2021

National Risk Assessment of Money Laundering and Terrorist Financing

National Commissioner of the Icelandic Police
March 2021

Table of Contents

Preface

The risk assessment of money laundering and terrorist financing for Iceland published here is the third one issued. The first risk assessment for Iceland was published in 2017 and the second in 2019. This risk assessment entails a re-examination and update of the risk assessment in 2019 published that year in April.

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. FATF has issued recommendations on the measures member states shall take in response to the threat stemming from money laundering and terrorist financing. FATF's 40 recommendations have become global guidelines. Among other things, the European Union's directives have been in accordance with these guidelines.[1] By joining FATF, Iceland obligated itself to coordinate its legislation with the action group's recommendations.

FATF's evaluation of Iceland's defences against money laundering and terrorist financing in 2017-2018 revealed various weaknesses in the Icelandic legislation regarding this. Subsequently, Iceland began working on its response. Among other things, it entailed legalising 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. Art. 4 of Act no. 140/2018 on Measures against Money Laundering and Terrorist Financing (AML Act) legalised Iceland's duty to draft a risk assessment for the country. 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. Iceland immediately began working to get 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" and the reasons for this.[3] At its annual meeting in June 2020, FATF declared that Iceland had satisfactorily completed measures and reforms regarding its defences against money laundering and terrorist financing. Following this, the parties arranged for FATF to visit the country to confirm this and ensure that there would be the required political will to maintain these results in the future. This involved FATF's “on-site visit”. The global coronavirus pandemic limited travel options considerably, and the on-site visit had to be postponed for the summer of 2020. The on-site visit went on at the end of September the same year, and in October FATF's annual meeting decided that Iceland's name would be

[1] *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.* FATF, Paris 2020.

[2] *Mutual Evaluation Report of Iceland*. FATF, Paris 2018.

[3] *Skýrsla dómsmálaráðherra og fjármála- og efnahags-ráðherra um aðdraganda og ástæður þess að Ísland hafnaði á „gráa lista“ FATF (Report of the Minister of Justice and the Minister of Finance and Economic Affairs on the lead-up to and reasons that Iceland ended up on FATF's "grey list").* Iceland's Government Offices, Reykjavik 2019.

taken off FATF's “grey list”.

The 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. Among 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 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. In presenting statistical information, figures were generally from 2019 and 2020.

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 generally preventing risk.

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

1 Introduction

1.1 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 to its project list.

The main policy of FATF's role and purview is threefold. First, to work out standards for the member states' measures against money laundering and terrorist financing. Second, to assess the measures of individual states to introduce these standards, and third, to investigate and learn to recognise the measures of those engaging in money laundering and terrorist financing. Based on this, FATF has worked out recommendations to its member states on anti-money laundering and anti-terrorist financing measures.

FATF evaluates each member state's legislation, rules and efficiency and publishes reports on their measures. Depending on relevance, the organisation's member states have agreed to pressure one another by putting individual states on a special list of "uncooperative states" if they do not fulfil the requirements the organisation sets. Such pressure can also entail setting stricter requirements for these states, or parties living there, regarding financial instruments or the publication of warnings about transactions with parties in those states possibly entailing a risk of money laundering.

Legal environment

Act no. 64/2006 on Measures against Money Laundering and Terrorist Financing legalised the third Directive 2005/60/EC of the European Parliament and of the Council. 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. 2001/97/308/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 Iceland with Act no. 140/2018 on Measures against Money Laundering and Terrorist Financing 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.

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 Art. 1 of 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 covers parties required to give notice 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 obliged entities 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 Art. 264 of the General Penal Code (GPC) no. 19/1940 defines money laundering as punishable.

Under par. 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 par. 2 of the provision, someone who has committed a predicate offence and also commits an offence under par. 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.

The wording of the provision, as amended in 2009, looked to Art. 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 Act on Measures against Money Laundering and Terrorist Financing takes note of the definition of the concept in Art. 264 of 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 Act on Measures against Money Laundering and Terrorist Financing, 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 Art. 100 (a.-c.) of GPC. Under Art. 100 (a) of GPC, the punishment for terrorism shall be up to life imprisonment for someone committing one or two 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.

Art. 100 (b) of 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. Art. 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 Art. 100 (a) or (b) of 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, Art. 69 of 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 judgement of the Landsréttur Appeal Court on 29 January 2020 in Case no. 19/2019 and the judgement of the Supreme Court of Iceland 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 and the International Sanctions Implementation Act no. 93/2008. 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 Freezing of Funds and the Designation of Entities on a Sanctions List in relation to Terrorism Financing and the Proliferation of Weapons of Mass Destruction no. 64/2019 (Freezing Act). It prescribes the freezing of assets in line with specified sanctions to hinder terrorist financing and the scope and financing of weapons of mass destruction. Finally, the third is Act No. 119/2019 on the Obligation of Non-profit Organisations to Register. It applies to all non-profit organisations (NPOs) established for the purpose of raising or disbursing funds for the public benefit that operate across borders.

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 Act on Measures against Money Laundering and Terrorist Financing 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. See Figure 1.

Ministry of Justice (MoJ): Supervises the issue category and appoints a steering committee on measures against money laundering and terrorist financing.

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.

The Central Bank of Iceland's Financial Supervisory Authority (FSA): Monitors that the parties specified in par. 1 (a.-k.) of Art. 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 (IRC): The agency that the Commissioner of Revenue and Customs operates, following the amendment of various acts with Act no. 141/2019, 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 (IRC's Money Laundering Division), which monitors whether the parties specified in sub-paragraphs l-u of Art. 2 (1) of AML Act

follow the act's provisions. This involves, for example, accounting firms, law firms, estate agencies, and car agencies. Also, IRC's Money Laundering Division monitors NPOs regarding money laundering and terrorist financing under Act No. 119/2019 on the Obligation of Non-profit Organisations to Register. Finally, IRC 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 Commissioner of 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 Commissioner Revenue and Customs.

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 offences under Art. 100 (a.-c.) of GPC and sees to investigating and prosecuting serious offences under the provisions of Art. 264 of the same act.

Law Enforcement Agencies (LEAs): 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.
Directorate of Tax Investigations (DTI) Responsible for investigations under the Income Tax Act no. 90/2003 and acts on other taxes and fees levied by IRC or that the office is entrusted to implement.

National Commissioner of the Icelandic Police (NCIP): Based on Police Act, no. 90/1996, *NCIP* handles police matters on behalf of the minister. Responsible for preparing national risk assessment under the Act on Measures against Money Laundering and Terrorist Financing and seeing to investigations related to terrorism, including the financing of terrorism.

Ministry of Foreign Affairs (MoFA): Among other things, responsible for the execution of Act no. 93/2008 on Carrying out International Restrictive Measures and the Freezing Act no. 64/2019.

Ministry of Industry and Innovation (MoII): Responsible for supervision. Matters of IRC's Registration Division are under the ministry. Also responsible for the implementation of the Act no. 82/2019 on the Registration of Beneficial Owners and Act No. 119/2019 on the Obligation of Non-profit Organisations to Register.

The Ministry of Finance and Economic Affairs (MoFE): Responsible for supervision. Among other things, the FSA's matters fall under the ministry.

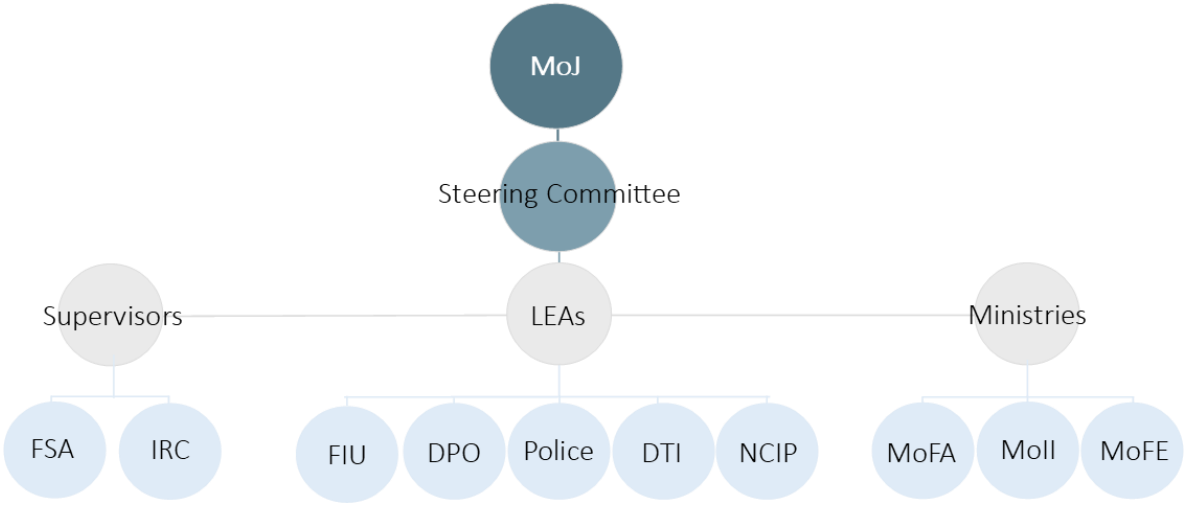


Figure 1. Government parties and other authorities involved in measures against money laundering and terrorist financing.

1.2 On predicate offences of money laundering

Predicate offences of money laundering mean offences resulting in unlawful gains that are later the object of money laundering. Below is a general discussion 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.[5] Despite 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, drug offences, and document violations.

Information from the police was gathered on the most common predicate offences (see Table 1). Furthermore, the most common predicate offences where money laundering was investigated in parallel were examined. For this purpose, statistical information from NCIP's police system (*LÖKE*) was utilised.

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, illegal, and secret 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.[6] NCIP's National Security Unit has called attention to increase in these kinds of offences in reports on organised criminal activities. The report in 2019 states: *"Mobile organised criminal groups from Eastern Europe have repeatedly come to the country in recent years for the sole purpose of committing organised burglaries and theft. Police suspect that these groups benefit, in at least some instances, from the guidance of assistants residing here in the country."*[7]

Drug offences entail the production, import, sale and distribution, custody, and handling of narcotics. Offences related to narcotics are amongst the most common predicate offences of money laundering. They can be offences against either special penal laws, cf. the Narcotics Act no. 65/1974, or the General Penal

Table 1. Main predicate offences of money laundering (ML)

Types of offences	2018		2019		2020*	
	Total number of offences	Number of offences along with ML	Total number of offences	Number of offences along with ML	Total number of offences	Number of offences along with ML
Theft	4571	51	4637	61	4638	34
Drug offences	483	21	473	37	299	39
Fraud	537	9	596	29	698	23
Embezzlement	65	8	81	22	82	27
Document violations	270	7	328	9	207	5
Total	**5926**	**96**	**6115**	**158**	**5924**	**128**

**Interim figures for 2020.*

[5] www.oecdbetterlifeindex.org/topics/safety/.

[6] Jónatan Thórmundsson: *Þættir um auðgunarbrot. Sérstakur hluti (Series on Crimes of Enrichment. Special Part)*. Reykjavik 2009, p. 66.

[7] *Skipulögð brotastarfsemi á Íslandi. Áhættumatsskýrsla greiningardeildar ríkislögreglustjóra (Organised Criminal Operations in Iceland. Risk Assessment Report of the National Security Unit of the National Commissioner of the Icelandic Police)*. National Commissioner of the Icelandic Police, Reykjavik 2019, p. 18.

Code if the offences are major, cf. Art. 173 GPC. 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 2019 regarding activities that are linked with narcotics states: *"The assessment of the police is that organised groups of criminals are operating in this country. Some of them have considerable strength and financial resources. As these groups grow in strength, it becomes more difficult for police to fight against their operations. It is getting easier for them to cover their tracks, and financial strength enables them to buy expertise and conceal the profits of their activities in legal operations. Such money laundering can directly affect markets, e.g., because of the better competitiveness that unlawful gain ensures."*[8]

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. Art. 248 GPC. The commonest fraud cases in Iceland entail utilising a specified service or purchasing a product without paying for it, e.g., by not paying for taxies or not paying for food in a restaurant. Such conduct does not entail direct unlawful gain that is later laundered. 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.

Embezzlement falls under enrichment crimes, cf. Art. 247 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.[9] 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. Art. 249 GPC.

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, i.e., 221 cases in 2018, 255 in 2019, and 178 cases in 2020. A number of these cases are traceable to forged identity papers, resulting from both document alteration and document forging from scratch. This mainly involves foreign parties coming to Iceland on forged identity papers or using them to obtain an ID number for foreign persons.

The number of cases regarding money laundering has increased greatly in recent years. Altogether, money laundering was investigated in 250 cases in 2020, compared to 16 cases in 2017. This increase has resulted from not only more offences being committed but also the police's greater emphasis on this category of cases. It has become more common to investigate money laundering with predicate offences. In 2018, money laundering was investigated in 96 cases in parallel with the main predicate offences of money laundering. In 2019 the number of cases was 158, and in 2020, there were 128. Finally, in the period 2018-2020, courts tried dozens of cases involving money laundering.

1.3 COVID-19

The COVID-19 pandemic has greatly disrupted society and the operations of important infrastructures. It has called for heavy restrictions on people's movement across borders. The spread of the coronavirus occurred with very little lead-up and has had extensive economic and social effects. The virus appeared in late 2019 and spread relatively quickly throughout the world in 2020. In April 2020, most states had resorted to strict quarantine measures and had substantially limited traffic across their borders.

[8] *Skipulögð brotastarfsemi á Íslandi. Áhættumatsskýrsla greiningardeildar ríkislögreglustjóra, p.* 24.

[9] Jónatan Thórmundsson: *Þættir um auðgunarbrot. Sérstakur hluti*. Reykjavik 2009, p. 151.

The pandemic has already caused the greatest economic global contraction in an entire century, and no one knows how long it will last. Besides the number of people unemployed and the reduced quality of life, it is uncertain what the long-term effects of this disturbance to daily life will have on people's health and well-being.

Responders in the country immediately began systematic collaboration in accordance with response plans in January 2020. The first confirmed COVID-19 infection in Iceland was diagnosed on 28 February 2020. The Icelandic Government resorted to extensive quarantine measures to restrict the outspread of the virus and reduce the load on the healthcare system, however, with the aim of disturbing the public's daily life as little as possible. Here, it is worth mentioning the restrictions on or closings of business operations, the general restrictions on the numbers of people and distancing restrictions, and instructions on hygiene and use of masks. Measures like extensive scanning, infection tracing, quarantining, and isolation were also taken. Likewise, harsh quarantine measures were taken at the border, and these measures, as well as the pandemic in general, have had enormous impact on the tourism industry.

Vaccination against COVID-19 started in Iceland on 29 December 2020. It can be said that this marked a definite milestone in the battle against the virus. The goal of vaccination is to build up herd immunity that hinders the outspread of the pandemic. If the Government's assumptions materialise, vaccination against COVID-19 in Iceland will be finished about the middle of next summer. Whether that milestone will be achieved in the country at that time or later, it is uncertain when the economy will revive. It is also clear that traditional life will not resume in the country until vaccinations worldwide are well along.

Effect of COVID-19 on the economy and business community

The COVID-19 global pandemic has already greatly damaged the Icelandic economy. Inflation has increased, and the krona exchange rate has weakened. In the last quarter of 2020, inflation was on average 3.6%, and in January 2021, inflation was 4.3%. However, there are signs that the effect of the exchange rate lowering on inflation has begun to decrease, and that inflation will decrease fast in the near future. The Gross Domestic Product (GDP) has likewise contracted, and unemployment has increased. Over the entire year, the GDP has contracted an estimated 6.6% in real terms. To a large extent, this may be attributed to the coronavirus pandemic. Finally, unemployment has increased. In December 2020, recorded unemployment was about 11%, which is an increase of about 6.4 percentage points over the same period the year before.[10]

The pandemic has had an enormous effect on tourism and the industries connected to it. Tourism's estimated share of the gross national product was 3.5% in 2020, compared to 8.0% in 2019.[11] In 2020, the number of tourists in Iceland contracted considerably. The total number of tourists arriving in the country on flights was less than half a million, compared to more than 2 million the year before. This is a decrease of more than 75% from the year before. Also, the number of passengers on luxury liners decreased by 99.6% from 2019, and only 2300 such passengers came to the country in 2020, compared to 500,000 the year before.[12] Likewise, the number of flights contracted substantially in the period. From November 2019 to October 2020, the total number of take-offs and landings was more than 50,000. This is a decrease of about 41%, compared to the same period in 2018-2019.[13]

It is also worth mentioning that the number of bankrupt companies that operated throughout their last fiscal year before going bankrupt increased by 9%. In 2020, there were 380 companies with such activity that went bankrupt, compared to 350 companies the year before. Of these companies, 92 were typical tourism services (48% increase).[14]

The Icelandic Government has assisted companies and individuals to withstand shocks from COVID-19

[10] *Peningamál (Monetary Affairs)*. Central Bank of Iceland, Reykjavik, 83rd monograph, 3 February 2021, p. 6 and www.hagstofa.is/utgafur/frettasafn/thjodhagsreikningar/thjodhagsreikningar-2020-aaetlun/.

[11] www.hagstofa.is/utgafur/frettasafn/frettasafn/thjodhagsreikningar/thjodhagsreikningar-2020-aaetlun/.

