Delna
SABIEDRĪBA PAR ATKLĀTĪBU
TRANSPARENCY INTERNATIONAL
LATVIJAS NODAĻA

Money Laundering in Latvia and the Baltics

Recent Developments, Ongoing Risks, and Future Challenges

Transparency International Latvia (Sabiedrība par atklātību – Delna) is a national chapter of the international coalition against corruption Transparency International. It is the leading watchdog organization in Latvia with the main aim of contributing to the formation of an open, just and democratic society, free from corruption in private and public sectors and interpersonal relationships.

Money Laundering in Latvia and the Baltics – Recent Developments, Ongoing Risks, and Future Challenges

Author: Antonio Greco (Transparency International Latvia)

Acknowledgements: We thank our colleague Maira Martini at the Transparency International Secretariat for her comments on an earlier version of this report

This publication was produced in the framework of the Global Anti-Corruption Consortium

Free download of this report is available at www.delna.lv

Published August 2021

© Cover image: iStock

Content

Executive summary

This report provides a bird's-eye view of the main features of the complex money laundering schemes carried out through Latvian and other Baltic banks, assessing governments' efforts to prevent the reoccurrence of similar schemes in the future as well as significant ongoing risks linked to the abuse of shell companies, the exploitation of corporate services, and the emergence of the e-money and digital payment industry.

Non-resident banking and money laundering in Latvia and the Baltics

As of today, at least three major "Laundromats" involving Baltic banks were uncovered by investigative journalists – the Russian Laundromat (2017)[1], the Azerbaijani Laundromat (2017)[2] and the Troika Laundromat (2019)[3]. These schemes enabled kleptocrats in the Former Soviet Union (FSU) to launder illicit funds of over $30-$80 billion derived from corruption, fraud and embezzlement, and use them for different purposes, including purchasing real estate and luxury assets, lavish expenses, silencing of human rights and much more.

Money laundering through banks in the Baltic countries, including Scandinavian banks with a high reputation, was facilitated by their "non-resident banking" business model. This consisted of the attraction of thousands of high-risk foreign customers located in the FSU, who were allowed to hold deposits through shell companies with little or no information on their beneficial owners and to carry out international transactions in US dollars across multiple jurisdictions thanks to correspondent banking relationships with reputable financial institutions based in the US.[4]

This business model brought disproportionate money laundering risks, not corresponding to the banks' capacity to handle them. The exposure of the Laundromats and other scandals, including the indictment of ABLV Bank in Latvia[5], prompted a crackdown by governments in Latvia and other Baltic countries on non-resident banks, and this resulted in a sharp fall in foreign deposits. Even though risks are not as high as in the past decade, the FinCEN files investigation published in September 2020 showed that there are still ongoing risks related to shell companies and TCSPs.[6]

The shell games

As revealed by the investigations on the Laundromats, criminal networks gradually moved from using shell companies registered in notorious offshore jurisdictions, such as the British Virgin Islands (BVI) and Panama, to using shell companies in reputable "onshore" jurisdictions. The majority of shell companies used in the Laundromats were registered in the UK. This was due to its veneer of legitimacy, the ease and low cost of incorporation of companies, and the *de facto* anonymity of beneficial ownership offered by partnership structures.[7]

While in April 2018 the Latvian government banned banks from servicing shell companies[8], and nowadays there is much more alertness about risks posed by UK companies, it is likely that criminals will keep seeking to set up shell companies in jurisdictions with features similar to the UK. The risk of this happening is exacerbated by the

[1] https://www.occrp.org/en/laundromat/the-russian-laundromat-exposed/
[2] https://www.occrp.org/en/azerbaijanilaundromat/
[3] https://www.occrp.org/en/troikalaundromat/
[4] Stack G. (2015), "Shell companies, Latvian-type correspondent banking, money laundering and illicit financial flows from Russia and the Former Soviet Union", *Journal of Money Laundering Control,* vol.18, no.4, pp. 496-512
[5] https://www.fincen.gov/news/news-releases/fincen-names-ablv-bank-latvia-institution-primary-money-laundering-concern-and
[6] https://www.icij.org/investigations/fincen-files/
[7] Transparency International Latvia / Delna (2018), *Connections – Money Laundering in Latvia and the Role of Company Service Providers*
[8] https://www.mk.gov.lv/en/article/saeima-imposes-ban-servicing-shell-companies

fact that beneficial ownership transparency and accessibility is still very low, both in Europe[9] and globally[10]. The Latvian government has mitigated such risks by opening a beneficial ownership register[11], but more decisive efforts are needed to end the shell games.

