foundations with no financial purpose that operate under a certified charter. Upon founding, money is paid into the fund or association by gifting, a will, or another private law instrument. These funds are intended to be utilised for one or more goals. The charter shall specify the initialisation funding, its source, what the goals of the fund or association are, and how the funds shall be spent to achieve those goals. Also, the appointment of the board and trustee shall be divulged.

Public surveillance of this operation is the responsibility of the District Commissioner of North West Iceland. In addition, the National Audit Office monitors submissions of accounts for this company form and no later than 30 June each year, the party responsible for a fund or association shall send the Icelandic National Audit Office the fund's or association's accounts for the previous year along with a report on the disposition of funds that year. The number is significant; there were 684 active funds and associations at the end of the year 2022. Of these, 58% had submitted their annual financial statement in December 2022 for the year 2021. The amount of income of funds and associations varies and so do their assets. These are significant amounts after income and assets have been assessed in their entirety, as the sums amount to billions of krónur. With regard to the operation of funds and associations across borders, the aim of some self-governing institutions is to contribute to humanitarian activity outside Iceland. There are also examples of the board members of this company form being foreign citizens.

¹³⁷ *Parochial dues 2022. Financial Management Authority, Reykjavík 2023, pg. 2.*

THREATS

A distinction must be made between, on the one hand, the threat of the operations of NPOs expressly founded and/or run for terrorist financing purposes and, on the other hand, the misuse of NPOs which participate in transferring funds to and from conflict areas where defences against terrorist financing are weak. Also, organisations considered NPOs are of different types and some of them pose a greater threat than others. For instance, NPOs working on humanitarian causes often operate in areas where the risk of terrorism is deemed very high or where there are militant units and/or terrorist groups.

The operation of NPOs in this country in risky areas is negligible. Moreover, there are no indications of terrorist financing through NPOs in this country or connections of such organisations with such conduct abroad. The main threats stemming from the operation of NPOs are to be examined considering that.

WEAKNESSES AND MITIGATING FACTORS

The main weaknesses of NPOs which may operate across borders are that they often belong to different company forms where different laws apply. This complicates oversight somewhat as there is not an unequivocal obligation for NPOs operating across borders to register. Also, public surveillance of the operations of NPOs is in place but it is not all handled by the same entities. In fact, four different authorities are responsible for it. Finally, the legal framework of both religious and lifestyle associations and funds and associations operating under a certified charter are past their prime and require revision, amongst other things, considering the threat of terrorist financing. It bears mentioning, however, that plans are afoot for amendments to laws regarding registered religious and lifestyle associations and the Act respecting Foundations Engaging in Business Operations Under a Certified Charter. The aim of the amendments is to respond to discussions in the last issue of the risk assessment.

As a mitigating factor, one might mention increased risk awareness, amongst other things with the publication of educational materials. Also, the lack of formality which seems to have been a characteristic of the operation of NPOs operating across borders has been addressed with legislation on the operation, cf. Act no. 119/2019.

RISK CLASSIFICATION

LOW

Considering the threats and weaknesses, the risk of terrorist financing from the operation of NPOs operating across borders is deemed low.

6. LIST OF THE MOST IMPORTANT ABBREVIATIONS

EEA	European Economic Area
EFTA	European Free Trade Association
EU	the European Union
FATF	Financial Action Task Force
GPC	General Penal Code 19/1940
HRD.	Supreme Court Ruling
LRD.	Land's Court Ruling
AML ACT.	Act on Measures against Money Laundering and Terrorist Financing no. 140/2018
NCIP	National Commissioner of the Icelandic Police
FIU	Financial intelligence unit
CBI	Central Bank of Iceland
DTI	the Director of Tax Investigations
UN	the United Nations