[12] www.ferdamalastofa.is/is/um-ferdamalastofu/frettir/category/1/heildarfjoldi-erlendra-ferdamanna-arid-2020.

[13] www.hagstofa.is/utgafur/frettasafn/ferdathjonusta/skammtimahagvisar-ferdathjonustu-i-november-2020/.

[14] www.hagstofa.is/utgafur/tilraunatolfraedi/gjaldthrot-og-virkni-fyrirtaekja-tt/.

and keep many people from becoming unemployed. The Government's responses have included:[15]

- The Central Bank lowered interest rates, increased access of domestic finance companies to capital, employed foreign exchange reserves to dampen exchange rate fluctuations and started buying state bonds.
- The Government has provided financial assistance to companies that have had to restrict or suspend their operations or had a drop in income due to the coronavirus pandemic. The Government's measures have also entailed helping companies to retain employees on part-time work benefits or by paying wages during termination periods.
- The Government announced various counterbalancing measures to assist homes and individuals to get through the circumstances spawned by the global pandemic, such as payment of wages in quarantine, the withdrawal of personal savings for free use, and extension of income-related unemployment compensation.
- The Government's other main support measures are support loans, supplementary loans, tax deferrals, and payment shelters.

The total amount of support provided to companies and individuals because of the coronavirus pandemic from March to December 2020 was nearly ISK 60 billion. Of this amount, direct financial support was approximately ISK 38.4 billion, postponements of tax payments about ISK 9.7 billion, and loan guarantees about ISK 11.8 billion.[16]

Economic development will mostly depend on how successfully the COVID-19 pandemic in Iceland and other countries is brought under control. Vaccination began at the end of last year, and plans call for it to cover majority of the population around midyear. Also, the quarantine measures, homes' strong position before the pandemic, Icelanders' increased domestic consumption, and the Government's counterbalancing measures have contributed to the revival of private consumption. On the other hand, uncertainty still prevails. There have been several hitches in the distribution and production of vaccines, and, in many other places, the pandemic has been on the offensive. Also, the outlook is for continuing high unemployment, not least for those who previously worked in travel services. It is uncertain when the tourism industry will revive. However, one may assume that the current arrangement at borders will be more or less unchanged for now. Finally, one may expect that companies' smaller investments will reduce the economy's growth capacity. It is therefore difficult to predict how fast the economy will recover, and this will depend on how successful the battle against the virus is.[17]

Threats and weaknesses

With changed economic and social circumstances in the wake of the COVID-19 pandemic, there are various challenges related to measures against money laundering and terrorist financing. The measures the Government has taken to resist the spread of COVID-19 can affect criminals' financial environment and can lead to changed methods for acquiring illegal assets. In this context, FATF has pointed out new threats and weaknesses related to money laundering and terrorist financing.[18]

With increased telecommuting, communications and the dissemination of information and data should take place on the Internet more often than before. In parallel with these changed conditions, the likelihood of cyber-attacks can increase. In this context, FATF has pointed out an increase in criminal offences in certain categories, such as fraudulent activities, fraud, and cybercrime.[19] Examples of fraudulent activities that indicators show are on the rise following the COVID-19 pandemic include the counterfeiting of products, for example, of health products, and impersonation of officials. Cybercrimes can entail social engineering to acquire payment information from individuals or companies, such as by phishing and ransomware attacks. Fraud cases in Iceland have increased in numbers the last several years, and most indications point to a further increase in fraud in 2020. Fraud covers cybercrimes and social engineering. However,

[15] www.stjornarradid.is/rikisstjorn/covid-19 (retrieved on 23 February 2021) and https://www.sedlabanki.is/utgefid-efni/tilkynningar-vegna-covid-19/ (retrieved on 2 March 2020).

[16] www.hagstofa.is/utgafur/tilraunatolfraedi/efnahagsadgerdir-vegna-koronuveirufaraldursins-tt/.

[17] *Peningamál*.

[18] *COVID-19-related Money Laundering and Terrorist Financing.* FATF, Paris 2020, p. 5.

[19] *COVID-19-related Money Laundering and Terrorist Financing, pp.* 6-7.

the criminal statistics from the police do not indicate an increase in this kind of fraud in 2020.

There is also deemed to be a risk that governmental financial support to companies and individuals, as well as international financial assistance, will be misused.[20] The total amount allocated from Iceland's State Treasury to support and/or through direct funding to individuals and companies because of the COVID-19 pandemic was close to ISK 60 billion from March to December 2020.[21] The implementation of solutions is in the hands of IRC, the Directorate of Labour, and CBI. There are no indications of the misuse of remedies or fraud regarding grants although it is not possible to rule out that such has happened or will happen.

FATF has also pointed out that the coronavirus pandemic could affect the capacity of the Government and parties subject to mandatory reporting to execute their mandatory duties related to anti-money laundering and anti-terrorist financing measures from maintaining surveillance, fulfilling their mandatory duty to notify, executing due diligences, and working toward international cooperation.[22]

[20] *COVID-19-related Money Laundering and Terrorist Financing, p.* 9.

[21] www.hagstofa.is/utgafur/tilraunatolfraedi/efnahagsadgerdir-vegna-koronuveirufaraldursins-tt/.

[22] *COVID-19-related Money Laundering and Terrorist Financing, pp.* 11-13.

2 Methodology and conclusions

2.1 Methodology

Generally
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. The members of the Steering Committee are representatives of the MoJ, MoFE, MoFA, MoII, DTI, DPO, FIU, the Reykjavik Metropolitan Police, CBI, and IRC.

Preparation of the risk assessment began in the fall of 2020. 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.[23] Information was also gathered from parties subject to mandatory reporting with the mediation of supervisors. Resources included available statistical information, as relevant. In addition, data collectors relied on the expertise of those involved in the issue category.

It is anticipated that all those having stakes in defences against money laundering and terrorist financing will utilise the risk assessment, 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.
- *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.
- *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.

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 assessment in 2019.[24]

In examining the methodology, the basic concepts are as follows:

- *Risk* consists of three elements, i.e., 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 behaviour 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. 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,

[23] *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.

[24] *FATF Guidance. National Money Laundering and Terrorist Financing Risk Assessment* and *FATF Report. Terrorist Financing Risk Assessment Guidance.* FATF, Paris 2019.

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.
- 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 first step of the risk assessment was to analyse the main threats of money laundering and terrorist financing besetting Icelandic interests. After analysing them, 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. This entails defining the existing threats and weaknesses/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. Threat-guided risk classification (on a scale of 1-4), depending on whether the analysed threat was low, medium, high, or very high.

Low	Medium	High	Very high

The following factors, among others, were considered when analysing a threat:
- Environment: Location and geographical factors, culture, and methods for transport and/or delivery of assets.
- Operations: Knowledge, orchestration of risk and innovation.
- Collaborators: New, unknown, trustworthy, etc.

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. By definition, the factors could increase the risk if they were weaknesses, or, depending on circumstances, if a mitigating factor was involved, it could reduce the threat.

The categories of weaknesses/mitigating factors examined 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.
- Surveillance, i.e., whether surveillance is in place and operating.

A mitigating factor within each category had an assigned weight, i.e., low, medium, high, and very high. The weights of assessment factors were further specified:
- When a mitigating factor was rated as very high, 7.5% was subtracted.
- When a mitigating factor was rated as high, 5% was subtracted.
- When a mitigating factor was rated as medium, 2.5% was subtracted.
- When a mitigating factor was rated low, nothing was subtracted.

The maximum lowering was therefore 30% from a threat if very high mitigating factors were present in all four categories considered. Weaknesses did not increase the percentage to the same degree as mitigating factors. Rather, their assessment involved an assessment, case by case, of what effect weaknesses had on the existing threat.

Part of the methodology of the risk assessment is to assess whether it is necessary to take measures to reduce an identified risk, and, if so, which measures are appropriate. Work will continue on the proposals emerging on processing the risk assessment, and an action plan for meeting them will be prepared.

2.2 Consolidated conclusions

The consolidated conclusions of the risk classification made on the basis of the above methodology are as follows (reference is otherwise made to the accompanying summary of the classification):

Money laundering

Analysed risk regarding money laundering was deemed **very high** when it came to tax fraud as a predicate offence of money laundering, transport of cash to and from the country, cash transactions, private limited companies, remittances, and collection boxes and lottery machines. Furthermore, analysed risk was deemed **high** when it came to large denomination banknotes in circulation, non-governmental organisations and other organisations, religious and life stance organisations, funds and associations operating under a certified charter, deposit operations, payment services, issue of electronic money, foreign exchange, operations of attorneys, operations of accountants, operations of estate agents, operations of car dealerships and car dealers, and products and services. On the other hand, risk was deemed **medium** in operations of limited liability companies, self-governing institutions, and limited partnerships, other charities and NPOs, BOs, loan operations, cryptocurrencies, operations of funds, trading and services for financial instruments, operation of bookkeepers, sweepstakes, precious metals and gems, and ID numbers for foreign citizens. Finally, risk was assessed as **low** in operations of other organisations, pension funds, life insurance operations, operations of ship brokers, lotteries, lotto, and gambling on the Internet.

Terrorist financing

The risk of terrorist financing because of the transport of assets out of the country was deemed to be **medium** and the corresponding risk of the operations of NPOs operating across borders was deemed **low**.

2.3 Risk classification summary

Low	Medium	High	Very high

Assessment factor	Risk classification
Money laundering	
Tax fraud	
Tax fraud as a predicate offence of money laundering	
Cash	
Cash – transport to and from Iceland	
Cash transactions	
Cash in circulation, large denomination banknotes	
Companies	
Private limited companies	
Limited liability companies, self-governing institutions, and limited partnerships	
Other organisations	
Non-governmental organisations and other organisations	
Religious and life stance associations	
Funds and associations operating under a certified charter	
Other charities and non-profit organisations	
Beneficial owners	
Financial market	
Deposit operations	
Loan operations	
Remittances	
Pension funds	
Life insurance operations	
Cryptocurrencies	
Operation of funds	
Payment services	
Trading and services for financial instruments	
Issue of electronic money	
Foreign exchange	
Specialists	
Attorneys	
Accountants	
Bookkeepers	
Estate agents	
Ship brokers	
Car dealerships and car dealers	
Gambling	
Sweepstakes	
Lotteries	
Lotto	
Collection boxes and lottery machines	
Gambling on the Internet	
Trade and services	
Precious metals and gems	
Products and services	
Other	
ID numbers for foreign citizens	
Terrorist financing	
Transport of assets out of the country	
Non-profit organisations operating across borders	

3 Money laundering

3.1 TAX FRAUD AS A PREDICATE OFFENCE OF MONEY LAUNDERING

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, e.g., when a party intentionally or through gross negligence gives wrong or misleading information intended for use with tax decisions. The same applies if a party neglects to provide information that may be significant for tax determinations. Tax fraud can regard both various special penal laws and the General Penal Code. The 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 Act no. 50/1988 on Value-added Tax. If violations of the above special penal laws are major, they fall under the provisions of Art. 262 of 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.

Generally – main threats

Tax fraud is one of the predicate offences of money laundering under Art. 264 of GPC. Investigations into tax offences (tax fraud) are the responsibility of DTI under Act no. 90/2003 on Income Tax and other laws on taxes and fees. During its investigations, DTI follows the provisions of the Act on Criminal Procedure, as applicable. On the other hand, the office does not see to investigations into money laundering. Cases regarding tax law violations can be concluded within the tax system with fines decided by DTI or the Taxation Reassessment Committee, and the cases are then not referred to the police. Also, case investigations completed by DTI are referred for tax reassessment on the basis of a DTI's investigation report. Such completion is not deemed to be a criminal proceeding. If major offences under tax laws are involved, they are referred to the police for handling, based on the Act on Criminal Procedure. If there is suspicion of money laundering during a tax investigation, that part of the case is sent to the police, independent of the case within the tax system. In the most serious cases, this is done during the first stages of investigation.

Tax fraud falls into the following categories:

- *Organised criminal activities:* Entail systematic breaches of the task system's regulations. An example of this could be illegal use of sales accounts 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. The basic factor is that a legal person or individual has an open value-added tax number.
- *Tax fraud:* Entails individuals or legal persons concealing information about income/assets or, purposely or with gross negligence, incorrectly filling out tax returns to avoid paying taxes. Examples of this can be misreported income of operators, a double invoicing system, payment of hidden wages, and unrecorded operating costs, both bogus and regarding personal use.
- *The hidden economy*: Often refers to a "business environment" that 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.

- *Tax avoidance:* Entails bending the tax system's rules to obtain more favourable taxation of income than its nature and origin justify to avoid tax payments, e.g., with simulated instruments. An example of tax avoidance could be interim pricing.

In 2016, the State's total tax income was more than ISK 663.7 billion, and the municipalities' taxes for the same year were ISK 241.4 billion. In 2020, the total tax revenues were ISK 662.7 billion, and local taxes that year were ISK 253.2 billion. No precise figures are available on the magnitude of tax fraud in Iceland. A report from a work group of the Minister of Finance and Economic Affairs states that tax avoidance over the last three decades has ranged from 3% to 7% of the gross domestic product (about 10% of the total tax income of the governmental sector). The report also proposes measures. The report includes the following: *"If avoided taxes in 2016 are assumed to be 4% of the Gross Domestic Product, then they amounted to ISK 100 billion. Added to this amount is the damage to society because of undeclared income related to offshore companies, which is estimated to be ISK 16 billion in financial income tax in the period 2006-2009 and ISK 42 billion from lost wealth tax for the six-year period 2009-2014. Altogether, this makes ISK 58 billion over a 9-year period regarding offshore assets."*[25]

According to information from DTI, the number of cases at the agency has continually increased in recent years. For example, the number of cases from the district public prosecutor, FIU, and the Commissioner of Revenue and Customs has increased. For example, the number of cases filed, based on FIU's analyses, has increased substantially. In 2019, the office processed a total of 482 cases where tax violations were suspected and completed 92 of them with a report. In 2020, the office processed over 600 cases and completed 82 of them with a report. Of these totals, 230 new cases were recorded in 2019 and 368 in 2020.

The percentage of cases where the investigation was dropped was relatively low – less than 20 cases in both years. Also, 27 cases were completed with a reassessment of taxes in 2019 and 43 cases in 2020, i.e., a total of 70 cases. The total amounts in cases closed with reassessment of taxes was about ISK 864.5 million in 2019 and more than ISK 1.9 billion in 2020. The total amount of overdue taxes in 2019 and 2020 was more than ISK 2.5 billion.

In 2019, 67 cases were referred to the district public prosecutor and 62 cases in 2020, i.e., 129 cases altogether. Of these cases, 29 were related to money laundering in 2019 and 32 in 2020.

Information from DTI indicates that tax fraud is more serious than before. In cases the office is investigating that are related to criminal offences under the Value-added Tax Act, the amounts involved are higher than before, and there is more cash in circulation. In some instances, the same individuals are involved with one company after another, and the criminal intent appears to be resolute. The deterrence that punishment and other sanctions are intended to have are, therefore, not having the intended effect in tax law offences.

The Directorate of Tax Investigations, for example, is investigating several offence groups that exploit companies for the purpose of manipulating the value-added tax system. The modus operandi is to issue and utilise bogus sales invoices, where there is no underlying business, that are paid to the supposed issuer. In nearly all cases, assets are withdrawn in cash, so that it is impossible to trace them. In these cases, the total amount of sales invoices and cash in circulation amount to approximately ISK 1 billion. Several such cases are also awaiting investigation by the office.

Finally, the analysis of data stemming from Airbnb operations in the country is in progress. The object involved is 80% of rental payments in the period 2015 to 2018 for the rental of premises here in the country, totalling about ISK 25 billion. At this time, information

[25] *Umfang skattundanskota og tillögur til aðgerða. Skýrsla starfshóps (Scope of unreported taxes and proposed measures. Work Group's Report).* Ministry of Finance and Economic Affairs, Reykjavik 2017, p. 3.

is not available on whether and how many cases will be investigated on the basis of these data.

Whether considering the number of cases or the amounts of money, tax fraud is definitely a serious problem in Iceland. The more serious instances are related to company operations where the company form is exploited, e.g., with contrived transactions, and cash is used to make the "business" untraceable. There is no information about the magnitude of tax fraud as a percentage of predicate offences of money laundering. However, based on a percentage of the gross domestic product, it is logical to estimate that tax fraud is by far the biggest portion of predicate offences of money laundering in the country.

Threats of tax fraud in the country are looked into, considering that tax fraud is a serious problem in Iceland, has been so for a long time, and the magnitude is considerable. Various things contribute to and/or facilitate committing such offences. In this regard, it is worth mentioning how easy access is to various types of companies and how easy it is to exploit companies, cf., the risk assessment's discussion of the operations of companies. Also, one can mention how easy it is to get cash into circulation, cf. the risk assessment's discussion of cash.

Weaknesses/mitigating factors

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. It also seems that penalties do not deter tax fraud as intended. This involves a considerable weakness.

There are various mitigating views to consider. The Government is aware of the magnitude of tax fraud. The number of cases is high, and the regulatory scheme is extensive. Considerable gains have been made regarding tax fraud and money laundering. For example, education has increased with the publication of instructional materials, e.g., regarding the organised avoidance of value-added tax in connection with contracting, and informative meetings on money laundering have been held for professions and organisations. Also, the collaboration of those with access to the issue group has increased, including through the publication of collaboration agreements between relevant governmental units. Finally, amendments have strengthened remedies counteracting ID number-hopping in business operations and exploitation of companies, cf. the discussion below of private limited companies.