The role of Trust and Company Service Providers

Trust and Company Service Providers (TCSPs) played a key role in the Laundromats and other major money laundering cases, helping criminals to create hundreds of shell companies in the UK and other jurisdictions. Crucially, they also handled the opening of accounts in Latvian and other Baltic banks, which, through cooperation agreements, relied on them to bring in new customers from the FSU, while applying little or no AML checks. At times, they also assumed the form of "para-bank" structures, and bankers themselves were found to run TCSPs as a side-business.[12]

While nowadays the use of TCSPs among Latvian and other Baltic banks is much less common, there are still thousands of businesses engaging in the creation and trade of shell companies, and the money laundering risk associated with those TCSPs operating in Latvia is still high due to the cross-border nature of the services they offer and their weak AML capacity.[13] In the past few years, the State Revenue Service has strengthened supervision of the sector, but the lack of licensing for these businesses and, more generally, the lack of a common approach to their supervision globally makes them very difficult to control.

E-money – a new frontier for high-risk business?

There are indications that the crackdown on Latvian and Baltic banks and the ensuing process of de-risking has coincided with a gradual migration of high-risk clients from the FSU to Electronic Money Institutions (EMIs) and Payment Institutions (PIs). A recent investigation found not only that several of such businesses in the UK are run by former executives and officers at Latvian non-resident banks that were fined for insufficient AML compliance, but also that the sector has become increasingly intertwined with the shell company business.[14]

In Latvia, the EMI/PI sector has been developing in recent years, and the FIU attributes to it a medium-high money laundering risk, explicitly noting the progressive shift of high-risk clients to this industry.[15] Following a strengthening of supervision rules in 2018 the number of registered EMIs in the country has dropped. However, EMIs/PIs with freedom to provide services across the EU still pose a high money laundering risk for Latvia, as they may be established in countries with a weaker supervisory system. This indicates a need for better cross-border supervision and intelligence sharing.

The EU's new AML package

Prompted by the growing concerns about money laundering, in July 2021 the EU Commission presented an ambitious package of legislative proposals to strengthen the EU's anti-money laundering system. This includes

[9] Transparency International (2021), *Access Denied? Availability and Accessibility of Beneficial Ownership data in the European Union*, https://www.transparency.org/en/publications/access-denied-availability-accessibility-beneficial-ownership-registers-data-european-union
[10] Tax Justice Network (2020), *The state of play of beneficial ownership registration in 2020*, https://taxjustice.net/wp-content/uploads/2020/11/State-of-play-of-beneficial-ownership-Update-2020-Tax-Justice-Network.pdf
[11] https://data.gov.lv/dati/lv/dataset/plg-bods
[12] Stack G. (2015), "Shell companies, Latvian-type correspondent banking, money laundering and illicit financial flows from Russia and the Former Soviet Union", *Journal of Money Laundering Control,* vol.18, no.4, pp. 496-512
[13] Financial Intelligence Unit of Latvia, National ML/TF/PF Risk Assessment 2017-2019 (Executive Summary), https://fid.gov.lv/uploads/files/2021/NRA_2017_2019_Executive_Summary%20%28002%29.pdf
[14] https://www.opendemocracy.net/en/dark-money-investigations/will-e-money-boom-make-uk-hub-money-laundering/
[15] Financial Intelligence Unit of Latvia, National ML/TF/PF Risk Assessment 2017-2019 (Executive Summary)

the creation of a new EU AML authority (AMLA); a new regulation on AML containing directly applicable rules, including in the areas of Customer Due Diligence and beneficial ownership; a 6th AML Directive containing provisions for the new rules to be transposed into national law; and a strengthening of AML rules for the crypto sector.[16]

While this is a much-welcomed move, it will still be a long time before Member States can fully adapt to the new framework and reap the benefits of enhanced cross-border AML monitoring and control by AMLA (assuming it will have adequate resources and governance). As such, governments in Latvia and other Baltic countries should not only fully support the EU Commission's proposal in Council negotiations, but already take some steps to tackle the most pressing problems identified in this report and to prepare themselves and facilitate the transition to the new rules.

Policy recommendations

Based on the findings of this report, we recommend the Latvian government to fully support current EU efforts to establish a supranational supervision and reporting mechanism for cross-border transactions, and work in concert with the FIU, the FCMC, the SRS, the Enterprise Register, and members of the Financial Sector Development Board to implement the following measures:

- Ensure the regular publication of accurate statistics about banks' relationships with TCSPs and EMIs/PIs, including at least: i) the number of TCSPs with whom they have a cooperation agreement and the number of EMIs/PIs to whom they provide correspondent banking accounts; ii) jurisdictions in which those TCSPs and EMIs/PIs are based and operate; iii) information about the different types of cooperation agreements and correspondent banking services

- Take steps to further strengthen the monitoring and transparency of the provision of corporate services in Latvia, by: i) developing licensing requirements for TCSPs, regardless of the specific business category to which they belong; ii) setting up a public register of all TCSPs under the supervision of the SRS; iii) publishing a list of disqualified TCSP owners and directors.