7. SOURCES

- Action plan 2021-2023 - Measures against money laundering and terrorist financing:* Steering Committee of the Minister of Justice on measures against money laundering and terrorist financing, Reykjavík 2021.
- Basel AML Index 2022: 11th Public Edition - Ranking money laundering and terrorist financing risk around the world.* Basel Institute on Governance, Basel 2022.
- Den nationale risikovurdering af hvidvask. Hvidvasksekretariatet 2022.* Danmarks finansielle efterretningsenhed (FIU,) Kaupmannahöfn 2023.
- Estimating Illicit Financial Flows Resulting from Drug Trafficking and other Transnational Organized Crimes - Research Report.* United Nations Office on Drugs and Crime, Vienna 2011.
- EU Serious and Organised Crime Threat Assessment (SOCTA) 2021 - A Corrupting Influence: The Infiltration and Undermining of Europe's Economy and Society by Organised Crime.* Europol, Luxembourg 2021.
- European Financial and Economic Crime Threat Assessment 2023 – The Other Side of the Coin: An Analysis of Financial and Economic Crime.* Europol, Luxembourg 2023.
- FATF Guidance. National Money Laundering and Terrorist Financing Risk Assessment.* FATF, Paris 2013.
- FATF Report. Emerging Terrorist Financing Risks.* FATF, Paris 2015.
- FATF Report. Money Laundering Through the Physical Transportation of Cash.* FATF, Paris 2015.
- FATF Report. Risk of Terrorist Abuse in Non-Profit Organisations.* FATF, Paris 2014.
- FATF Report. Terrorist Financing Risk Assessment Guidance.* FATF, Paris 2019.
- Financial infrastructure.* CBI, Reykjavík, Volume 7, 24 June 2019.
- Financial Stability, 2022(1).* CBI, Reykjavík, Volume 30. 16 March 2022.
- Financial Stability, 2022(2.)* CBI, Reykjavík, Volume 31. 28 September 2022.
- Financial Stability, 2023(2).* CBI, Reykjavík, Volume 33. 20 September 2023.
- Execution of risk assessment relating to money laundering and terrorist financing. Academic report. First edition.* CBI, Reykjavík 2022.
- Global Gender Gap Report 2023 - Insight report.* World Economic Forum, Colongny/Geneva 2023.

- Global Peace Index 2023: Measuring Peace in a Complex World*. Institute for Economics & Peace, Sydney 2023.
- Terrorist Threat in Iceland. Risk Assessment Report of the Department of Research and Analysis of the National Commissioner of the Icelandic Police*. National Commissioner of the Icelandic Police, Reykjavík 2022.
- Collection of court fines – Administrative Profile*. National Audit Office, Reykjavík 2022.
- International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. The FATF Recommendations. FATF, Paris 2023.
- Jónatan Þórmundsson: Episodes of Crimes of Enrichment. Special part*. Reykjavík 2009.
- Guidelines with the questionnaire of the Central Bank of Iceland regarding risk assessment of measures against money laundering and terrorist financing*. CBI, Reykjavík 2023.
- Mutual Evaluation Report of Iceland*. FATF, Paris 2018.
- Neobanker – En rapport om neobanker och deras risker relaterade till penningtvätt och finansiering av terrorism*. Polismyndigheten, Stockholm 2022.
- OSCE Handbook on Data Collection in Support of Money Laundering and Terrorism Financing, National Risk Assessments*. Organization for Security and Co-operation in Europe, Vienna 2012.
- Money Affairs, 2023(3)*. CBI, Reykjavík, Volume 93. 23 August 2023.
- Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing*. COM(2021)/420. EU, Brussels, 2021.
- Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, Second edition and supplement on special recommendation IX*. The World Bank, Washington 2006.
- Judicial improvements in the field of lotteries - reports and proposals*. Chairman of a task force which was meant to investigate possible judicial improvements in the field of lotteries, Reykjavík 2022.
- State Accounts 2022*. The Ministry of Finance and Economic Affairs, Financial Management Authority, Reykjavík 2023.
- Self-governing institutions and funds that operate under an approved charter for the 2021 operating year*. Excerpt from the annual accounts. National Audit Office, Reykjavík 2023.
- Organised Criminal Activity 2021. Assessment of the Department of Research and Analysis of the National Commissioner of the Icelandic Police*. National Commissioner of the Icelandic Police, Reykjavík 2011.
- Organised criminal activity in Iceland. Risk Assessment Report of the Department of Research and Analysis of the National Commissioner of the Icelandic Police*. National Commissioner of the Icelandic Police, Reykjavík 2019.

- Report of the Minister of Justice and the Minister of Finance and Economic Affairs on what led to Iceland ending up on FATF's "grey list."* Ministry Offices, Reykjavík 2019.
- Report of the task force of the Ministry of Social Affairs and Children against social underbidding and illegitimate operations in the labour market.* Ministry of Social Affairs, Reykjavík 2019.
- Parochial dues 2022.* Financial Management Authority, Reykjavík 2023.
- Supra-National Risk Assessment Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.* SWD(2019)/650. EU, Brussels, 2019.
- Supra-National Risk Assessment Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.* SWD(2022)/554. EU, Brussels, 2022.
- Technical Assistance Report – Nordic Baltic Technical Assistance project: Financial Flows Analysis, AML/CFT Supervision, and Financial Stability.* IMF Country report no. 23/320. International Monetary Fund, Washington 2023.
- Committee proposals for the investigation and prosecution of tax law violations.* Reykjavík, 2019.
- Proposals and summary of the representatives of lottery companies in a task force regarding judicial improvements in the field of lottery affairs to the Minister of Justice regarding amendments to jurisprudence regarding lotteries.* Reykjavík 2022.
- Opportunity and risk in the field of digital financial services based on a distributed transaction register. Report of task force.* The Prime Ministry, Reykjavík 2023.
- Scope of tax evasion and proposals for actions. Report of task force.* The Ministry of Finance and Economic Affairs, Reykjavík, 2017.
- Issuance of Bogus Invoices - The Nature of the Behaviour and Possible Scope - Proposals for Actions.* The Ministry of Finance and Economic Affairs, Reykjavík 2023.
- Website of The World Bank, data.worldbank.org
- Website of International Monetary Fund, www.imf.org
- Website of the Icelandic Parliament, www.althingi.is
- Website of the European Banking Authority www.eba.europa.eu
- Website of the European Union, commission.europa.eu
- Website of the Icelandic Tourist Board, www.ferdamalastofa.is
- Website of Forbes Advisor, www.forbes.com/advisor/
- Website of Statista, www.statista.com
- Website of Statistics Iceland, www.hagstofa.is
- Website of the National Association of Pension Funds, www.lifeyrismal.is
- Website of the police, www.logreglan.is