Risk classification

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 **very high**.

3.2 CASH

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. Threats and weaknesses related to the use of cash are therefore specifically discussed here. This discussion especially emphasises the transport of cash to and from Iceland, operations where transactions and payments in cash are prevalent, and issues related to the use of bigger banknotes. The analysis and following risk classification utilised information and reports from institutions and other administrative parties, information from the police and FIU, and appropriate legislation.

Cash – transport to and from Iceland

Risk classification

Generally – main threats

Pursuant to Art. 27 of the Tax Act no. 88/2005, importers, exporters and, depending on circumstances, customs agents, tourists, and itinerants have a duty to specifically inform the Directorate of Customs of liquid assets in the form of cash or bearer certificates, including travellers' cheques, transported into the country from other countries or out of the country to other countries in amounts of €10,000 or more, based on the official exchange rate, as recorded each time. Pursuant to Act no. 88/2005, the Directorate of Customs is responsible for customs control.

According to the Regulation on Custody and Customs Clearance for Products no. 1100/2006, there are 23 ports of entry for customs clearance. Their locations are as follows: Reykjavik, Grundartangi, Akranes, Grundarfjördur, Ísafjördur, Skagaströnd, Saudárkrókur, Siglufjördur, Akureyri, Húsavík, Vopnafjördur, Seydisfjördur, Neskaupstadur, Eskifjördur, Reydarfjördur, Egilsstadir, Höfn í Hornafirdi, Vestmannaeyjar, Thorlákshöfn, Keflavik, Keflavik Airport, Hafnarfjördur and Kópavogur.

Most tourists arriving in Iceland go through the Keflavik Airport. On the other hand, there are many ways into and out of the country. In addition to Keflavik Airport, there are three other international airports in the country, i.e., Reykjavik Airport, Akureyri Airport, and Egilsstadir Airport. There are also some arrivals, mainly privately owned aircraft, at other smaller airports. The main cargo ports are Reykjavik Harbour, Grundartangi, Reydarfjördur, Seydisfjördur, and Thorlákshöfn. Most cargo shipments to and from the country go through them. Part of the year, a passenger ferry comes and goes at Seydisfjördur, and a ferry carries cargo once a week to and from Thorlákshöfn. Finally, there is considerable export of fish through many ports in rural areas. 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 known that pressure is increasing to allow luxury liners to land in more places than the recognised customs ports of entry, following new rules on electronic service for craft and even allowing them to ferry passengers ashore in remote tourist destinations.

In past years, the number of tourists has greatly increased. The exception was last year since there was a considerable contraction in the arrivals of foreign tourists to Iceland. 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 notice. In the last three years, there were fewer than 30 such notices. In 2020, two cases arose where a party carrying cash exceeding €10,000 was stopped at departure by employees of the Directorate of Customs. This was an increase from previous years. In addition, there were three cases where, without notice, cash exceeding €10,000 was found in a postal delivery, expedited delivery, or cargo shipment. Again, this involves an increase in numbers, as there were no examples of this type of case in previous years.

The main threat with the transport of cash is that it is easy, simple, and inexpensive to transport cash across Iceland's borders, and it is possible to pack a great quantity of cash into a relatively small space, especially if big denomination banknotes are involved. Except in 2020, very many people arrive in and leave the country, and there are many ways to do so by aeroplane, ship, and automobile. In addition, disclosure is limited to the individual duty if in possession of cash exceeding €10,000, or reliant on discovery upon inspection by customs authorities.

Finally, cases have come under police investigation, where unlawful gain is converted into foreign currency and moved out of the country. However, during the investigation of such cases, the police have seized a small quantity of cash in past years.

Weaknesses/mitigating factors

There are very few notices upon arrival to or departure from the country of cash that exceeds the permitted limit. Furthermore, few employees see to customs control, relative to the scope involved. There is little monitoring of the transport of assets across borders. The very few cases that customs authorities uncover, where passengers smuggle cash in luggage and goods shipments, reflects this even though an increase in the number of cases of this kind may be seen.

Amongst mitigating factors worth mentioning is the ongoing training of the Customs' dogs to search for money. Also, the office of the Director of Customs has enhanced its education, and new work procedure has been adopted. Furthermore, collaboration between the police and customs authorities has increased. Likewise, it is worth mentioning that amendments to the Customs Act are being planned. This entails planned strengthening of customs surveillance authorisations to monitor and impose penalties.[26] Finally, a new passenger analysis system, intended to strengthen governmental surveillance of borders, is expected.

Risk classification

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

Cash transactions

Generally – main threats

Generally, access to banking is good in Iceland. The Regulation on normal and healthy business practices of financial undertakings, paying agencies, and electronic money entities no. 1001/2018 states in part that the policies, procedures, and implementation of the operations of a financial entity, paying agency and electronic money entity shall not limit or abnormally prevent access to general financial services. This entails having to provide all parties access to basic banking services.

The use of cash in this country is small, relative to the use of payment cards. At year-end 2020, the number of active payment cards was about 460,000. In addition, on a global scale, the use of cash in Iceland is small. In states of the European Union, households use cash for 79% of cash transactions, compared to just under 13% in Iceland.[27] However, it can prove difficult in Iceland to measure what part cash plays in cash transactions, and a precise analysis has not been done. Existing information on the use of cash includes:

- Iceland uses nearly the least cash of any country in the world.
- The use of cash in the country in cash transactions has decreased. The proportion of cash is about 8% of cash transactions.
- Only about 10% of product sales (food, fuel, furniture) is paid in cash.
- In addition, there are indications that quite a quantity of banknotes is not used for regular transactions. Rather, they lie nearly untouched with their owners.
- Many industries make little or no use of cash, for

[26] https://samradsgatt.island.is/oll-mal/$Cases/Details/?id=2853

[27] *Fjármálainnviðir (Financial Infrastructure).* The Central Bank of Iceland, Reykjavik, 7th Monograph 24 June 2019, pp. 31-32.

example, in the sale of airline tickets and households' payment for electricity and heating.

The circulation of cash in the country has increased as a percentage of gross national product. Following the economic collapse in 2008, the use of cash increased from less than 1% of GNP to more than 2%. At nominal par, the use of cash has increased in recent years. The growth was over 13% in 2016 and more than 9% in 2017. Generally, cash use as a percentage of gross national product has been estimated at 2%-2.5%. At the end of 2020, the cash in circulation was about ISK 77 billion.

In parallel with the increase in cash, there has been a great increase in the number of tourists coming to the country, i.e., from more than 800,000 in 2013 to about 2.3 million in 2018. Despite a definite low in the travel industry because of the global pandemic, this is probably the industry that will revive. The increase in the number of foreign tourists is a possible explanation of the increased cash in circulation in Iceland in recent years.[28] Foreign tourists visiting Iceland have arrived with a lot of Icelandic cash, and the turnover of foreign payment cards has also increased. To this must be added the proviso that the information on the use of foreign payment cards does not distinguish between whether foreign tourists are involved, or foreign payment cards owned by parties residing in the country. Finally, foreign tourists buy Icelandic currency in bank branches and other money exchange services in the country.

Information on the use of cash in company operations is not available. 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. There are exceptions to this as previously mentioned. 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. The risk assessment deals elsewhere with estate agents, and reference is made to that discussion.

Comparatively little is therefore known about the actual use of cash by companies and individuals, and there are few restrictions on its use. Additionally, no regulations apply to the use of cash – for example regarding deposits and withdrawals – aside from with automatic teller machines (ATMs). Finally, there is no monitoring of the use of cash, other than CBI ensuring that sufficient cash is in circulation.

The main threats with cash transactions are that the accessibility of cash in this country is good, and it is therefore easy to get it quickly into circulation. Cash in circulation is untraceable, and for this reason, it is easy, for example, to put unlawful gain from criminal activities into circulation. 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. There are 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 kronur for it.

Weaknesses/mitigating factors

There are no constraints or restrictions on the use of cash, and rather little is known about the ultimate use of cash. 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”.[29] Also, there is almost no monitoring of the use of cash except for aspects of economic management. It is mainly the tax authorities that monitor black operations and the police in connection with investigations of individual cases. Finally, it appears that risk awareness of the use of cash is not high.

However, it is worth mentioning as a mitigating factor that the use of cash in Iceland is small, compared to many other European countries, including countries in the European Union. Also, authorities have increased education and the publication of instructional material where operations entail voluminous cash transactions.

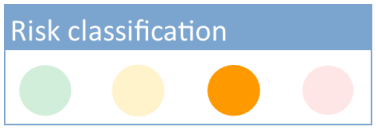
Risk classification

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

[28] *Fjármálainnviðir.* The Central Bank of Iceland, Reykjavik, 5th Monograph 7 June 2017, p. 11.

[29] *Umfang skattundanskota og tillögur til aðgerða. Skýrsla starfshóps,* p. 36.

Cash in circulation, large denomination banknotes



Generally – main threats
The discussion of the use of large denomination banknotes intertwines with the previous discussion of cash.

Five kinds of banknotes are circulating in Iceland. This arrangement has been in place since the latter part of 2013. Then 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, among other things, reducing the number of banknotes in circulation.

At the end of 2020, banknotes in circulation, apart from CBI, were as shown in Table 2.

The most numerous banknotes in circulation are ISK 1000 bills and the least numerous are ISK 2000 bills. About 52% of all banknotes in circulation are ISK 500 and ISK 1000 bills. About 47% 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.

Table 2. Banknotes in circulation apart from those from the Central Bank of Iceland (CBI).

Denomination of banknotes	Circulation apart from CBI	%	Number of banknotes	%
ISK 10,000 bills	49,942,500,000	64.8	4,994,250	26.8
ISK 5000 bills	18,826,000,000	24.4	3,765,200	20.2
ISK 2000 bills	212,000,000	0.3	106,000	0.6
ISK 1000 bills	6,415,000,000	8.3	6,415,000	34.5
ISK 500 bills	1,669,750,000	2.2	3,339,500	17.9
Total	**77,065,250,000**	**100**	**18,619,950**	**100**

Regarding cash transactions with foreign currency in Iceland, the following information is available from CBI on the purchase and sale of foreign currency in 2018-2020 in Tables 3 and 4.

Information is not available on further use of foreign banknotes in Iceland, and/or which individual banknotes have the biggest circulation. It is public knowledge that the European Central Bank recently quit issuing €500 bills although the bills will continue to be legal tender. As an example, it is worth mentioning that using large denomination banknotes makes it

Table 3. Cash transactions with foreign currency, broken down by customers.

Customers	2018	2019	2020
Domestic individuals	33.8	30.7	8.6
Foreign individuals	7.2	8.8	4.3
Domestic legal persons	32.3	40.0	9.8
Tourists	10.2	7.5	0.6
Total	**83.6**	**87.1**	**23.3**

Amounts in billions of ISK.

Table 4. Cash transactions with foreign currency, broken down by currency.

Breakdown by currency	2018	2019	2020
EUR	45.1	49.1	12.6
USD	18.4	17.7	5.3
GBP	6.7	6.4	1.4
PLN	4.7	5.6	1.6
DKK	3.1	3.3	0.8
SEK	1.3	1.2	0.3
NOK	1.5	1.7	0.4

Amounts in billions of ISK.

possible to transport considerable sums between countries. For example, one can put about €6 million in €500 bills into a regular briefcase, which is more than ISK 900 million.

The main threats are comparable to those in cash transactions. Additionally, it is fairly easy to get high-denomination bills into circulation since it is generally easy to pay in cash, and there are few restrictions on doing so. Also, a large part the cash in circulation, in terms of the amounts, is in the form of large denomination banknotes, and their percentage, in terms of numbers, has increased despite still being proportionately less than lower denomination bills. In this way, it is rather easy to get large sums of money into circulation despite the use of cash generally being proportionally small.

Also, a known example of money laundering in police cases is the conversion of unlawful gains into foreign currency, often Euros, and the suspicion is that it is transported out of the country. On the other hand, nothing indicates that large denomination banknotes are used more than other bills in criminal activities in Iceland. To exemplify, of the cases where police have been involved where money has been seized, the percentage of large denomination banknotes is not high.

Weaknesses/mitigating factors

It is not known where the business community most uses large denomination banknotes. Information is also lacking on the use of cash, regarding both Icelandic and foreign banknotes – if they are accessible and distinguishable.

A mitigating factor worth mentioning is that the biggest issued bank note in Iceland is the ISK 10,000 bill, which was put into circulation at year-end 2013. This is not a particularly high amount, compared to banknotes in other currencies. Also, the use of cash generally in Iceland is small, compared to other European countries.

Risk classification

The risk of using large denomination banknotes is deemed **high**.

3.3 COMPANY OPERATIONS

COMPANIES WITH A FINANCIAL PURPOSE AND GENERAL COMPANIES
Iceland has great many companies and organisations, and their forms vary. 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. 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. 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, come private limited companies. Second, there are limited companies, limited partnerships and private institutions engaging in business operations. Third, come other companies. Finally, there is a discussion of general associations and non-governmental organisations (NGOs) having no financial purpose. The analysis and following risk classification drew on information from the Business Registry, police, DTI, reports from other governmental units and appropriate legislation.

Private limited companies

Founding, operations, and winding up – main threats
Act no. 138/1994 applies to private limited companies. This is the most common company form by far. There were nearly 41,000 private limited companies at the start of 2021. In 2019 about 2200 new private limited company were founded and in 2020, nearly 2500. Information on the winding up of such companies or bankruptcy for the same period is not available, but in 2019, about 800 companies in Iceland went bankrupt.[30] From this it can be inferred that many more private limited companies are founded each year than are wound up. Information on how many registered private limited companies are operating is not available. 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), member states of the European Free Trade Association or the Faeroe Islands, can also be founders.
- Proposed by-laws stating, among 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.

[30] www.hagstofa.is/talnaefni/atvinnuvegir/fyrirtaeki/gjaldthrot/.

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 and control over his finances.

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 General Penal Code 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 IRC. There is no condition for a private limited company to be in operation or in business. 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, judgements 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, among 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 Act no. 3/2006 and are obligated to have an accountant or examiner. 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 with the associated review of an examiner or accountant. 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. Monitoring of the submission of annual financial statements is the responsibility of IRC's Register of Annual Accounts. The submission of annual financial statements has gradually improved in previous years. In 2019, the submission of annual financial statements was close to 90%. That year nearly 36,000 of more than 41,000 companies submitted annual financial statements. On the other hand, nearly half of companies submitted annual financial statements after the mandatory submission date, 31 August. Furthermore, fines regarding late submissions of annual financial statements were imposed in 3500 instances.

Generally, a private limited company can cease to exist in three ways, i.e., by merger, winding-up or bankruptcy. Act no. 138/1994 deals with companies' winding-up and merger. 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.

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 the number of them and the frequency of their founding, it is simple and easy to establish a network of companies that can be used to launder money through tax fraud and other predicate offences of money laundering. It is also possible to have companies with no operations, i.e., "dummy companies", since there are no requirements regarding operations or activities.
- 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.

- There is also the familiar manoeuvre shortly before bankruptcy of swapping the spokespersons of private limited companies with "funeral directors". This entails getting individuals on record as board members of a company to conceal its real directors.
- 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 judgement on 20 November 2020 in Case no. 533/2019, Supreme Court of Iceland judgement on 3 November 2016 in Case no. 738/2015, and Supreme Court of Iceland judgement on 22 September 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. Supreme Court of Iceland judgement on 6 April 2017 in Case no. 770/2015 and Supreme Court of Iceland judgement on 28 April 2016 in Case no. 74/2015.
- Active monitoring of the submission of annual financial statements is limited, not building, for example, on systematic analysis of the modus operandi, e.g., regarding the analysis of profit in annual financial statements of companies in the same line of work, operational expenses, and possible tax avoidance.
- Black operations thrive in Iceland. Among other things, reports about tax evasion have been written and made public. Figures regarding this vary, but observers deem that the scope of hidden operations can range from 3% to 7% of gross national product. 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.[31]
- One form of criminal activities within otherwise lawful operations are various transactions between related parties that, for example, can stretch across borders. The private limited company form has been used for this purpose, e.g., to sever the money trail. The disposition of such money can entail money laundering if unlawful gains are involved.
- 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. Supreme Court of Iceland judgement on 6 April 2017 in Case no. 770/2015.
- There is no duty to wind up a private limited company that has shut down operations. There are instances of “empty” companies having been misused and their bank accounts used to conceal a trail of money.