- Engage with competent authorities in Estonia and Lithuania to ensure interoperability among corporate registries in the three countries and harness their AML intelligence value, by: i) adopting common open data standards; ii) developing common tools and indicators to detect suspicious TCSP activities (e.g., bulk-formation of companies); iii) developing technical solutions that allow for cross-border verification of accuracy of basic beneficial ownership information (e.g., verifying whether information provided by a Latvian national setting up a company in Estonia corresponds to information held by Latvian authorities about that person).

- Seek to upscale financial intelligence cooperation and information sharing related to EMIs/PIs across the three Baltic States, by: i) undertaking a joint cross-border risk assessment or thematic study focused on current money laundering threats posed by EMIs/PIs operating in the three countries and targeting high-risk customers from the FSU; ii) establishing regional Expert Groups to share intelligence with the largest private EMIs/PIs operating in the three countries; and iii) consider the introduction of mandatory targeted transaction and record-keeping requirements on EMIs/PIs serving legal entities owned by high-risk customers

[16] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690

Introduction

Money laundering has been a growing concern for Latvia and the other Baltic countries. A series of journalist investigations in the past decade have shown how banks operating in the Baltic states, including Scandinavian banks with a high reputation, have been exploited by corrupt politicians, organized crime networks and oligarchs from the Former Soviet Union to carry out so-called "Laundromats".[17] These were highly sophisticated schemes using networks of anonymous shell companies engaging in complex transactions to secretly launder money, invest ill-gotten gains, evade taxes and fulfill other goals.

While the exposure of such cases has led to a crackdown on Latvian and other Baltic banks, the FinCEN files investigation[18], uncovered in September 2020 and identifying at least 2 trillion USD in suspicious transactions by global banks between 2006 and 2017 (including 7.6 billion USD flowing through nine Latvian banks), has provided additional evidence about the workings of the Laundromats and the continuing threat posed by the abuse of anonymous shell companies and uncontrolled company formation activities at the global level.

Against this backdrop, this report provides a bird's-eye view of the main features of the complex money laundering schemes through Latvian and other Baltic banks, assessing governments' efforts to prevent their occurrence in the future as well as significant ongoing risks linked to the abuse of shell companies and corporate services, and to the progressive migration to the e-money and digital payment industry, which presents significant challenges on its own.[19]

The report, which focuses on Latvia, was developed through desk-based research, drawing on extensive material from journalist investigations, academic research, money laundering risk assessments by national and international bodies, governments' strategic policy documents, as well as through consultations with senior policymakers within AML bodies in Latvia.

The first part provides an overview of the problem of money laundering and the key services that may be exploited by criminal networks to manage their illicit wealth, as well as of the existing international standards in the field. The second part traces the evolution of money laundering through Latvia and other Baltic countries, looking at correspondent banking, the abuse of shell companies, the role of company service providers, and the progressive migration to the e-money sector. In the final part, we provide recommendations to public authorities in Latvia and the EU to tackle the problem.

[17] https://www.occrp.org/en/laundromat/the-russian-laundromat-exposed/ ; https://www.occrp.org/en/azerbaijanilaundromat/ ; https://www.occrp.org/en/troikalaundromat/
[18] https://www.icij.org/investigations/fincen-files/
[19] https://www.opendemocracy.net/en/dark-money-investigations/will-e-money-boom-make-uk-hub-money-laundering/

1. The problem of money laundering

What is money laundering?

Money laundering can be generally defined as the process by which criminals disguise the original ownership and control of the proceeds of criminal activities (e.g., drug trafficking, corruption, tax evasion, etc.) by making such proceeds appear to have derived from a legitimate source.[20] It is a crucial activity that enables corruption and criminal networks to thrive by enjoying the profits of their crimes or reinvesting them to expand their activities and power.