Website of the commercial research institute, Veltan, www.veltan.is

Website of Reuters, www.reuters.com

Website of the State Prosecutor, www.rikissaksoknari.is

Website of UN Human Development Reports hdr.undp.org

Website of The Confederation of Icelandic Employers, www.sa.is

Website of Fisheries Iceland, www.sfs.is

Website of the Icelandic Association of Local Authorities, www.samband.is

Website of the Consultation Portal, www.samradsgatt.island.is

Website of Iceland Revenue, www.skatturinn.is

Website of Digital Iceland, www.islandi.is

Website of the Government Offices of Iceland, www.stjornarradid.is

Website of Transparency International, www.transparency.org

Website of The Guardian, www.theguardian.com

Website www.neobanks.app

Websites of the House and Construction Institution, www.hms.is and www.fasteignaskra.is

Websites of the Organisation for Economic Co-operation and Development (OECD), stats.oecd.org and www.oecdbetterlifeindex.org

Websites of the Central Bank of Iceland, www.sedlabanki.is and www.fme.is

8. APPENDIX

RISK CLASSIFICATION OF ASSESSMENT FACTORS – COMPARISON

The conclusions of risk classification of the assessment factors examined during the preparation of the risk assessment can be seen in the summary below, compared with the conclusions of the risk classification of risk assessments from the years 2019 and 2021, which were based on the same methodology.

LOW	MEDIUM	HIGH	VERY HIGH
------------	---------------	-------------	------------------

Money laundering predicate offences	2019	2021	2023
Tax fraud as predicate offence of money laundering			
Cash and crypto-assets			
Cash - transport to and from Iceland			
Cash transactions			
Cash in circulation, large bills			
Crypto-assets (not assessed in 2019 and 2021)			
Financial market			
Deposit operations			
Loan operations			
Payment services			
Remittances.			
Foreign exchange with cash (not assessed in 2019)			
Issue of electronic money			
Business and services with crypto-assets (was called cryptocurrency in 2019 and 2021)			
Trade and services for financial instruments			
Operation of funds			
Operation of pension funds (was called pension funds in 2019 and 2021)			
Life insurance activity			
Digital financial services monitored by other states (not assessed in 2019 and 2021)			
Specialists			
Attorneys			
Accountants			

	2019	2021	2023
Bookkeepers (not assessed in 2019)			
Estate agents and real estate transactions (was called Estate agents in 2019 and 2021)			
Ship brokers			
Car dealerships, car dealers and vehicle transactions (not assessed in 2019)			
Jewellers and gold-buyers, precious metals and gems (was called Precious metals and gems in 2019 and 2021)			
Art dealers and art brokers, art objects market (not assessed in 2019 and 2021)			
Gambling			
Lotto			
Lottery			
Sweepstakes (was called betting in 2019)			
Gaming machines – slot machines and lottery machines			
Gambling on the internet – foreign operators (only domestic parties assessed in 2019 and 2021)			
Bingo (not assessed in 2021 and 2023)			
Operation of companies			
Private limited companies			
Limited liability companies, limited partnerships and self-governing institutions			
Other companies with a financial purpose (was called Other companies in 2019 and 2021)			
Non-governmental companies and organisations (not assessed in 2019)			
Religious and lifestyle associations			
Funds and associations operating under a certified charter			
Other non-profit organisations			
Beneficial owners (only discussed but not risk assessed in 2023)			
Retail Operations and Services and Others			
ID numbers for foreign citizens (only discussed but not risk assessed in 2023)			
Products and services (part of Cash Transactions and Private Limited Companies in 2023)			
Lifting of capital controls (not assessed in 2021 and 2023)			
Increase in the number of tourists (only discussed in 2021 and 2023)			
Terrorist financing (only discussed in 2019)			
Transport of cash across borders			
Transport of assets to and from Iceland through the financial system			
Transport of assets to and from Iceland by money remittances			
Non-profit organisations operating across borders			
Transport of assets out of the country (not an assessment factor 2023)			