Weaknesses/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. Examples include the qualifications of founders, board members, and owners of private limited companies, swapping the directors of private

[31] *Umfang skattundanskota og tillögur til aðgerða. Skýrsla starfshóps.*

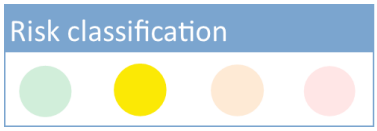
limited companies shortly before bankruptcy for "funeral directors", checking up on board members' loss of eligibility in private limited companies, more stringent penalties for deficiencies in submissions of annual financial statements, and de-registration and winding up of companies when they are no longer in operation. Governments also lack legal remedies enabling them to exchange information on company operations, regarding, for example, the loss of eligibility. 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. 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 Iceland regarding private limited companies' operations and money laundering, as authorities' determination to address ID number-hopping shows.[32] In this regard, also worth mentioning is 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. There ID number-hopping is the primary target. More specifically, this involves amendments to Art. 262 of GPC regarding prohibited business activities.[33] A parliamentary bill was also introduced to amend the Act on Bankruptcy etc., no. 21/1991 (prohibited business activities). The purpose was to clamp down on the misuse of the limited company form and ID number-hopping in business activities.[34] However, the bill did not pass. Finally, the passage of Act no. 82/2019 on the Registration of Beneficial Owners is a substantial improvement. It requires information to be on file on the real ownership of companies. The relevant authorities will therefore always have access to information on companies' beneficial ownership.

Risk classification

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 **high**.

Limited liability companies, self-governing institutions, and limited partnerships



Foundation, operations, and winding up – main threats

Act no. 2/1995 applies to limited liability companies and partnerships limited by shares. In most ways the legal requirements for limited liability companies and partnerships limited by shares are comparable to those applying to private limited 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 liability in partnerships limited by shares and limited partnerships is mixed.

Act no. 33/1999 applies to self-governing institutions that engage in business operations. A self-governing institution is not a company but rather a specific form of organisation. Such an institution's main characteristic is that no defined party lays claim to the assets of self-governing foundations. Self-governing

[32] *Skýrsla samstarfshóps félags- og barnamálaráðherra um félagsleg undirboð og brotastarfsemi á vinnumarkaði (Report of the Minister of Social Affairs and Children on dumping and criminal activities on the labour market).* Ministry of Social Affairs and Children, Reykjavik 2019.

[33] Act no. 56/2019 amending the General Penal Code, Act on Limited Companies, Act on Private Limited Companies, and Act on Self-governing Institutions Engaging in Business Operations (misuse of company form and conditions of qualification).

[34] www.althingi.is/altext/150/s/1429.html.

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 institutions. However, the same qualifications are required for the board members and managing director as in limited liability companies and private limited liability companies.

The combined number of limited liability companies, partnerships limited by shares, limited partnerships and self-governing institutions that engage in business operations is more than 3800. Thereof limited partnerships are by far the most numerous – more than 3000.

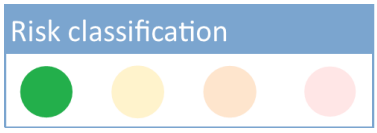
Many of the threats applying to private limited liability companies apply to limited liability companies, partnerships limited by shares, limited partnerships, and self-governing institutions that engage in business operations. On the other hand, these organisations are many times fewer. Fewer of them are founded per year, and the instances of their misuse are nowhere near the percentage for the private limited liability company form. It is thereby more difficult to use these company forms to launder unlawful gains.

Weaknesses/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 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.

Mitigating factors applying to private limited liability companies also apply to these company forms.

Risk classification
The risk related to the founding, operation and winding up of limited liability companies, partnerships limited by shares, limited partnerships and self-governing institutions that engage in business operations is **medium**.

Other organisations



Foundation, operations, and winding up – main threats
Hereunder are company forms other than those discussed above having a financial purpose. Most of these organisations are partnerships. There are more than 2000 of them. The number of them has decreased a bit since the last risk assessment. Other company forms are, for example, cooperatives, European financial interest groups and European companies. Special acts apply to all of the above company forms.

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

Weaknesses/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
For the above reasons, the risk regarding the founding, operations, and wind-up of companies other than those previously discussed is **low**.

Non-governmental organisations and other organisations

Risk classification

Generally – main threats

This category of general associations and non-governmental organisations (NGOs) belongs to organisations that are not operated for profit. These organisations are structured, permanent organisations of two or more parties that are founded with a private law instrument. No act provides for the structure of general organisations or clubs, 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, and cultural associations. It is possible to register general associations and NGOs in the Business Registry under the Act on the Business Registry no. 17/2003. However, they have no duty to register and must apply to do so.

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.

The Business Registry supervises the registration of general associations. Information about associations' founding documents and their registered articles of association can also be found in the Business Registry, if registered. However, the operations of such associations are not monitored, and no association or organisation has the function of overseeing their operations. Each association's articles of association delimit its operations. However, there are no general qualifications set for their founders, owners or spokespersons or the know-how to see to finances and accounting. In addition, there is no information anywhere on how finances and accounting of general associations are arranged. Also, no rules or instructions apply to the operations of general associations except that they must have a lawful purpose. Finally, no instructions have been issued on the management practices of such associations.

At year-end 2020, there were about 12,000 general associations and NGOs. The number of them has decreased by about 4000 since the last risk assessment. One can suppose that this stems from the entrance into force of Act no. 82/2019 on the Registration of Beneficial Owners.

The main threat is that this form of company will be misused regarding money laundering is the lack of oversight, the great access to such companies, and the ease of founding them, along with the great number of organisations and clubs that are registered. It is also easy to launder money through their operations since such companies have no requirements regarding finances. Finally, misusing the company form requires no expertise.

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

Weaknesses/mitigating factors

A comprehensive overview of general organisations and associations is lacking as well as monitoring and a legal framework for their operations. There is no instruction on the operations of general organisations and clubs, e.g., on good management practices or instructions on finances and accounting, with the exception of NPOs under Act No. 119/2019 on the Obligation of Non-profit Organisations to Register. No other rules apply to the operations of such companies and clubs, other than those they set for themselves as articles of association.

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. Act no. 82/2019 on the Registration of Beneficial Owners.

Risk classification

Considering the above threats and weaknesses, and after taking into account mitigating factors, it must be deemed that there is a **high** risk that this organisation form can be misused.

NON-PROFIT ORGANISATIONS

The risk assessment considered non-profit organisations (NPOs). The purpose of these associations 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'."*[1] On this basis, the discussion was limited to registered religious and life stance associations, associations and funds that operate under a certified charter and other NPOs. Please note that companies operating in accordance with Act no. 119/2019 on the Obligation of Non-Profit Organisations to Register regarding NPOs operating across borders are separately discussed in the section of the risk assessment on terrorist financing. The analysis here, for example, utilised information from the Business Registry, supervisors, police and DTI, information and reports from other governmental units and appropriate legislation.

Religious and life stance associations

Risk classification

Generally – main threats

Religious and life stance associations operate under Act no. 108/1999 on Registered Religious and Life Stance Associations 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. There are 51 religious and life stance associations. Of these, 45 are religious organisations, and six are life stance 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 2020, this amount was ISK 11,700 per person per year. In 2020, about ISK 2.6 billion in congregational fees was paid from the State Treasury.[35] The act sets several general conditions for the registration of such associations.

Spokespersons for registered religious and life stance 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.

There are no rules on the disposition of the funds of religious and life stance associations, except that these associations are obligated to send a district commissioner an annual report on their activities. Also, the monitoring of these companies' finances and accounting is limited, and the legal remedies of the party seeing to the monitoring are limited. No qualifications are required for those seeing to the associations' finances. They can be their spokespersons, or others, depending on what the by-laws of the relevant associations stipulate.

The District Commissioner of North-east Iceland supervises the registration of religious and life stance associations and sees to their monitoring. The district commissioner's monitoring especially involves 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

[35] *Sóknargjöld 2020 (Parish fees 2020)*. Financial Management Authority, Reykjavik 2021, p. 2.

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.

In the last two to three years, submissions to the District Commissioner of reports from religious and life stance associations' finances have decreased. Before 2017, 36 associations submitted the report. Before 2018, there were 32 submissions, and in 2019 there were 26.

The main threat from operations like these is that the company form will be misused to benefit criminal activities, including for laundering unlawful gains. There is one known example a religious association that was misused to engage in alleged punishable conduct. That case is going through the criminal justice system.

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

Weaknesses/mitigating factors
There are weaknesses in the framework, legislation, and monitoring of registered religious and life stance 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.

On the other hand, few religious and life stance associations are registered, and cases related to the misuse of this company form are rare. Since the last risk assessment was prepared, 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.

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

Funds and associations operating under a certified charter

Generally – main threats
Here Act no. 19/1988 on Funds and Associations Operating under a Certified Charter and Regulation no. 140/2008 on the same subject are discussed. 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 2021, a fund's minimum initialisation funding may be ISK 1,285,000.[36] 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, not 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

[36] www.syslumenn.is/thjonusta/thinglysingar-og-stadfestingar/stadfestingar-a-skipulagsskram-fyrir-sjodi-eda-stofnanir/.

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 Accounting Office, shall 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 annual financial statements of associations and funds. According to published abstracts for fiscal 2019, at the end of the year, there were 696 active associations and funds operating under a certified charter. Also, 7 new charters were confirmed during the year, and 16 associations and funds, deemed unqualified, were closed down. At the start of 2021, 473 funds and associations submitted annual financial statements to the Icelandic National Audit Office for fiscal 2019. Altogether, 705 funds and associations were obligated to submit annual financial statements for that year, and therefore 67% of the annual financial statements were received six months after the deadline. A total of 54 funds and associations have never submitted an annual financial statement.[37]

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 56 funds submitting an annual financial statement for 2019 were less than ISK 500,000. Of these, eight funds had no assets at the end of 2019, and a majority of those was closed down that year. Of the 473 associations and funds submitting annual financial statements, 216 of them had income in 2019. Of the 257 funds that had no income during the year, 128 of them had no expenditures. In addition, five funds had neither income nor expenditures, nor did they have assets at year-end 2019.

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 30% of more than 700 associations and funds do not submit annual financial statements or submit them too late.

Finally, there is an example of a fund or foundation being misused to perpetrate alleged punishable conduct. The police are processing that case.

Weaknesses/mitigating factors

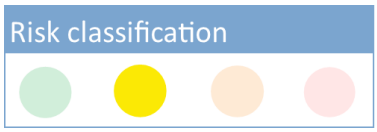
Act no. 19/1988 is past its prime and requires comprehensive re-examination, keeping in mind that far too many funds and associations do not submit annual financial statements, and monitoring of the operations is limited. There are no penalties for failing to submit an annual financial statement. The remedies the act prescribes are few and appear not to be utilised as mandated. Furthermore, there are no conditions in the act on the qualifications of those directing such funds and associations. On the other hand, cases related to misuse of this organisation form are rare.

Risk classification

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

[37] *Útdráttur úr ársreikningum sjálfseignarstofnana og sjóða sem starfa samkvæmt staðfestri skipulagsskrá, fyrir rekstrarárið 2019 (Abstract from annual financial statements of private foundations and funds operating under a confirmed charter for fiscal 2019).* National Audit Office, Reykjavik 2021, p. 2.

Other charities and non-profit organisations



Generally – main threats

This category includes organisations and associations working in the public interest. Therefore, the consideration here is the organisation's purpose, not its form. On one hand, under the category come general organisations and associations that are not operated for profit but work in the public interest. The risk assessment, under general organisations and associations, has already discussed this form of organisation. On the other hand, this category includes NPOs operating under Act no. 119/2019 on the Obligation of Non-profit Organisations to Register.

At the end of 2020, there were about 12,000 general organisations and associations. The Business Registry does not classify organisations according to their purpose. For this reason, there is no information on how many of the registered general organisations and associations are working in the public interest. From the previous risk assessment, it can be supposed that the organisations working in the public interest number a few hundred – 450 at most. If their operations reach across borders, registration is mandatory for them.

NPOs operating across borders are dealt with in the aforementioned Act no. 119/2019. Registration of them is mandatory. They number just under 30. The requirements for the above organisational form are suitable, given their number. The scope of these companies is not great. According to Art. 38 (2) of AML Act, cf. the act amending Act no. 96/2020, IRC monitors such organisations.

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.

Weaknesses/mitigating factors

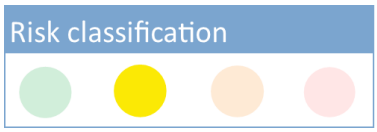
A comprehensive overview of general companies and associations in the public interest is lacking as well as monitoring of and a legal framework for their operations. It is simple and inexpensive to found these associations. No coordinated rules apply to their operations, and they are not monitored. There is no education on the operations of general associations and clubs, for example, on good management practices or instructions on finances and accounting, except for organisations operating across borders under Act No. 119/2019. No other rules apply to the operations of general organisations and clubs working in the public interest domestically, other than what they set for themselves in articles of association.

A mitigating factor is the duty to register BO of a general organisation or club. This is intended to detect and prevent money laundering, cf. Act no. 82/2019 on the Registration of Beneficial Owners. One must also consider that the percentage of the organisations working in the public interest, compared to the total number of general organisations and clubs, is low. Finally, there have been educational meetings for organisations operating across borders, based on Act no. 119/2019.

Risk classification

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**.

Beneficial owners



Generally – main threats

Beneficial owner (BO) is defined in Act no. 140/2018 on Measures against Money Laundering and Terrorist Financing 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. Act no. 82/2019 on the Registration of Beneficial Owners 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.

On 6 July 2019, Act no. 82/2019 on the Registration of Beneficial Owners entered into force. It was the first legislation of this kind in Iceland. It was a major judicial reform. Up to this time, the registration of owners of legal persons varied. After the enactment of the new legislation, the de-registration of companies increased. The goal of the law is to ensure that there is always correct and reliable information on BOs of legal persons to which the law applies so that it is possible to detect and prevent money laundering and terrorist financing, cf. par. 1 of Art. 1 of the act. The act covers legal persons engaging in business operations in Iceland or that are registered in the Icelandic Business Information Centre, including foreign branches of limited companies and private limited companies, cf. Art. 2 (1) of the act. The act also applies to foreign trust funds or comparable parties engaging in business in the country, cf. par. 2 of the same provision. 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, cf. par. 3. In case of doubt, IRC will determine whether a party or category of parties falls under the act, cf. par. 4 under Art. 1 (2) of the act. Information about BOs of a legal person shall be on record in the Business Registry operated by IRC. Registration agents must provide notice of all changes in registration, cf. Art. 6 of the act.

Section III of Act no. 82/2019 prescribes penalties. The act provides two kinds of penalties, i.e., day fines for parties with a duty to register under Art. 14 and non-criminal fines for an individual or a legal person under Art. 15. The act also authorises the wind-up and de-registration of a party with a duty to register.

Information provided by the Business Registry states that nearly 95% of all parties with a duty to register completed registration of BOs by the end of 2020, i.e., more than 59,400 legal persons. At the same time, notices of planned day fines had been sent to nearly 11,500 legal persons, and the fines levied numbered nearly 2250. Also, rulings on day fines had been sent to nearly 2700 legal persons.

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. On the other hand, it entails a risk for the individual undertaking such responsibility, and the Business Registry likewise monitors this, and there are many examples in DTI's investigations of violations regarding value-added tax that individuals have been obtained to register on the company's Board of Directors to conceal who governs it. This can occur right at the start of operations, during the company's operations, or with "funeral directors" right before the end of operations. One may suppose that the new legislation will clamp down on this, but there is currently insufficient experience with this. The main threats must be assessed considering the short period that Act no. 82/2019 has been in force, the great number of parties having a duty to register, and that day fines have been levied.

Weaknesses/mitigating factors

The main weaknesses involve the short period that Act no. 82/2019 has been in force and the limited experience accumulated regarding it, in addition to the

great number of parties having a duty to register.

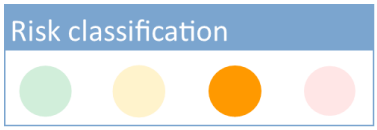
On the other hand, the registration of parties obligated to register has been outstanding. Also, the act provides remedies to penalise and de-register companies that have not registered BO. Moreover, the publication of educational materials addressing this issue category has increased.

Risk classification
In light of the great improvements in the registration of BOs, the risk of this assessment factor is deemed **medium**.

3.4 FINANCIAL MARKET

This section discusses the assessment and analysis of the risk of money laundering and terrorist financing in the Icelandic financial market. The Central Bank of Iceland's Financial Supervisory Authority (FSA) is the supervisory body responsible for following up on parties subject to mandatory reporting in the financial market under the Act on Measures against Money Laundering and Terrorist Financing, regulations, rules, and related criterial rules. FSA 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 evaluation of threats and weaknesses/mitigating factors was done, for example, in light of the know-how and experience of relevant governmental parties and law enforcement institutions in the financial market. Finally, the evaluation is based on various statistics related to a party's operations in the financial market.

Deposit operations



Generally – main threats

Deposit operations mean the receipt of repayable assets from the public in the form of deposits under Art. 3 (a) of Act no. 161/2002 on Financial Undertakings.

Four banks and four savings banks have permits to receive deposits under the Act on Financial Undertakings. The total amounts of the banks' and savings banks' deposits were as follows:

- In 2017 – ISK 1697 billion
- In 2018 – ISK 1849 billion
- In 2019 – ISK 1899 billion

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 criminal activities. Accessibility to these services is easy, for most people can open deposit accounts in domestic banks and savings banks. In addition, it is easy to utilise these services since they do not require much organisation or specialised knowledge.

Organised criminals and/or a criminal organisation can use deposits to launder unlawful gains. The main threat entails the opening of numerous deposit accounts where transfers, deposits, and withdrawals are frequent, often involving low amounts that may have the purpose of escaping notice.

Money laundering through deposit accounts is one of the commonest methods known to the police, FIU and DTI. 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.