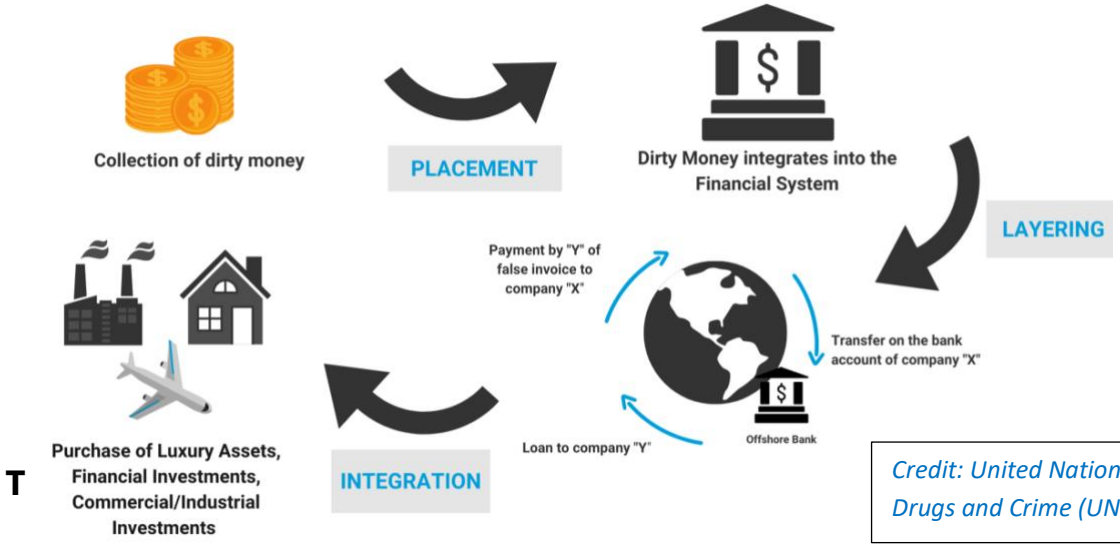
Money laundering involves a complex series of activities that are often difficult to separate; however, typical schemes usually take place **in three stages: i) placement; ii) layering and iii) integration**.[21]

In the **placement** stage, the illicit money is introduced into the financial system through legitimate business. This can be done in a number of different ways, for example by depositing small amounts of cash in several bank accounts to avoid detection, or by mixing illegitimate and legitimate funds into cash-intensive businesses (e.g., restaurants, casinos, carwashes, etc.). Large amounts of cash can also be smuggled across borders and placed into complicit, negligent, or unwitting banks.

In the **layering** stage, the proceeds of crime get separated from their source to disguise their origins and owners, making it difficult for law enforcement authorities to follow the money trail. This can be done, for example, by using networks of anonymous shell companies engaging in complex banking transactions or fictitious trade activities across multiple jurisdictions, or by investing the funds in stock markets and engaging in complex financial operations.

In the **integration stage,** the funds are re-entered into the economy through their use in seemingly normal business or personal transactions to create the appearance of legitimacy. This is done, for example by investing in real estate, by purchasing luxury assets such as precious metals and pieces of art, or by acquiring shares in legal businesses.

Picture 1 – The Money Laundering Cycle



Credit: United Nations Office for Drugs and Crime (UNODC)

[20] https://www.unodc.org/unodc/en/money-laundering/overview.html
[21] Ibid.

Due to its clandestine nature, there is currently no exact measure of how much illicit money is laundered globally; however, the United Nations Office for Drugs and Crime (UNODC), estimates the total amount of money going through the money laundering cycle every year to be between 2% and 5% of the global GDP, corresponding to US$2 trillion.[22]

Money laundering can have damaging consequences for both developing and developed countries. It enables corruption and organized crime networks to thrive, thus weakening state institutions and fostering political unrest, and eroding the safety and security of society. Money laundering schemes can also be used to finance terrorism and/or evade international sanctions on nuclear proliferation, thus contributing to global instability.[23]

Furthermore, money laundering can have negative economic consequences. It can result in the loss of governments' fiscal revenue and damage a country's reputation and attractiveness to foreign investors. It can also contribute to the distortion of normal market operations and delegitimization of the private sector (e.g., when criminal groups infiltrate the legal economy), and to the weakening of banks and other financial institutions.[24]

Setting up the money laundering structure

As criminal networks rarely have the internal expertise to perform the several complex operations needed to carry out money laundering schemes, they often rely on professional intermediaries or 'enablers' operating in the legal economy. These can provide specific services, expertise and infrastructure that can help criminals establish a parallel underground financial and legal system to process transactions and payments without being traced, including access to the banking network, setting up complex corporate structures and management of illicit wealth and assets.