Weaknesses/mitigating factors

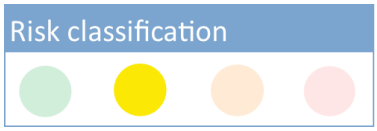
Despite the methods resorted to by parties subject to mandatory notification being generally considered acceptable, there are weaknesses, including customers' risk classification and risk-based monitoring. It is also important to mention that new technology can create new risks and opportunities.

On the other hand, one can mention that anonymous transactions are not permitted, and the legal framework seems 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. Considering the acceptable

efficiency of internal monitoring, deposit operations are less exposed to money laundering. Also, the four commercial banks do not have branches in other countries, and they have few foreign customers even though their number has been increasing. Finally, the publication of educational material has increased.

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

Loan operations



Generally – main threats
Deposit operations entail granting loans to individuals and companies. Commercial banks make comprehensive loans to individuals and companies. 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. There is also one specialised lending company that finances auto-mobiles and equipment. There is one credit agency seeing specifically to acquiring service, along with providing consumer loans, for example, in the form of credit card loans. Other parties subject to mandatory reporting provide loans, although more limited in number or in lower amounts than the above parties do, for example, pension funds, creditors, and payment agencies.

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 is increasing.

The main threat of money laundering besetting loan operations is the repayment of loans with proceeds from criminal activities. On the other hand, there are few examples and/or indications that criminals or organised crime utilise this option to launder unlawful gains. For this reason, one must suppose that lending operations are not very exposed to such threats.

Weaknesses/mitigating factors
Despite the methods resorted to by parties subject to mandatory notification being generally considered acceptable, there are weaknesses, including customers' risk classification and risk-based monitoring. Also, 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. Such operations generally demand expertise on the operations of companies to enable laundering considerable sums with this method.

The internal monitoring of loan operations is generally deemed 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 Act no. 118/2016 on Mortgage Lending to Consumers provide for lending institutions having acceptable internal lending rules and processes. Also, 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 acceptable. Likewise, the authorities have published educational materials related to the issue category.

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

Remittances

Generally – main threats

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. the Act on Payment Services no. 120/2011. Customers do not have to have accounts with the payment service provider to engage in these transactions.

In Iceland, four agents of foreign paying agencies are authorised to engage in remittances, but only two of them are active in the market. The total amount of money remittances in 2020 was about ISK 2.44 billion.

Remittances in Iceland are only done by agents of foreign paying agencies. This entails considerable risk, not least because it is generally difficult for paying agencies employing agents to control and monitor them. Money transfer services that agents provide on behalf of foreign payment services generally operate in parallel with other different operations, e.g., store operations.

The service provided by paying agencies and their agents that engage in remittances build in many respects on transactions with cash. 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.

The threats facing these operations mean that business relations are often not for the long term and only involve several individual transactions, where limited due diligence is carried out. These characteristics of the operations, along with possibly forged personal identity papers being used to confirm identity, cf. the discussion of ID numbers for foreign citizens, possibly contribute to the limited availability of information about customers and the purpose of a transfer. In addition, it should be mentioned that money laundering through these operations does not require special know-how or organisation. Finally, financial services of this type being operated in parallel with other unrelated operations are deemed to entail a threat.

FIU has received several notices regarding the suspicion of money laundering through remittances.

Weaknesses/mitigating factors

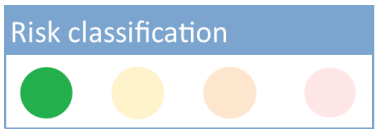
The amount of cash transfers is substantial in Iceland, considering the number of transactions. There are indications that despite parties subject to mandatory reporting having resorted to specific measures to guard against money laundering, there are still considerable weaknesses regarding the introduction of a risk-based approach, regarding, for example, customers and risk-based monitoring.

Since 1 January 2019, the FSA has monitored agents, and the legal framework is deemed acceptable. Relative to the scope of the FSA's operations, its monitoring of the above operations has been considerable. It includes monitoring in connection with anonymous transactions. Risk awareness is deemed to be average, cf. notifications to FIU. Finally, the publication of educational materials has increased.

Risk classification

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

Pension funds



Generally – main threats

Coinsurance

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. This is generally 2% from the employer and 2% or 4% from the employee. However, it is possible to negotiate a higher percentage for the employer and get a tax credit regarding the premium. 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. However, foreign citizens may get pension payments after they have moved away from Iceland. Pension fund payments are taxed as income when paid.

Twenty-one pension funds are operating in Iceland. Their total net assets in 2019 were ISK 5284 billion. Also, pension funds are one of Icelanders' most important savings options. On the other hand, despite the substantial level of funds in pension funds, the following characteristics of operations 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.
- 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 two years having passed since the first premium payment. However, foreign citizens can get paid when they move away from the country.
- In 99% of cases, the payments go through accounts at financial companies (no use of cash).

There are no examples of pension funds having been used in Iceland to launder money. Such would require expertise and organisation. On the other hand, two kinds of threat exist. The first is related to pension funds' loans to their members in the form of real-estate secured bonds. The risk entails the fund member's taking of a loan from the pension fund that is paid back in a short period, even with cash. Nearly all pension funds in Iceland offer loans to fund members although there are substantial restrictions on loans to them. Second, regarding payments into private property funds, the threat is that substantially high cash premiums will come in over a short period regarding an individual who has acquired the right to get the balance paid out and even has a tax domicile

abroad. Such an individual could get the balance paid out tax-free in a foreign bank before the Icelandic tax authorities' monitoring of the premium payments caught up. Thus, this individual could launder funds through the system without paying tax.

Weaknesses/mitigating factors
Risk awareness 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.

Risk classification
Considering the above, the risk of money laundering in pension funds' operations is deemed **low**.

Life insurance operations

Generally – main threats
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.

The brokerage of life insurance, or other cash-value life insurance, means presenting, offering, or 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 Art. 21 of Act no. 100/2016 on Insurance Operations. Also, eight insurance brokers are authorised to broker life and health insurance for insurance companies under Act no. 62/201 on the Brokerage of Insurance. All except three of them do so. Also, three branches of foreign life insurance companies are operating in the country.

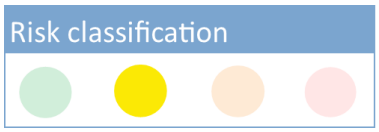
Two out of four life insurance companies offer life insurance with a cash component. Their amount in 2020 was about ISK 12.2 million. The total amount of premiums regarding other life insurance (health insurance and high-risk life insurance) was almost ISK 5.8 billion. Therefore, insurance with a cash component was nearly 0.2%. In addition, it is correct to mention that insurance brokers and branches also broker life insurance from foreign companies. The above amounts do not include premiums paid to foreign companies. Data for 2020 are not available. However, in 2019, the total amount paid to foreign companies regarding life insurance products was about ISK 13.9 billion.

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. Accessibility to this service 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. In addition, the complex arrangement of the operations, which requires considerable expertise to engage in money laundering through it, has indicated that this course is not feasible in this regard. Finally, FIU has received no notices of money laundering connected with life insurance.

Weaknesses/mitigating factors
Risk awareness 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 fund operations in Iceland.

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

Cryptocurrencies



Generally – main threats

The Act on Measures against Money Laundering and Terrorist Financing states the following definitions related to cryptocurrency operations.

- *Cryptocurrencies (virtual currency):* Any type of digital money that is neither electronic money in the sense of the Act on Issue and Handling of Electronic Money nor a fiat currency. An example of a cryptocurrency is Bitcoin.
- *Currency:* Banknotes, coins, and other currency items which central banks or other competent public bodies issue and which are accepted as legal tender.
  Custodian wallet service provider: A natural or legal person which offers services for the management of 'private keys' for virtual currency (cryptocurrencies), whether this is done through software, systems or another means of managing, keeping and transferring virtual currency (cryptocurrencies).

Amendments are also planned to provisions of the Act on Measures against Money Laundering and Terrorist Financing. These amendments entail, among other things, that the concept of cryptocurrency will be virtual assets.[38]

Service providers of transactions between cryptocurrencies, electronic money, and currencies, and service providers of digital wallets are obligated to register with FSA. 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 and Automatic Teller Machines that exchange cryptocurrencies.

In Iceland, three service providers for transactions between cryptocurrencies, electronic money, and currencies have been registered at FSA. They operate exchange markets between cryptocurrencies and currencies that run solely on the Internet. The total amount of these transactions in the country has increased greatly. In 2020 the scope was nearly ISK 1.3 billion, compared to ISK 312 million in 2018.

It is generally necessary to consider new ways and opportunities that financial technology solutions can create and ways to increase the automatic notifications from mandatory parties with measures against money laundering. Transactions in cryptocurrencies are by nature international. They flow freely across borders, and it can be difficult to figure out the origin of cryptocurrencies and an actual owner despite it generally being possible to trace the path of transfers in cryptocurrencies in blockchains. Blockchain means a chain of blocks. Each block stores coded data of transactions or other information to promote increased trust in transactions. Transactions with cryptocurrencies generally occur in telecommunications, and great speed characterises these transactions.

The greatest threat with these operations regarding money laundering is that their scope has noticeably increased in recent quarters and the methods of perpetration with criminal activities are unknown. Also, the markets for cryptocurrencies can be volatile. There are few practical examples within the country of cryptocurrencies being used to launder money.

Weaknesses/mitigating factors

Despite three parties engaging in these operations in Iceland, they are not deemed extensive. However, their weaknesses are not fully known.

Services related to cryptocurrencies in this country do not entail the use of cash. This reduces the risk of money laundering. Also, it requires considerable expertise to engage in these transactions. For example, parties must identify themselves with electronic documents and usually link the exchange market to a

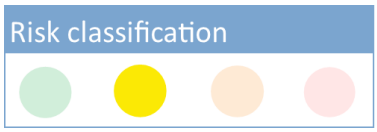
[38] https://samradsgatt.island.is/oll-mal/$Cases/Details/?id=2853

bank account. Also, there is no automatic teller machine with cryptocurrencies in Iceland.

The legal framework related to the operations of service providers is deemed satisfactory and is administered by FSA, with risk-based surveillance. This way of laundering money is generally deemed to be uncommon in Iceland, as far as known, on one hand, because of the technical know-how required and, on the other hand, because markets for cryptocurrencies can be unstable. Finally, it is worth mentioning that the FIU has received notifications of money laundering, which indicates risk awareness of parties subject to mandatory reporting.

Risk classification
The risk of money laundering that is related to service providers of cryptocurrencies, concerning the above viewpoints, are assessed as **medium.**

Operation of funds



Generally – main threats
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. It should be mentioned that most operating companies are either subsidiaries or affiliates of commercial banks and outsource second-tier monitoring to them, such as anti-money laundering and anti-terrorist financing measures, including due diligence.

Nine operating companies of securities funds have operating permits in Iceland, under Act no. 161/2002 on Financial Undertakings. These operating companies are also authorised to be operators of specialised funds, cf. the Act on Operators of Specialised Funds no. 45/2020. Also, 10 operators of specialised funds are obligated to register.

The total assets of securities funds, investment funds, and professional investor funds (specialised funds other than investment funds) were ISK 908.6 billion in 2020. They increased by 11% from the year before.

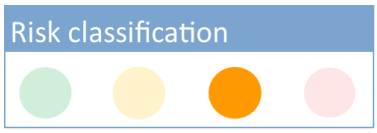
The main threat of the operations of management companies of securities funds regarding money laundering is that the amount of investments in funds is considerable. It is generally easy to engage in transactions with units in funds. Also, the operations are tied to the domestic market. Customers need a good working knowledge of the financial market to be able to launder unlawful gains through funds. There are no known examples of this.

Weaknesses/mitigating factors
Commercial banks that usually handle second-tier monitoring for management companies are generally sufficiently aware of the risk of money laundering, and monitoring of the commercial banks is strict. On the other hand, internal monitoring is not sufficiently risk-based. This can create a problem that commercial banks will employ general procedures when purchasing units in funds, i.e., that they would apply the same measures regardless of the kind of financial services involved, and the measures might therefore not be sufficiently specialised for unit purchases in funds.

A mitigating factor worth mentioning is that there are almost no cash transactions in this area, and there are no examples of notices to FIU related to money laundering in fund operations. It is also worth mentioning that the management companies have no branches in other countries.

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

Payment services



Generally – main threats

Under Art. 4 of Act no. 120/2011 on Payment Services, "payment services" means the following:

- Services enabling cash contributions into a payment account, along with other necessary measures for a payment account's operations.
- Services enabling cash withdrawals from a payment account, along with other necessary measures for the operations of a payment account.
- 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:
    a. execution of direct payments, including individual direct payments,
    b. execution of payments with a payment card or comparable device,
    c. execution of asset transfers, including payments by credit card.
- Execution of payments if funds are insured with a line of credit for a payment services user:
    a. execution of direct payments, including individual direct payments,
    b. execution of payments with a payment card or comparable device,
    c. execution of asset transfers, including payments by credit card.
- Issue of payment media and/or payment processing.
- Money remittances.
- Execution of payments if a payer grants approval for execution of the payment through telecommunications, digital equipment or information technology equipment, and the recipient of the payment is an operator of the telecommunications company, information technology system or network system that is only acting as a liaison between a user of payment services and a party delivering goods and services.

Four banks, four savings banks, one credit company, and two paying agencies are payment service providers in Iceland under Act no. 120/2011.

In connection with analysing the risk of money laundering, information was gathered on the size of the interbank system, total payment card turnover, and international transfer of funds. Information on payments to and from foreign states, including risky states, shows that most of the payments are in euros and US dollars. The main trading countries of Iceland are the United States, Britain, Germany, and Denmark. Payments to and from risky states are about 0.1% of the total payments to and from foreign states. On the other hand, there are indications that the turnover of payments through offshore companies is a substantial amount, but no separate analysis of this is available.

The main threats of these operations stem from the characteristics of payment services and the number of transactions that payment service parties execute. It is also necessary to consider new threats that financial technology solutions can create and ways to increase the automation of mandatory notification parties with measures against money laundering. One of the threats that mandatory notification parties face is related to new methods of payment. Such methods offer the speedy transfer of funds between parties since transactions increasingly occur on the Internet with less face-to-face communication. Such circumstances can create increased opportunities for anonymity. The speedy development of new electronic payment methods to do business can attract parties engaging in money laundering. Also, criminals can utilise the Internet's lack of borders since it is more difficult to monitor financial services that are provided on the Internet. Considering the above, it must be deemed that the risk of money laundering will increase with the new payment methods and new technology.

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

Weaknesses/mitigating factors

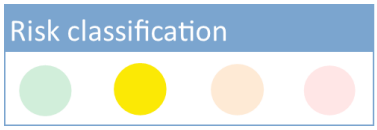
Despite the methods resorted to by parties subject to mandatory notification being generally considered acceptable, there are weaknesses, including customers' risk classification and risk-based monitoring. Furthermore, one must keep in mind that access to such services is good and the funds flow going through payment services is great.

Considering the efficiency of internal monitoring, for example, of monitoring systems with entries, payment services are less exposed to money laundering. Payment service providers do not have branches in other countries, and there are few funds' transfers to and from high-risk states. The legal framework is satisfactory, and supervisors carry out detailed risk-based monitoring of the operations. The risk awareness of parties engaging in payment services is deemed acceptable, and anonymous transactions are forbidden. Finally, it is worth mentioning that Icelandic payment service providers do not provide any of their services through agents. It is generally deemed that the use of such parties entails increased risk since agents are perhaps not as familiar as payment service providers with anti-money laundering measures.

Risk classification

Concerning existing threats and weaknesses, after considering mitigating factors, the risk related to money laundering from these operations is deemed **high**.

Trading and services for financial instruments



Generally – main threats

Mandatory operating permits for transactions and services for financial instruments under Act no. 108/2007 on Securities Transactions in Iceland, entail the following:

- Receipt and brokerage of directions from customers on one or more financial instruments.
- Execution of directions on behalf of customers.
- Assets management.
- Investment advice.
- Underwriting in connection with the issue of financial instruments and/or tenders of financial instruments.
- Supervising tenders of financial instruments without underwriting and accepting securities for trading on an organised securities market.
- Operation of a marketplace for financial instruments (MFI).

Four banks and nine securities companies are authorised to engage in transactions and services for financial instruments under the Securities Services Act no. 108/2007. All four banks offer assets management, and this is called either *assets management* or *private banking services*. Four of the nine securities companies engage in assets management, but two of them provide such services only to pension funds. The total assets managed at banks and securities companies in 2019, except for pension funds' assets, were about ISK 1348 billion.

Services related to transactions with financial instruments are offered at commercial banks for individuals. All commercial banks see to brokering instructions related to the purchase and sale of shares and bonds on domestic and foreign markets for parties other than general investors as well as five of the securities firms.

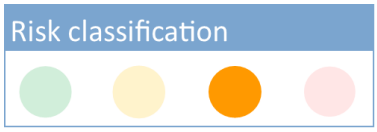
The main threats related to securities services are receiving considerable assets from customers since they often involve financially strong individuals and legal persons wanting to invest in financial instruments to increase their profit. Such customers are often more risk-seeking than other bank customers, and their risk awareness is limited. High amounts go through parties offering securities services. Accessibility to these services is also relatively good, and investment in financial instruments generally does not demand great expertise. On the other hand, there are extremely few notifications to FIU on money laundering in these operations.

Weaknesses/mitigating factors

Despite the methods resorted to by parties subject to mandatory notification being generally considered acceptable, there are weaknesses, including customers' risk classification and risk-based monitoring. The instruction of authorities has increased. Also, this market has certain basic legal requirements regarding anti-money laundering measures. In addition, the transactions are almost exclusively engaged in here in Iceland. Finally, anonymity is not allowed, and there are almost no cash transactions. The supervisors' monitoring is risk-based.

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

Issue of electronic money



Generally – main threats
Act no. 17/2013 on the Handling and Issue of Electronic Money defines electronic money 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. According to information from banks, savings banks, and credit companies, they issue electronic money only to named parties. 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.

In Iceland, the bigger commercial banks, savings banks, and credit companies have issued electronic money. All these parties issue prepaid payment cards, but only the banks and savings banks also issue "gift cards". In addition to the above, an electronic money company operates in Iceland. However, it has not opened transactions to the general public. In 2020, electronic money for ISK 28.8 billion was issued. Of this amount, gift cards for ISK 3.3 billion were issued.

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.

There are very few notices to FIU regarding transactions with electronic money.

Weaknesses/mitigating factors
Despite the methods resorted to by parties subject to mandatory notification being generally considered acceptable, there are weaknesses, including customers' risk classification and risk-based monitoring. 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 authorities have increased the publication of educational materials. Finally, transactions with electronic money are not anonymous; amounts are restricted, and the issue of such cards is tied to operations within the country.

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

Foreign exchange

Generally – main threats
Foreign exchange entails exchanging domestic currency for foreign currency, foreign currency for domestic currency, one foreign currency for another, or charge accounts, which are the equivalent of foreign currency being paid or received under Art. 1 of Act no. 87/1992 on Foreign Exchange.

Act no. 161/2002 on Financial Undertakings authorises foreign exchange for lending institutions. Also, the purchase and sale of foreign exchange occur at money exchange services that are subject to mandatory registration under Art. 35 of AML Act at FSA. The definition of a money exchange service in Art. 3 (8) of AML Act is as follows: "*a business activity which, in the way of business, engages in buying and selling domestic and foreign currency*". Rules no. 535/2019 on the registration of money exchange services and service providers of cryptocurrencies and digital wallets also apply to the operations of money exchange services.

In Iceland, commercial banks and savings banks engage in foreign exchange in addition to money exchange services. There is one registered money exchange service in the country that began operating in June 2019.

The percentage of foreign customers varies, depending on which financial undertaking is involved, but it ranges from 3% to 14%. Of foreign customers, the proportion of EEA citizens is in the range of 67% to 85%. The number of foreign customers involved has increased, but the percentages of customers from the EEA area are relatively similar, as well as the percentage of customers from high-risk states which is about 0.3%. The portion of foreign customers of the only money exchange service in Iceland is about 82%. Also, about 1.5% of the service's customers are from high-risk states.

In 2018 the turnover of cash transactions in foreign exchange in the country was close to ISK 83.6 billion, and in 2019 the same turnover was about ISK 87.1 billion. In 2020, the turnover contracted substantially to about ISK 23.3 billion. The global coronavirus pandemic is a likely explanation of this contraction.

The main threats from foreign exchange operations are good access to the services and a high proportion of cash transactions making it possible to conceal the source of assets. Another threat, to a certain degree, is anonymous transactions by the same customer, e.g., when the individual does not have an Icelandic ID number. There are indications that transactions of this kind occur in an organised manner. This is examined considering the number of remittances in the country and how easy it is to transport cash across borders. An assessment of threats indicates that it is rather common for criminals to use foreign exchange to launder money. It is also easy to access these services, and there is no special expertise or technical know-how required.

Notices to FIU of suspicious foreign exchange transactions are rather common.

Weaknesses/mitigating factors
Usually, transactions in foreign currency are not anonymous. Nevertheless, they can be when the amounts are low. FSA's monitoring and findings indicate the presence of weaknesses in internal monitoring, especially regarding customers' risk classification and risk-based monitoring. Also, the risk awareness of parties obligated to notify in this market varies.

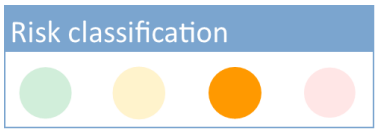
The legal framework for foreign exchange is deemed acceptable, and the monitoring of parties engaging in foreign exchange transactions is thorough. Finally, authorities have increased the publication of educational materials in this issue category.

Risk classification
Considering the main threats and weaknesses, after taking into account mitigating factors, this risk component is deemed **high**.

3.5 SPECIALISTS

The following sections discuss specialists. Specifically included are attorneys, accountants, estate agents, ship brokers, bookkeepers, and car salesmen. In addition, this report will examine whether there is risk in Iceland 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 bookkeeping 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 unaware that their services are being misused in such a manner, or that they are fully aware of this and take fees for it. Information from supervisors, the police, FIU, DTI, and appropriate legislation especially supported the analysis.

Attorneys



Generally – main threats

Law firms, attorneys and other specialists are parties subject to mandatory reporting in the meaning of the Act on Measures against Money Laundering and Terrorist Financing when they:

- See to or represent their clients in any kind of financial or real estate transactions.
- 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.
- Procure capital necessary to found, operate or direct companies or assist with the founding, operating or managing of funds, companies 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.

There are 1070 attorneys in Iceland. Part 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 730, and the number of law firms is 203. In addition, 98 attorneys practise under their names. The size of law firms can vary considerably, from one attorney to large law firms where more than 40 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 Art. 12 of the Act on Attorneys no. 77/1998, which deals, among 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.

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 Act on Measures against Money Laundering and Terrorist Financing. 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.

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.
- 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.

According to information from supervisors, there are indications that some attorneys do not fulfil the conditions of the Act on Measures against Money Laundering and Terrorist Financing. For example, law firms, attorneys, and other specialists do not sufficiently execute due diligence on customers, do not conduct risk-based monitoring, do not work according to their risk assessment and do not legally preserve documents. The above practices enable the analysis of suspicious transactions and control of risk under the Act on Measures against Money Laundering and Terrorist Financing and the Freezing Act no. 64/2019. There are also examples where attorneys are connected with cases being handled by authorities, both the police and DTI, because of various kinds of help that can relate to the assistance of criminal activities. There is also an example of an attorney being convicted under a punitive provision on money laundering of Art. 264 of GPC, cf. Landsréttur Appeal Court judgement on 11 October 2019 in case no. 725/2018.

Finally, FIU received very few notices of suspected money laundering in 2020 as well as the previous year. This is noteworthy, considering the extent of these operations.

Weaknesses/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.

IRC's Money Laundering Division maintains surveillance by checking that attorneys fulfil their duties under the Act on Measures against Money Laundering and Terrorist Financing. From the entry into force of the act through the end of 2020, there have been 53 checks of attorneys and law firms. These checks cover nearly 500 working attorneys in Iceland. The checks have revealed weaknesses and their failure to satisfactorily fulfil their duties under the provisions of the Act on Measures against Money Laundering and Terrorist Financing in addition to the Freezing Act.

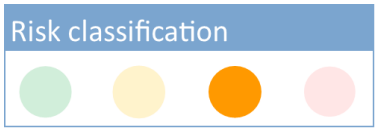
It must also be said that despite not monitoring this issue category, the Icelandic Bar Association has set rules of guidance for its members, and IRC's Money Laundering Division has held informative lectures for attorneys as well as participated in teaching a course on litigation rights for district courts.

The few notices of suspicion regarding attorneys sent to FIU indicate that risk awareness is still lacking to some degree. On the other hand, attorneys' risk awareness has been increasing with the advent of active monitoring in the last two years and the issuance of educational materials and informative lectures under governmental auspices.

Risk classification

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

Accountants



Generally – main threats

Accounting firms, accountants, tax advisers, 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 Act on Measures against Money Laundering and Terrorist Financing. The discussion below is solely about accountants.

Under Act no. 94/2019 on Accountants and Accounting, all parties except accountants and accounting firms are forbidden to use the words accountant and accounting in their titles or business name, cf. Art. 6 (1) of the act. Art. 4 (1) (4) 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 Art. 3 (1) 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. Art. 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. Art. 8.

Accounting firms shall have a work permit and be on the Register of Accountants, under Art. 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 or the Faeroe Islands, 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.

There are 312 accountants in Iceland and 38 registered accounting firms. 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.

The Accountants' Council sees to monitoring that accountants and accounting firms work under Act no. 94/2019, cf. Art. 33 of the act.

As of 1 January 2019, the IRC's Money Laundering Division has monitored whether accountants follow the instructions in the Act on Measures against Money Laundering and Terrorist Financing.

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 Act on Measures against Money Laundering and Terrorist Financing. 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 addition, there is always a risk that an accountant will be too dependent on his client.

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 the beneficial ownership.
- Services with related companies/parties.
- Assistance with the founding of 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.

The last two years, accountants' monitoring of money laundering has been the responsibility of IRC's Money Laundering Division. In addition, the Accountants' Council sees to quality control, for example, where details regarding anti-money laundering and anti-terrorist financing are checked. Overall, this monitoring indicates fairly close adherence to the Act on Measures against Money Laundering and Terrorist Financing. Despite this, there are indications that accountants are not sufficiently cautious when endorsing accounts and doing due diligence, that they skirt past parties with political connections, related parties, and reputations when analysing whether suspicious transactions are involved. There are also examples where accountants are connected with cases being handled by authorities, both the police and DTI, because of various kinds of help that can be related to assisting criminal activities.

FIU receives few notices from accountants.

Weaknesses/mitigating factors

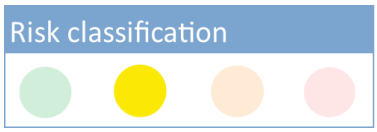
There is an inherent risk within the profession that strong defences cannot fully prevent. In this regard, one must keep in mind the interests of accountants' operations – i.e., the auditing of financial statements – because nearly all companies have a financial purpose. There are also weaknesses in the profession's operations. On the other hand, there are mitigating factors like active monitoring, educational materials, ample qualification requirements, regular quality control, a code of ethics, and the risk of losing their accountants' licence.

The monitoring of accountants has been quite acceptable as well as their legal framework. The few notices of suspicion from accountants received by FIU indicate that they still lack risk awareness, to some decree. On the other hand, 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

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

Bookkeepers



Generally – main threats

Accounting firms, accountants, tax advisers, and persons who provide bookkeeping services for third parties in exchange for remuneration are parties subject to mandatory reporting in the meaning of the Act on Measures against Money Laundering and Terrorist Financing. The following discussion pertains only to parties keeping books or performing accounting services.

According to Art. 43 (1) of Act no. 145/1994 on Accounting, only those registered on the list of certified bookkeepers (supervised by MoII) may call themselves certified bookkeepers. People seeking certification as a bookkeeper and registration on the list shall fulfil the conditions set out in Art. 43 (2) of the act, i.e., being domiciled in Iceland, within the EEA Area, within a member state of the Free Trade Association of Europe or the Faeroe Islands, be legally competent and in possession of his estate, and have passed an examination under par. 3 of the same provision. The regulation on the courses and examination for certified bookkeepers no. 649/2019 provides details on the examination for the certification of bookkeepers.

About 1200 certified bookkeepers are on MoII's register, and they 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. One can also assume that some of those on the ministry's register do not work in bookkeeping even though they have qualified to do so.

The interest group for those having rights as certified bookkeepers is The Association of Certified Bookkeepers. It has 523 members, and its purposes include maintaining and increasing the members' knowledge, cf. Art. 4 of the association's Articles of Association. The association has requirements on continuing education and organises courses. Membership in the association is not mandatory.

As of 1 January 2019, the IRC's Money Laundering Division has monitored whether members working as bookkeepers or performing bookkeeping services for remuneration follow the instructions on the measures to counteract money laundering and terrorist financing.

The main threats in bookkeepers' operations are that those doing bookkeeping or performing bookkeeping services for remuneration could, knowingly or unknowingly, participate in lending unlawful transactions or operations a lawful appearance and that bookkeepers' involvement could be requested to cover a trail of money or unlawful gains for tax avoidance.

The transactions entailing increased risk are mainly:

- Transactions with parties in a risk group.
- Services with related companies/parties.
- Customers having operations engaging heavily in cash transactions.

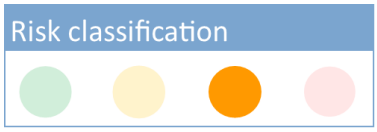
Weaknesses/mitigating factors

There is an inherent risk in the field regarding existing threats, and, in many instances, precautions against them are not sufficiently strong. There are also various weaknesses within the operations.

Monitoring of bookkeepers is the responsibility of IRC's Money Laundering Division. Overall, this monitoring indicates fairly close adherence to the Act on Measures against Money Laundering and Terrorist Financing. Despite this, there are indications that bookkeepers do not satisfactorily carry out a risk assessment of their operations, do unsatisfactory due diligence to check beneficial ownership and ignore parties with political ties, related parties, and reputation when analysing whether suspicious transactions are involved. FIU has received few notices of suspicious transactions from bookkeepers, which indicates, to some degree, that they still lack risk awareness. On the other hand, the occupation's risk awareness has been increasing with additional educational materials and active monitoring. Authorities have organised the publication of educational materials in the issue area and held informative meetings to increase knowledge of the issue area.

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

Estate agents



Generally – main threats
In Iceland, a licence for estate agency operations is mandatory. Furthermore, only estate agents certified by a district commissioner may represent others in purchasing, selling, or exchanging real estate, cf. Art. 2 of Act no. 70/2015 on the Sale of Real Estate and Ships. An exception to this is that people can sell their real estate without the involvement of an estate agent.

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 monitors that the conditions of certification are fulfilled, both upon the granting of the permit, its surrender, and reissue. The law allows the closing of an office if the operations entail the sale of real estate by an unlicensed party.

Since 1 January 2019, the IRC's Money Laundering Division has monitored whether estate agents follow the instructions in the Act on Measures against Money Laundering and Terrorist Financing. The Estate Agents Surveillance Committee monitors estate agents' work procedures.

There is an organised interest group for estate agents, The Estate Agents' Association. Membership in this association is not mandatory, unlike what applies to attorneys and accountants. Of the 530 certified estate agents, 312 belong to the association. The association sees to its members' education, including on money laundering, and sets a code of ethics.

At the start of 2021, there were 530 estate agents. According to Statistics Iceland, the total real estate transactions in 2020 were ISK 667 billion in nearly 13,900 contracts of sale. The year before, there were 12,200 registered contracts of sale, worth ISK 460 billion.

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. It is easy to conceal ownership when real estate is transferred into a company founded for the sole purpose of holding the real estate involved. Known ways include selling an asset at a price below or above the going price, paying part of the price in cash, or even so that part of the payment is nowhere stated, as well as when the same asset changes owners often. The main threats are:

- The scope of real estate transactions is great.
- Payment of the purchase price with cash or liquid assets.
- Real estate transactions where a company is a buyer or seller.

Weaknesses/mitigating factors
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.

Monitoring of estate agents' operations regarding measures against money laundering and terrorist financing is now the responsibility of IRC's Money Laundering Division, and the monitoring has been active since the entry into force of the Act on Measures against Money Laundering and Terrorist Financing. Considering the checks run by IRC's Money Laundering Division, there are indications that estate agents do not satisfactorily carry out due diligence, which is the basis for analysing whether suspicious transactions are involved. FIU received one notice of suspicion from estate agents in 2020. Considering the number of real estate transactions, one can argue that the field still lacks risk awareness. However, measures have been

taken to increase estate agents' risk awareness, with increased instruction and the publication of educational materials. Also, informative meetings on the issue category have been held, specifically intended for estate agents.

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

Ship brokers

Generally – main threats
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.

Less than 10 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 boats.

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 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.

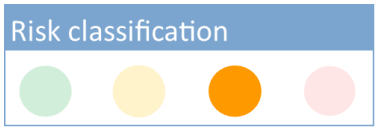
The Icelandic Transport Authority publishes the Icelandic International Ship Register, which contains the registration of ships subject to mandatory registration, including initial registrations, re-registrations, de-registrations, etc. For this reason, the Icelandic Transport Authority also monitors 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.

There are no known examples of brokers being used to launder money. Few parties are seeing to ship brokerage, and the number of transactions is small. Threats in the operations are, therefore, not very high, given the current environment.

Weaknesses/mitigating factors
The main weaknesses related to ship brokerage are the lack of ship brokers' risk awareness and the risk that conditions of the Act on Measures against Money Laundering and Terrorist Financing will not be fulfilled, particularly regarding satisfactory due diligence.

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

Car dealerships and car dealers



Generally – main threats

Act no. 19/2020 amended various acts regarding the issuance of permits. One of the amendments involved Act no. 28/1998 on Retail Work. It revoked the certification of car dealers. Therefore, everyone is now free to engage in transactions with cars. Despite the above, Act no. 28/1998 applies to the sale of used vehicles with mandatory registration for business purposes. Act no. 50/2000 on the Sale of Goods generally pertains to a first-hand transaction with a vehicle. Regulation no. 44/2003 on the duty to inform in transactions with used vehicles contains detailed information on the requirements for minimum information to be provided in transactions with 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.