In the latest Serious and Organised Crime Threat Assessment (2021), Europol has observed the development and proliferation of the so-called "crime-as-a-service business model", which involves the delivery of specialised services enabling criminal activities, including money laundering. According to Europol, at least 32% of detected organised crime groups in the European Union have access and make use of money laundering service providers.[25]

Transparency International UK has identified at least nine core services that are vulnerable to exploitation for money laundering, including banking services, company formation and maintenance, property transactions, trade of high-value goods, lifestyle management, legal defence, lobbying, high-profile investments and education.[26] This report focuses on banking and financial transaction services, legal entities and company formation and maintenance services.

It is important to note that professional intermediaries' degree of involvement in money laundering can vary along a continuum from unwitting involvement to wilful blindness to complicit participation. From

[22] Ibid.
[23] https://www.fatf-gafi.org/faq/moneylaundering/
[24] Ibid.
[25] Europol (2021), *European Union Serious and Organised Crime Threat Assessment 2021*, https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment
[26] Transparency International UK (2019), *At Your Service – Investigating how UK businesses and institutions help corrupt individuals and regimes launder their money and reputations*, https://www.transparency.org.uk/publications/at-your-service/

a criminal intelligence perspective, while professional intermediaries that are corrupt or complicit in money laundering can be regarded as high-value targets, since disrupting their activities would strike a blow to criminal networks, professionals who provide services that are vulnerable for exploitation also have an important role to play in the detection and prevention of financial crime.[27]

Banking services

Banks have historically been, and continue to be, crucial intermediaries for money laundering, given that they are the primary means to transfer and use money across the globe. There are different types of banking services that can be exploited to carry out money laundering schemes, including private banking, correspondent banking, retail banking and capital market operations.[28]

Among those services, correspondent banking is particularly vulnerable to money laundering. This is the practice of a bank (the "correspondent bank") in a certain country providing intermediary services on behalf of another bank ("the respondent bank") based in another country, aimed at allowing the latter to perform operations in jurisdictions where it does not have a physical presence.[29] While this is essential for the global economy, correspondent banks are not in direct contact with the origin or destination of the funds. This makes them reliant on the Anti-Money Laundering (AML) systems of respondent banks involved in the transactions, which may or may not be effective and adequate in relation to the risk posed by servicing specific categories of customers.

E-money and new payment products and services

In recent years, the evolution and cheaper cost of digital technologies have contributed to the emergence of "electronic money" (or "e-money") – broadly defined as an electronic storage of monetary value on a technical device that can be used to make payments to multiple legal entities or natural persons[30] – and the proliferation of associated new payment products and services (NPPSs), including prepaid cards, internet-based and mobile-based payment services.[31]

These can be provided by different actors, including specialised "Electronic Money Institutions" (EMIs), banks, and mobile network operators (often a combination of all three). NPPSs act as prepaid instruments which can be funded in different ways and do not necessarily involve bank accounts in the transactions. While they are widely considered to be very important for financial inclusion, their capacity to allow persons or businesses to transfer funds, carry out payments, make purchases and access cash across multiple jurisdictions, makes them attractive for easily and quickly laundering money.

Apart from geographical reach, there are other factors making NPPSs attractive, including non-face-to-face contacts, anonymity and methods of funding. Internet and mobile payment services often rely on non-face-to-face contacts in acquiring new customers, which entails risks of identity fraud. Prepaid

[27] Ibid.
[28] Ibid.
[29] Financial Action Task Force (FATF) (2016), *Guidance on Correspondent Banking Services*, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/correspondent-banking-services.html
[30] https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html
[31] FATF (2013), *Guidance for a Risk-Based Approach on Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf

cards can easily be passed to, and used by, third parties unknown to the issuer, thus allowing for anonymity. Moreover, some NPPSs allow for funding that may obscure the origins of the funds (e.g., cash or third parties that do not identify customers).

Shell companies and corporate service providers

The use of shell companies – companies that exist only on paper, without significant assets or operations – to facilitate money laundering has been well documented. A 2011 report by the World Bank showed that 70% of reviewed grand corruption schemes were carried out using shell companies.[32] According to Europol's Serious and Organised Crime Threat Assessment 2021, as many as 80% of crimes committed by criminal networks and organisations across Europe featured the use of business structures, including not only shell companies, but also legitimate businesses.[33]

While shell companies can be used for legal purposes (e.g., business finance, mergers and acquisitions, estate and tax planning, etc.), they also allow for a wide range of business operations to disguise the transfer of illicit funds, for example lending, simulating trade activities, paying out fictitious salaries and expenses, and purchasing real estate. Criminals may also use "front companies" engaging in real economic activity to mix illicit funds with legitimate profits or to infiltrate the legal economy.[34]