Act no. 96/2020 amended the Act on Measures against Money Laundering and Terrorist Financing to include the operations of car dealerships and car dealers. Monitoring regarding the measures has therefore recently begun at IRC's Money Laundering Division.

There is an interest group of employers selling vehicles, products, and services related to them, i.e., 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. There are 116 members, and they span a broader area than just car dealerships and car dealers. Involved here are car repair shops, tyre repair shops, painting and body shops, car workshops, and spare parts sales. Operations of the motor trades are extensive, and their total turnover in 2019 was ISK 146.4 billion.[39]

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.

Known ways to launder money, where cars are the object of transactions, include acquiring cars to pay off debts and paying the purchase price of a car with cash. The main threats of the above operations are:

- The number of car transactions is great.
- Laundering unlawful gains through car transactions require little expertise.
- Payment of the purchase price with cash.
- Car transactions where a company is a buyer or seller.
- Car transactions where a car is used as part of the payment for paying off debt.

Notices to FIU of suspected money laundering with car transactions are nearly unknown.

Weaknesses/mitigating factors

The field entails considerable inherent risk. In addition, threats and weaknesses are inherent in the car trade.

Mandatory notices from car dealerships and car dealers are recent. However, before then, there was little monitoring of the operations. The observations of IRC's Money Laundering Division have indicated that car dealers are still not sufficiently aware of their duties regarding measures against money laundering. For these reasons, one can argue that the field still lacks risk awareness.

Risk classification

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

[39] *Árbók bílgreina 2020. Hagtölur um íslenskar bílgreinar (Motor Trades Yearbook 2020. Statistics on the Icelandic Motor Trade)*. The Research Centre for Retail (RCR) and the Icelandic Federation for Motor Trades and Repairs, Reykjavik 2020, p. 3.

3.6 GAMBLING

Art. 183 of GPC forbids gambling in Iceland, and anyone gambling or betting as a business or urging others to participate can be fined or imprisoned for up to 1 year. Despite this, various operations in the country having the characteristics of gambling and/or betting may be allowed. There the main operations worth mentioning are lotteries, lotto, bingo, betting, and slot machines. One of the main characteristics of the above operations is that all profit shall go to charities. 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 in the same context. During the analysis, information from supervisors, police, FIU, DTI, and appropriate legislation especially provided support.

Sweepstakes

Risk classification

Generally – main threats

Iceland offers two kinds of sweepstakes – *Lengjan* and *1x2*. Both games are connected with sweepstakes since people guess the outcome of sports events, e.g., the winner, number of goals or the last goal. 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 are 207. 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, for 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 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 are traceable.

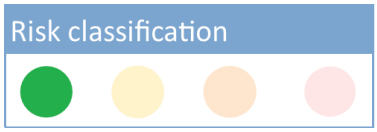
FIU has received very few notices regarding suspicion of money laundering connected with sweepstakes. The police have investigated few cases related to sweepstakes, and there have been no cases concerning tampering with results.

Weaknesses/mitigating factors

One weakness is that these operations are not subject to mandatory monitoring under the Act on Measures against Money Laundering and Terrorist Financing. On the other hand, betting operations are uniform and only allowed for Icelandic sweepstakes, cf. Act no. 59/1972 on Sweepstakes. Winnings exceeding a low amount are only paid out at operators, and information on National IDs and bank accounts is required to get the payment. The above arrangement consequently enables an operator to systematically monitor the amount 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, risk awareness has increased, and authorities have also organised the publication of educational materials on gambling.

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

Lotteries



Generally – main threats
Lotteries are 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 no. 38/2005 on Lotteries. On the other hand, special laws cover lotteries, e.g., Act no. 13/1973 on the Lotteries of the University of Iceland, Act no. 16/1973 on Elderly Fishermen's Home, and 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.

The total turnover in 2020 for the three lotteries was ISK 3.5 billion and about ISK 2.1 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.

Statutes determine the organisation of these lottery operators, and there is thorough monitoring of their drawings and finances.

Ticket lotteries operate under the Law on Lotteries
Such lotteries must apply to the District Commissioner of South Iceland for a permit. The permit may 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 2019, 39 permits were issued, and in 2020, 33 permits.

Winnings in these lotteries are only products or services, such as automobiles, trips, household appliances or other inexpensive products. The total turnover of these lotteries in 2019 was about ISK 370 million, and ISK 139 million was paid in winnings. Final information on winnings in 2020 is not available. These lotteries must submit reports or accounts on their operations to the district commissioner's office, which sees to monitoring the Law on Lotteries.

These operations seem to entail no threats. Lotteries appear not to be a desirable way to launder money because of the protective measures in place for lotteries under special acts, 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. Regarding other lotteries, winning is also based on luck, and the prizes are only products where the biggest prizes can only be cars, but the value of other prizes is generally much lower. 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/mitigating factors
There are no particular weaknesses in these operations. Also, supervisory control has been established; risk awareness has increased, and authorities have organised the publication of educational materials on gambling.

Risk classification
Considering the above, the risk regarding lotteries is deemed **low**.

Lotto

Risk classification

Generally – main threats

Three kinds of lotto operate in Iceland: Lotto, Vikingalotto, and Eurojackpot. Participants choose 5 figures (Lotto), 6 figures (Vikingalotto) 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 getspá*, which operates under the Act on Numbers Lotteries no. 26/1986. The National Olympic and Sports Association of Iceland owns 46.67% of *Íslensk getspá*; the Organisation of Disabled People in Iceland owns 40%, and the Youth Association of Iceland owns 13.33%. The profits of *Íslensk getspá'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.

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. The statistical probability of a first prize is low, cf. Art. 13 of Regulation no. 1170/2012 on Numbers Lotteries, as amended. Winnings other than for the first prize are generally low. The total turnover of lotto games in 2020 was ISK 5.5 billion and the market purchase value of winnings was ISK 2.6 billion.

Even though the accessibility is easy, and requires no special knowledge to participate, 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. Therefore, these operations seem to entail no particular 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/mitigating factors

Despite there being no threats in these operations, it is worth mentioning that it is deemed a weakness that these operations are not subject to mandatory monitoring under the Act on Measures against Money Laundering and Terrorist Financing. 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.

Risk classification

The risk of money laundering related to lotto is **low**.

Collection boxes and lottery machines

Generally – main threats

The operators of collection boxes are *Íslandsspil ehf*. and the University of Iceland Lottery (UIL). Their operations build on statutory authorisation, cf. Act no. 73/1994 on Collection Boxes and Act no. 13/1973 on the University of Iceland's Lottery. 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 collection boxes or lotteries in Iceland.

It is only possible to play for cash in the collection boxes or for winning tickets. It is possible to load a maximum of ISK 100,000 at a time in a single collection box. 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.

Neither *Íslandsspil ehf*. nor UIL have a special requirement regarding operators' reputations. There are very few instances where agreements with operators have been revoked, and this was because of arrears or violations of rules, e.g., when youths have gotten to play the boxes. There are no rules on the amount of winnings at gaming sites, i.e., whether payment is made with cash or digitally, but it is commonest for winnings to be paid out in cash. No due diligence is done on winners when a gaming site pays out winnings except for requiring a domestic bank account and National ID when winnings are paid digitally. No maximum has been defined for the amount of winnings that gaming sites may pay out, but if substantially high winnings are involved, and a gaming site does not have that much money, the winner must redeem the winnings from the operator, which pays about 80-90% of winnings digitally.

There are 25 gaming sites for the University of Iceland (UI) lotto machines. They are mainly in the Reykjavik Metropolitan Area and are either bars or special casinos. There are 495 lottery machines in use. *Íslandsspil ehf.* has 58 gaming locations with collection boxes. They are mainly in the Reykjavik Metropolitan Area and are either bars or special casinos. There are 377 collection boxes in use.

The total turnover in 2020 of collection boxes was about ISK 7 billion, and the winnings paid out the same year were about ISK 4.9 billion, despite the points of sale of collection boxes having been closed most of the year.

There is a high risk that collection boxes can be utilised for money laundering, and there are indications of such. The accessibility to collection boxes is considerable, and the only way to pay is with cash. The main threats of the operations are:

- The scope of risk regarding both the number and turnover of collection boxes.
- The use of cash.
- The possibility of loading in cash and then printing out lottery tickets without playing or playing a few games.
- The accessibility of gaming sites and other places to purchase lottery tickets.
- The players' anonymity.

The number of notices to FIU has increased in the last two years, and the suspicion is that this channel has been repeatedly used for money laundering.

Weaknesses/mitigating factors

Money laundering with collection boxes does not require expertise, special preparation, or cost outlays. Not requiring collection box sites to have a good reputation is a serious weakness because of their accessibility for purchasing lottery tickets. It is deemed a weakness that monitoring established for these operations covers only those authorised to operate the data libraries but not authorised dealers. However, there are indications that risk awareness has increased, given the increase in notices to FIU. Finally, the authorities have organised the publication of educational materials on gambling.

Risk classification

According to the above, the risk of money laundering in connection with the operations of collection boxes and lottery machines is **high**.

Gambling on the Internet

Generally – main threats

Gambling on the Internet means all kinds of gambling done on the Internet without personally meeting dealers. The gambling available electronically on Icelandic web pages is lotteries, betting and lotto as described under these headings.

To participate in the gambling, a player must identify himself specifically, cf. the following:

- Purchase of lottery tickets from UI, DAS and SIBS goes through the operator's website. Buying tickets requires opening access to a valid National ID and connecting a bank account or payment card associated with the National ID involved. Winnings are only paid out to a registered ticket owner.
- It is possible to place bets and participate in lotto through an operator's homepage. A player must open a gaming account with a valid National ID (it is possible to register a National ID only once) and link a payment card to the gaming account associated with it. Winnings are only paid out to the party having the relevant National ID.

Icelanders have access to foreign gambling websites, for it is possible to find all kinds of gambling on the Internet whether it involves poker, gambling, lotto, or collection boxes. Information on the scope of such participation is not available. However, considering that 99% of Icelanders between the ages of 16 and 74 use the Internet (which is the most usage in European countries), one can infer that it is likely that some of them engage in gambling on foreign websites. Also, those gambling websites are not subject to Icelandic law and are beyond the jurisdiction of the Icelandic Government.

In assessing the threat of gambling on the Internet, one may consider that it is unlikely that gambling accounts are bought and sold since they do not entail direct value, and since an evaluation of them can only occur by transferring money into a bank account or credit card owned by the National ID no. registered to the gambling account. One must also consider that there is little likelihood that participants can play anonymously. Finally, there are no indications that gambling through Icelandic websites has been used to launder money, and no cases of this nature have involved the police.

Weaknesses/mitigating factors

The main weaknesses related to gambling on foreign websites involve winnings that are not declared as tax bases and are therefore directly connected with tax fraud as a predicate offence. Furthermore, there has been no analysis of the scope of gambling on foreign websites, and there is no monitoring of it.

Risk classification

Considering all of the above, the risk related to gambling on the Internet is deemed **low**.

3.7 TRADE AND SERVICES

The following two sections discuss the assessed risk of money laundering when it comes to trade and services. This involves a market, where using cash in great quantity may generally be anticipated. On one hand, goods and services are generally examined. On the other hand, there is a separate discussion of the nature and characteristics of precious metals and gems. The analysis relied especially on information from supervisors, the police, FIU, and appropriate legislation.

Precious metals and gems

Risk classification

Generally – main threats

Here in Iceland, the retail, wholesale and design of imported precious metals and gems occur. In most instances, gems are bought from recognised parties in Europe that have undergone the Kimberley Process Certification Scheme that requires a certificate of origin for diamonds. In addition, it is forbidden to import uncut diamonds to Iceland from conflict areas.

Act no. 77/2002 on products processed from precious metals, defines such metals as follows: "[G]old containing 375 thousandths or more of pure gold, silver containing 800 thousandths or more of pure silver, platinum containing 850 thousandths or more of pure platinum, and palladium containing 500 thousandths 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 making gold and silver are protected trades, cf. Art. 1 of the Regulation on Protected Trades no. 940/1999, cf. par. 1 of Art. 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, and the Consumer Agency monitors this. The market in Iceland, regarding sales of precious metals and precious gems and other products sold in jewellery stores, is deemed small, relative to the gross national product.

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 smuggle because of their size. The Act on Measures against Money Laundering and Terrorist Financing applies only to sellers of precious metals and precious gems where the payment amounts to €10,000 or more and is in a lump sum or more instalments that appear connected. However, there are no indications of unlawful transactions with these products.

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. In addition, FIU has received no notices since the last risk assessment, and the police have generally not been involved much in cases related to this product category.

Weaknesses/mitigating factors

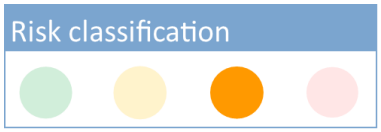
Iceland does not have restrictions on the use of cash. Therefore, there may also be a risk that sellers and buyers will be conscious or unconscious participants in money laundering if such goods are bought and sold for cash. However, dealers' replies indicate that the proportion of cash transactions in Iceland is low. Also, the monitoring of dealers on the market is complicated since dealers 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 one-person operations and

may find it difficult to fulfil their duties under the Act on Measures against Money Laundering and Terrorist Financing and do not even have sufficient knowledge in that field. The above can lead to due diligence not being executed under the Act on Measures against Money Laundering and Terrorist Financing 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. Finally, 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 under the auspices of the Federation of Trade and Services to review the duties of mandatory-notice parties.

Risk classification
In light of the above, the risk of money laundering in the market for precious metals and precious gems is deemed to be **medium**.

Products and services



Generally – main threats
Coming under consideration here are both the purchase and sale of goods and services. A market is involved, where it is generally expected that cash will be used in greater measure than in other markets. Regarding the legal framework, Act no. 50/2000 on the Sale of Goods applies to the extent that no other law directs otherwise. However, laws also apply to exchanges, as relevant. The act also applies to purchase orders and international purchases, with the special rules entailed in them. Regarding the purchase of services, Act no. 42/2000 on purchases of services applies. Art. 1 of the act covers any kind of agreement on the purchase of services offered to consumers for business purposes against payment, and when services are provided, they include the work and services detailed in the provision.

Act no. 48/2003 specifically governs consumer purchases. It applies to such purchases to the extent that another law does not direct otherwise. Consumer purchases mean the sale of an item to a consumer when a seller or his agent derives work from the sale, while a consumer, in the meaning of the act, is someone who buys an item in his capacity. Regarding trade for business purposes, the Merchants and Trade Act no. 28/1998 applies, whether the work is done on one's account or another person's account or in one's name or another person's name. “Trade” means any kind of mediation regarding the transfer of a direct ownership right in goods. However, the act does not cover special provisions of other acts setting special conditions regarding specific products or industries.

According to Statistics Iceland, the total import of goods to Iceland in 2020 was ISK 771 billion. Service is not specifically defined. However, postal, telephone, other personal, social, and financial services amounted to nearly ISK 230 billion in 2020.

Iceland has no limitations in force on cash transactions. Also, cash in circulation in Iceland has increased, despite the increase in digital payment arrangements, and cash has not necessarily increased in transactions.[40] The European Union's risk assessment states that although cash is not consumers' main payment medium, it is still the main tool of criminals for money laundering.[41]

In markets where transactions using cash are frequent, there is a risk that criminals will try to launder profits from illegal activities by mixing such funds into lawful operations occurring during the sales of products and

[40] *Fjármálainnviðir ,* 7th monograph 24 June 2019.

[41] *Supranational Risk Assessment of the Money Laundering and Terrorist Financing Risks affecting the Union.* The European Union, Brussels 2019.

services. In that regard, it must be kept in mind, on one hand, the ties between such transactions and tax fraud as a predicate offence and, on the other hand, the use of cash, discussed in other sections of the risk assessment.

The main threat of money laundering stemming from a market with goods and services is that criminals and parties related to organised crime will establish operations or utilise connections in the field of trade or services to launder unlawful gains or use them to buy products or services. It is usually deemed easy for criminals to move ill-gotten money into circulation through trade and service operations, for example, through the operations of companies.

Figures from CBI show that the use of cash as a percentage of the gross national product has more than doubled since 2008. Since 2010, the percentage has stayed between 2% and 2.5%. Inevitably, an assessment of threats in trade and service operations is linked with the use of cash, and these factors are intertwined to a great degree since there are few restrictions on the use of cash, cf. the discussion in the risk assessment of cash in Iceland. Trade and service operations make it easier for criminals to enter cash and anonymous entries under €10,000 since there is seldom a requirement of the traceability of entries. Despite this, few notices are sent to FIU.

Weaknesses/mitigating factors

Since the beginning of 2019, the monitoring of anti-money laundering measures involving cash transactions in one or more related €10,000 payments or more has been the responsibility of IRC's Money Laundering Division. It is thought that the following risk could exist: that dealers and service providers, particularly smaller parties, will not carry out a risk assessment or due diligence or adhere to their obligations when the use of cash of more than €10,000 is involved since the same duties do not apply to them as when the use of cash under the same amount is involved. Also, the dealers' answers to survey questions and monitoring procedures show clear signs that there is little use of cash.

Despite the above, risk awareness amongst parties in the market has increased. Furthermore, authorities have published educational materials on operations where the use of cash is great. In addition, informative meetings have been held for parties in the market.

Risk classification

Considering the above, the risk of money laundering in the field of trade and services is deemed to be **high**.

3.8 OTHER

The following section examines the risk of money laundering regarding ID numbers that foreign citizens can have issued regarding special interests in Iceland. The analysis and risk classification relied on answers to questionnaires sent to relevant parties, information and reports from institutions and other governmental parties, information and reports from institutions and other public sector bodies, information from the police, FIU and DTI, and appropriate legislation.

ID numbers for foreign citizens

Risk classification

Generally – main threats

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. On 1 January 2020, a new comprehensive law, Act no. 140/2019, entered into force on the registration of individuals. The law legalised, for the first time, ID numbers for foreign citizens and the application process for it. The law 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. Now, financial institutions and other private parties can no longer establish such an ID number.

Those utilising ID numbers for foreign citizens are:

- Foreign employees receiving wages in Iceland for temporary work.
- Foreign students.
- Employees of embassies.
- Individuals sitting on boards of directors of Icelandic companies.
- Individuals accepting payments of some kind from Iceland, e.g., because of pensions.

All instances, therefore, involve individuals not domiciled in Iceland. No rights are attached to ID numbers for foreign citizens, and they therefore only facilitate people's access to specified services like healthcare services. Individuals requiring ID numbers for foreign citizens must turn to a public party to be an intermediary for the application for the ID numbers, such as IRC or an educational institution, 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. There are instances when the person involved never resides in Iceland and has never come to the country.

According to the register of ID numbers that Registers Iceland keeps, the number of applications has decreased since 2017. The number of applications was more than 13,000 in 2017, more than 11,000 in 2018, and about 7200 in 2019. Registers Iceland received only about 1500 applications in 2020, and the reason for this great decrease of applications that year were probably twofold. First, the COVID-19 global pandemic greatly affected the flow of people between countries. Additionally, the number of jobs decreased. Most applications for ID numbers for foreign citizens is because of temporary participation in the job market. However, increased unemployment and less available tours have reduced the number of individuals coming to the country to work temporarily. Second, it may be deemed likely in general that the innovation in the law entering into force on 1 January 2020 that only public parties can apply for ID numbers for foreign citizens has reduced the number of applications.

By far the most applications for ID numbers for foreign citizens regard EEA citizens, specifically those from countries in Eastern Europe. There are few applications regarding individuals from states deemed to be risky states (less than 1%). Most applications regard employment – 84% in 2019 and 57% in 2020. In 2018 and 2019, the biggest group of applicants was financial institutions and employers. In 2020 the biggest group was Iceland Revenue and Customs and Registers Iceland. The reason for the number of applications from Registers Iceland in 2020 is that the institution has had to be the intermediary regarding businesses and pension payments since banks are legal persons and can therefore no longer apply for ID numbers for foreign citizens. The percentage of rejected applications was more than 7% in 2018, about 6% in 2019 and nearly 19% in 2020. Also, there are known instances of applications for ID numbers for foreign citizens, based on suspected forged identity papers in 5-9% of rejected applications.

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 individual with an ID number for a foreign citizen can, for example, establish a bank account, acquire electronic identity papers, found a company, and purchase real estate. Thus, there are known instances where ID numbers for foreign citizens have been used to found and operate private limited companies, and ID numbers for foreign citizens are also registered for just under 500 pieces of real estate in the country.

Considering how the application for and issue of an ID number for a foreign citizen is set up, it is worth looking into cases involving the forgery of identity papers. Information from the police in Sudurnes on people presenting forged identity papers upon arrival in Iceland shows that instances of this have increased at least since 2013 and possibly as far back as 2007. Furthermore, 2019 was a record year for forged identity cases. There were 100 such cases that year. The higher number of passengers passing through the flight terminal partially explains this. However, other explanations come from external factors. The number of cases (39) involving forged identity papers in the air terminal in 2020 reflects the extraordinary decrease in the number of passengers going through the Keflavik Air Terminal that year. However, the interesting aspect of the number of cases involving forged identity papers was how high it was relative to the little traffic through the terminal. Finally, there has also been an increase in the number of forged identity papers cases coming up inside the country, including in Registers Iceland and the police in all parts of the country.

The issue of ID numbers for foreign citizens, based on unsatisfactory information, poses a considerable threat. 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.

Weaknesses/mitigating factors

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.

More requirements than before for the issue of ID numbers for foreign citizens are deemed a mitigating factor. Under the new legislation, financial institutions and private parties cannot be intermediaries. The authorities have realised the problem in greater measure and are also actively looking out for forged identity papers.

Risk classification

Considering the above, the risk that ID numbers for foreign citizens will be used to launder money must be deemed **medium**.

4 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 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 Art. 100 (a.-c.) of 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 Iceland.

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 no. 404/2007 on the National Security Unit of the National Commissioner of the Icelandic Police, the unit assesses the risk of terrorism in Iceland. The NCIP assesses that it is generally not possible to rule out the risk of terrorism regarding domestic or world affairs, and the risk of terrorism in Iceland is deemed medium. The assumptions underlying the assessment in the NCIP's National Security Unit's report of January 2021 include that the risk of terrorism in Iceland *"primarily stems from individuals who, because of propensity toward militant extremism and hate of society, are ready to perpetrate terrorist acts."* [42]

The assessment of terrorist financing in Iceland draws somewhat on the NCIP's assessment of the risk stemming from terrorism in Iceland.

On 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.

[42] *Hryðjuverkaógn á Íslandi (Terrorist Threat in Iceland)*. National Commissioner of the Icelandic Police, Reykjavik 2021, pp. 14-15.

The NCIP's National Security Unit handles investigations of criminal cases related to terrorism under the provisions of Regulation no. 660/2070 on the supervision of police investigations and cooperation of the district attorney and chief of police during the investigation of criminal cases. For that reason, based on the Act on Measures against Money Laundering and Terrorist Financing, 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 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 that, for example, send 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.[43]

The risk assessment also considered that Iceland is a homogeneous society with relatively few residents, where about 13.5% of them are of foreign origin. The frequency of crime is low.[44] The police are generally unarmed day-to-day, and Iceland has no military and no special ties to states regarded as risky concerning terrorism. No confirmed cases connected with terrorist financing have come up in the country. The same applies to terrorist offences and support for such conduct.

The main premises for the evaluation of threat are as follows:

- No terrorism has been perpetrated in Iceland after the entry into force of the current provisions on terrorism.
- There are no indications of terrorists or terrorist groups operating in Iceland.
- There are no indications that Icelandic terrorist groups are operating in other countries.
- There are no visible signs that an association of extremist religious or life stance groups have formed in Iceland.
- There are no visible signs that leaders or influencers engage in or organise indoctrination of an extremist ideology or advocate terrorism.
- There are no indications of trips from Iceland of foreign fighters.
- The number of received and sent requests, based on international collaboration on sharing of information regarding terrorist financing, is very small.
- The proportion of notices to FIU regarding suspicious transactions connected with terrorist financing is extremely low.

On the other hand, there are threats connected with possible terrorist financing. Those threats are known as international threats that FATF and others have called attention to. They relate to the transfer of cash across borders, remittances, and the operations of associations for the public good.

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. Finally, it must be mentioned that the general overview of associations' operations is curtailed, given the number of associations, their divergent forms, and limited public monitoring.

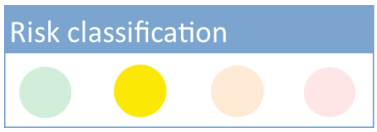
Regarding mitigating factors, the collaboration of authorities and institutions is very good and efficient in this area. Also, the work procedure is tightly constrained and documented, at both FIU and the police, regarding the processing of notices and clues regarding terrorist financing, as well as case investigations.

[43] *FATF Report. Emerging Terrorist Financing Risks.* FATF, Paris 2015.

[44] www.hagstofa.is/talnaefni/ibuar/mannfjoldi/bakgrunnur/.

Risk assessment and risk assessment factors of terrorist financing take note of this.

4.1 TRANSPORT OF ASSETS OUT OF THE COUNTRY



Generally – main threats
Transferring assets out of the country can occur mainly in two ways. On one hand, an individual may transport assets across the border when leaving the country, in the form of either cash – e.g., in baggage – or a withdrawal with an Icelandic payment card from an automatic teller machine after arriving in another country. On the other hand, it is possible to send assets out of the country with electronic remittances.

It is easy to transport cash out of the country, cf. the risk assessment's discussion on the transport of cash to and from Iceland. It is also possible to transfer cash rapidly between countries with money remittances. The turnover of these operations is high (ISK 2.4 billion in 2020), and transferring cash anonymously is possible even though this is forbidden. Both will be examined, considering that access to foreign currency in Iceland is good, and it is easy to convert Icelandic kronur to foreign currency, cf. the risk assessment's discussion of foreign exchange regarding money laundering. There, the discussion also states that the percentage of cash transactions in these services is high. Also, it is possible to exchange low sums anonymously despite this being forbidden. Finally, a somewhat high percentage of customers of the only foreign exchange office operated in Iceland is of foreign origin, and about 4% of the customers are from high-risk states.

No cases have come up where assets have been transported out of Iceland for terrorist financing. On the other hand, there is an example of an Icelandic payment cardholder loaning another person his card to use for a withdrawal from an automatic teller machine in another country to get money overland to a risky state. There are also very few notices to FIU of suspicious transactions regarding terrorist financing.

Threats in these operations therefore exist but are not considered great.

Weaknesses/mitigating factors
The monitoring of money remittances on borders is limited but there are promises of improvement with clearer legal authority to check the luggage of travellers leaving the country, cf. the previous discussion in the risk assessment of the transport of cash to and from Iceland. Also, the legal framework and monitoring of both money remittances and foreign exchange transactions are in rather good shape. As well, the authorities are aware of the threats stemming from the transport of assets out of the country. Also, risk awareness has increased in this area, both in public administration and for mandatory-notice parties. Finally, the authorities have organised the publication of educational materials

Risk classification
Considering existing threats and weaknesses as well as mitigating factors, the risk of terrorist financing because of the transport of assets out of the country is deemed to be **medium**.

4.2 NON-PROFIT ORGANISATIONS OPERATING ACROSS BORDERS

Iceland's risk assessment specially examined NPOs with operations across borders. The main reason for considering such organisations is that there are examples in FATF states of public interest organisations with a non-financial purpose being misused, especially for terrorist financing.[45] 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'."*[46] On this basis, the discussion was limited to NPOs with operations across borders, registered religious and life stance associations and associations and funds operating under a confirmed charter.

Generally – main threats

Regarding organisations deemed to be general associations and clubs operating for the public good with operations across borders, Act No 119/2019 on the Obligation of Non-profit Organisations to Register is deemed to apply. The act entered into force on 11 October 2019. Up to then, this form of organisation had no duty to register. Registration is now mandatory for these organisations and they number 28. The requirements for the above organisational form are suitable, given their number. The scope of these organisations is great, considering their financial activities. Under Art. 38 (2) of AML Act, cf. the act amending Act no. 96/2020, IRC's Money Laundering Division monitors such organisations.

Religious and life stance associations work in the public interest and are NPOs, according to FATF's definition. They operate under Act no. 108/1999 on registered religious and life stance associations and Regulation no. 106/2014 on the registration of such associations. The act provides for people's right to found religious associations and practice their religion following their convictions. The number of religious associations at the end of 2020/beginning of 2021 was 45, and the number of life stance associations for the same period was six. There are no examples of Icelandic religious and life stance associations having operations across borders. On the other hand, their legal framework and the structure of the organisation form does not require the founders or directors of such organisations, for example, to require spokespersons for such organisations to reside in Iceland or have other connections with the country. This results in a spokesperson for such an organisation in Iceland being able to reside in another country at the same time as the congregation fees go to the association. In 2020, the State Treasury paid about ISK 2.6 billion in church taxes. Of this amount, nearly ISK 512 million went to religious associations that are outside the National Church congregations in Iceland.[47] This involved church taxes from approximately 43,700 individuals. Public monitoring of this organisation form is the responsibility of the District Commissioner in North-east Iceland.

Finally, funds and associations operating under a confirmed charter, based on Act no. 19/1988 and Regulation no. 140/2008, may belong to the category of NPOs under FATF's definition. This involves quite a number – about 700 funds and associations. Of these, 473 submitted annual financial statements in 2019, and 216 of them had income the same year. The income of funds and associations varies as do their assets. This involves substantial amounts when income and assets are assessed in their entirety since the amounts run to billions of Icelandic kronur. There are no examples of associations and funds operating across borders. Public monitoring of these operations is the responsibility of the District Commissioner in Northwest Iceland. Also, the Icelandic National Audit

[45] *FATF Report. Risk of Terrorist Abuse in Non-Profit Organisations*. FATF, Paris 2014, pp. 36-48.

[46] *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. p.* 63.

[47] *Sóknargjöld 2020*, p. 2.

Office monitors the financial statements of this form of organisation.

In practice, there are no examples in Iceland of terrorist financing or connections with such conduct in other countries, and there are no examples of associations connected with terrorist operations working across borders. The main threats stemming from the operations of NPOs are examined considering this.

Weaknesses/mitigating factors

The main weaknesses of associations working in the public interest and operating across borders are that they involve different forms of association where the same rules of law do not apply. This makes their overview rather burdensome since no unequivocal duty to register is involved for NPOs working across borders. Also, there is official monitoring of the operations for NPOs, but it is not all in one place but the responsibility of four different authorities. Finally, the legal framework of both religious and life stance associations and funds and associations operating under a confirmed charter is past its prime and needs revising, among other things, considering threats of terrorist financing.

There are no specific mitigating factors to consider.

Risk classification

Considering the existing threats and weaknesses, the risk of public interest of associations' operations across borders regarding terrorist financing is **low**.

List of the most important abbreviations

AML	Act no. 140/2018 on Measures against Money Laundering and Terrorist Financing
BO	Beneficial owner
CBI	Central Bank of Iceland
DTI	Directorate of Tax Investigations
DPO	District Prosecutor's Office
FATF	Financial Action Task Force
FSA	The Financial Supervisory Authority of the Central Bank of Iceland
FIU	Financial Intelligence Unit
GPC	General Penal Code Act No. 19/1940
IRC	Iceland Revenue and Customs
LEAs	Law Enforcement Agencies
MoII	Ministry of Industries and Innovation
MoJ	Ministry of Justice
MoFE	Ministry of Finance and Economic Affairs
MoFA	Ministry of Foreign Affairs
NCIP	National Commissioner of the Icelandic Police
NGO	Non-governmental organisation
NPO	Non-profit organisation

References

Árbók bílgreina 2020. Hagtölur um íslenskar bílgreinar. The Research Centre for Retail (RCR) and the Icelandic Federation for Motor Trades and Repairs, Reykjavik 2020.

COVID-19-related Money Laundering and Terrorist Financing. FATF, Paris 2020.

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

FATF Report. Emerging Terrorist Financing Risks. FATF, Paris 2015.

FATF Report. Risk of Terrorist Abuse in Non-Profit Organisations. FATF, Paris 2014, pp. 36-48.

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

Fjármálainnviðir. Central Bank of Iceland, Reykjavik, 5th Monograph 7 June 2017.

Fjármálainnviðir. Central Bank of Iceland, Reykjavik, 7th Monograph 24 June 2019.

Hryðjuverkaógn á Íslandi. National Commissioner of the Icelandic Police, Reykjavik 2021.

International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. FATF, Paris 2020.

Jónatan Thórmundsson: *Þættir um auðgunarbrot. Sérstakur hluti*. Reykjavik 2009.

Mutual Evaluation Report of Iceland. FATF, Paris 2018.

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.

Peningamál. Central Bank of Iceland, Reykjavik, 83rd Monograph 3 February 2021.

Skipulögð brotastarfsemi á Íslandi. Áhættumatsskýrsla greiningardeildar ríkislögreglustjóra. National Commissioner of the Icelandic Police, Reykjavik 2019.

Skýrsla dómsmálaráðherra og fjármála- og efnahagsráðherra um aðdraganda og ástæður þess að Ísland hafnaði á „gráa lista" FATF. Iceland's Government Offices, Reykjavik 2019.

Skýrsla samstarfshóps félags- og barnamálaráðherra um félagsleg undirboð og brotastarfsemi á vinnumarkaði. Ministry of Social Affairs and Children, Reykjavik 2019.

Sóknargjöld 2020. Financial Management Authority, Reykjavik 2021.

Supranational Risk Assessment of the Money Laundering and Terrorist Financing Risks affecting the Union. The European Union, Brussels 2019.

Umfang skattundanskota og tillögur til aðgerða. Skýrsla starfshóps. Ministry of Finance and Economic Affairs, Reykjavik 2017.

Útdráttur úr ársreikningum sjálfseignarstofnana og sjóða sem starfa samkvæmt staðfestri skipulagsskrá, fyrir rekstrarárið 2019. National Audit Office, Reykjavik 2021.

Webpage of Althingi, www.althingi.is.

Website of the Icelandic Tourist Board, www.ferdamalastofa.is.

Webpage of Statistics Iceland, www.hagstofa.is.

Webpage of the Organisation of Europe for Economic Co-operation and Development (OECD), www.oecdbetterlifeindex.org.

Webpage of the Consultative Gateway, www.samradsgatt.island.is

Webpage of Iceland's Government Offices, www.stjornarradid.is.

Webpage of the District Commissioners, www.syslumenn.is.