Anonymity of the shell companies is a precondition for criminal networks to effectively carry out such operations, and they have different ways to achieve it. For example, they can set up complex shell company structures with parent companies and subsidiaries spanning multiple jurisdictions, including tax havens with strict secrecy laws. They can also use "nominees" – individuals, often with no criminal records, who act as owners, officers, directors, partners (or similar positions) of the company. These techniques make it very cumbersome, or impossible, to carry out criminal investigations.[35]

Although money launderers can easily create shell companies and other legal entities by themselves, to carry out this activity in a more effective and systematic manner they usually rely on Trust and Company Service Providers (TCSPs). TCSPs are businesses that provide any of the following services to third parties[36]:

- Incorporation of companies and other legal entities across multiple jurisdictions
- Provision of registered office, business address or mail correspondence for a legal entity
- Arrangement of bank accounts for legal entities and clients ('introduction' services)
- Provision of nominee services – acting as (or arranging for another person to act as) director, shareholder, secretary, trustee, partner or similar position in a legal entity
- Filing of company accounts and submission of annual paperwork

While the services listed above are fully legitimate, they also have a clear value for criminals seeking to hide their identity and manage their funds without raising suspicions. For example, introduction services might be exploited to get access to the financial system. Nominees can be used to sign off

[32] Van der Does de Willebois E., Halter E., Harrison R.A., Park J.W., Sharman J.C. (2011), *The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It,* World Bank, https://openknowledge.worldbank.org/handle/10986/2363
[33] Europol (2021), *European Union Serious and Organised Crime Threat Assessment 2021*
[34] Van der Does de Willebois E., Halter E., Harrison R.A., Park J.W., Sharman J.C. (2011), *The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It,* World Bank
[35] Ibid.
[36] Ibid.

paperwork and annual accounts. TCSPs may also engage in the sale of "shelf companies" – shell companies that have been created and "put on the shelf" to be later sold – to give an impression of corporate history (and, in case of criminal activity, raise less suspicions for investigators).[37]

International AML standards

International efforts to tackle money laundering gathered pace towards the end of the 20th century. The issue was first put on the global policy agenda through the 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (also known as "Vienna Convention"), which sought to tackle the issue in the context of the fight of international drug trafficking.[38] Thereafter, in 1989, the Group of Seven nations (G7) set up the Financial Action Task Force (FATF), an international body whose main task is to promulgate AML guidance to governments across the globe.[39]

In 1990, the FATF issued 40 Recommendations which provide a comprehensive set of minimum standards to tackle money laundering and terrorist financing and have effectively become the world's blueprint for policy measures in these areas.[40] The recommendations, which were revised in 1996, 2003 and 2012, cover identification of risks and development of appropriate policies, AML regulation of the financial system, criminal justice system and law enforcement, transparency of legal persons and arrangements, and international cooperation.

As a first step, countries should identify, assess and understand their exposure to money laundering and terrorist financing risks, and then devise appropriate measures to mitigate them. The same should be done by financial and non-financial institutions subject to AML regulations (including banks, e-money providers and TCSPs). Such "risk-based approach" allows countries and obliged entities to allocate limited resources in a targeted and flexible manner that is in line with the national context and the circumstances of their operations.

Countries should also ensure that obliged entities are required to carry out customer due diligence (CDD) on their clients (i.e., verification of the identity and purpose for the business relationship), monitor and keep records on their transactions and activities and report those deemed as suspicious to the country's Financial Intelligence Unit. Enhanced CDD measures may apply when dealing with specific high-risk customers, such as politically exposed persons (PEPs), or services provided (e.g., correspondent banking and international payment products).

Furthermore, countries should take appropriate measures to prevent the misuse of legal persons for money laundering. This includes ensuring that information about the beneficial owners of legal persons is available to competent authorities. The term "beneficial owner" refers to the natural persons who ultimately own and/or control a legal entity, including through other legal entities that might "nominally" own the company. There should also be mechanisms in place to verify the identity of declared beneficial owners and the accuracy of company records.

The recommendations also provide indications regarding responsibilities of competent authorities. Statutory supervisors should be tasked with monitoring AML compliance by obliged entities within their

[37] Ibid.
[38] https://www.unodc.org/unodc/en/treaties/illicit-trafficking.html?ref=menuside
[39] https://www.fatf-gafi.org
[40] https://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate)

jurisdiction and have the mandate to issue fines in case of breaches to the law. Financial Intelligence Units (FIUs) should be tasked with collecting and analysing Suspicious Transaction Reports (STRs) filed by obliged entities and disseminating the resulting intelligence to law enforcement authorities (LEAs), who investigate money laundering and seize or freeze criminal assets where found.

While these authorities should have sufficient resources and powers to effectively carry out their duties, governments should also provide them with a wide range of mutual legal assistance mechanisms when engaging in international cooperation over money laundering investigations.

The implementation of the FATF recommendations globally is monitored through mutual evaluations by FATF itself in its 37 member countries, and by associate regional bodies in other jurisdictions across the world.[41] Neither FATF nor regional bodies have the power to impose penalties against countries for not being compliant with the Recommendations; however, it does have a practice of "naming and shaming" high-risk jurisdictions with deficiencies in their AML systems[42], which in practice works as a deterrent by discouraging member countries to engage in financial transactions with them.

Besides the FATF and its associate regional bodies, a number of other international organisations provide guidance and monitor countries' compliance with AML standards. These include, but are not limited to, the United Nations[43], the World Bank[44], the International Monetary Fund[45], the OECD[46], and the Basel Committee on Banking Supervision.[47]

Anti-Money Laundering regulation in the European Union

AML in the EU is regulated by Directive (EU) 2018/843 – also known as EU 5th AML Directive.[48] The Directive, effective as of January 2020, requires EU Member States to adapt their national AML legislation to high-level anti-money laundering standards. It is largely based on FATF 40 Recommendations, and it is even more ambitious in some areas. For example, the Directive mandates Member States, until January 2021, to set up central registers holding beneficial ownership information on legal entities within the jurisdiction and make them available to the public.

On 20 July 2021, the EU Commission presented an ambitious package of legislative proposals to further strengthen the EU's anti-money laundering system.[49] This includes the creation of a new EU AML authority (AMLA); a regulation on AML containing directly applicable rules, including in the areas of Customer Due Diligence and Beneficial Ownership; a 6th AML Directive containing provisions for the new rules to be transposed into national law; and a strengthening of AML rules for the crypto sector, including stricter CDD requirements and full traceability of crypto-asset transfers. These measures are expected to enter into force by 2026.

[41] https://www.fatf-gafi.org/about/membersandobservers/
[42] https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)
[43] https://www.unodc.org/unodc/en/money-laundering/index.html
[44] https://www.worldbank.org/en/topic/financialmarketintegrity
[45] https://www.imf.org/external/np/leg/amlcft/eng/
[46] https://www.oecd.org/tax/crime/
[47] https://www.bis.org/bcbs/
[48] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing_en
[49] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690

2. Money laundering in Latvia and the Baltics

Money laundering has been a growing concern for the Baltic countries. A series of recent investigations from national and international media outlets have provided mounting evidence of how in the past decade kleptocratic networks from countries of the Former Soviet Union (FSU) have exploited Baltic and Scandinavian banks in Latvia, Estonia and Lithuania to launder billions of dollars derived from corruption, fraud and embezzlement, and use them for different purposes, including capital flight, purchase of real estate and luxury assets, and silencing of human rights.

As of today, at least three major "Laundromats" have been uncovered by investigative journalists at the Organised Crime and Corruption Reporting Project (OCCRP) and partner media outlets – the Russian Laundromat (2017)[50], the Azerbaijani Laundromat (2017)[51] and the Troika Laundromat (2019)[52]. These provided a stark picture of the capacity of kleptocratic networks in the FSU to assemble sophisticated shadow financial systems enabling them to launder illicit funds for over $30-$80 billion.

Though each Laundromat had its own complex ways of operating, the accumulation of evidence allows for the identification of some common features:

- Exploitation of Baltic banks with weak AML systems, whose correspondent banking relationships with reputable US financial institutions allowed criminals to carry out transactions in US dollars across multiple jurisdictions without raising suspicions. This was facilitated by a business model based on the active attraction of high-risk clients from the FSU.
- Use of networks of anonymous shell companies, most of them incorporated in "prestigious" jurisdictions, such as the UK. These engaged in complex chains of transactions, supported by fraudulent documentation, to give the appearance of normal business operations.
- Widespread involvement of loose but well-organised networks of Trust and Company Service Providers (TCSPs), who enabled criminals to set up and operate the shell company networks while at the same time opening accounts for them in banks in the Baltic countries, with which they had cooperation agreements.

The exposure of the Laundromats prompted a crackdown by governments in Latvia and other Baltic countries on banks servicing high-risk customers from the FSU, which resulted in a sharp fall in foreign deposits. However, the "FinCEN files" investigation, based on a leak of 2,600 SARs filed by global banks to the US FIU (FinCEN) between 2009 and 2017 – provided additional evidence and details about the "shell company trade" and the role of TCSPs therein, showing that this is an ongoing global problem, and countries need to find effective solutions to tackle it.[53]

Furthermore, there is emerging evidence that "de-risking" in Baltic banks has coincided with a progressive shift of high-risk customers from the FSU to e-money institutions and digital payment services, in some cases provided by former executives and employees at non-resident banks.[54] While the use of these services has become increasingly intertwined with the shell company formation business, their rapid development and their inherent cross-border nature makes it imperative to devise better solutions for their supervision and control, both at the EU and global level.

[50] https://www.occrp.org/en/laundromat/the-russian-laundromat-exposed/
[51] https://www.occrp.org/en/azerbaijanilaundromat/
[52] https://www.occrp.org/en/troikalaundromat/
[53] https://www.icij.org/investigations/fincen-files/
[54] https://www.opendemocracy.net/en/dark-money-investigations/will-e-money-boom-make-uk-hub-money-laundering/

Non-resident banking and money laundering in Latvia and the Baltics

Money laundering through banks in the Baltic countries was facilitated by their "non-resident banking" business model. This consisted in the attraction of thousands of high-risk foreign customers located in Russia and other jurisdictions of the Former Soviet Union, who were allowed to hold deposits through shell companies with little or no information on their beneficial owners and carry out international transactions in US dollars across multiple jurisdictions through correspondent banking relationships with reputable financial institutions based in the US.

While this business model significantly contributed to increase Baltic banks' performance and profits, it also brought disproportionate money laundering risks, not corresponding to their capacity to handle them. US-based correspondent banks also played a critical role, as they overlooked many obvious money laundering signs associated with financial flows from the Baltics. As we shall see below, this resulted in some of the biggest money laundering schemes of the 21st century.

The rise and fall of Latvia's non-resident banking business

Latvian commercial banks pioneered the non-resident banking model already in the 1990s, when, after the regained independence of Latvia, they began to establish correspondent banking relations with several US financial institutions. This allowed them to market themselves as a "financial bridge" between the East and the West, offering clients in Russia and other countries of the FSU the possibility of holding short-term deposits through shell companies and carrying out international payments in US dollars while providing discretion and additional services in Russian language.[55]

By the end of the 2000s, Latvian non-resident banks had already been associated with a number of significant money-laundering scandals, including the Magnitsky affair[56] as well as cases of political corruption and embezzlement by elites in Ukraine, Kazakhstan and Kyrgyzstan. Even though Latvia was formally compliant with international AML standards, these were weakly enforced. Banks were found to have outdated CDD systems, and, in some cases, officers blatantly neglected their AML duties. At the same time, regulatory fines were deemed to be too low and non-dissuasive.[57]

Despite being aware of the risks associated with non-resident banking, the Latvian financial regulator – the Financial Capital and Market Commission (FCMC) – endorsed the export of financial services, as it improved Latvia's balance of payment. Latvia's adoption of the euro in 2014 made it an even more attractive location and the share of foreign deposits in Latvian banks kept climbing until it reached its peak of 53.1% in 2015.[58] In the meanwhile, some of the biggest money laundering schemes in Eastern Europe were taking place, with far-reaching consequences for Latvia's reputation.

One of such cases was the "Russian Laundromat", which ran from 2012 and 2015 and was labelled "the biggest money-laundering scheme ever operating in Eastern Europe". Journalist investigations revealed that a criminal network of about 500 individuals across Russia, Ukraine and Moldova managed

[55] Stack G. (2015), "Shell companies, Latvian-type correspondent banking, money laundering and illicit financial flows from Russia and the Former Soviet Union", *Journal of Money Laundering Control,* vol.18, no.4, pp. 496-512
[56] The Magnitsky Affair refers to a $230 million tax fraud perpetrated by Russian public officials and criminal figures and uncovered by the lawyer Sergey Magnitsky in 2008. He was later arrested and died in prison after being denied medical assistance for serious illnesses.
[57] Transparency International Latvia / Delna (2018), *Connections – Money Laundering in Latvia and the Role of Company Service Providers*, https://delna.lv/wp-content/uploads/2018/01/Delna_Connections_2018_small.pdf
[58] Ibid.

to launder at least $20.8 billion through a sophisticated system of fake loan repayments (certified by corrupt Moldovan judges) among a network of 21 shell companies with accounts in the Moldovan bank Moldinconbank and the Latvian bank Trasta Komercbanka.[59]

In another significant case that came to be known as the "Moldovan bank fraud", taking place in 2014-15, a criminal network with connections to political elites in Moldova fraudulently acquired ownership of three major banks in the country and stole around $1 billion. This was done using a network of UK shell companies with accounts in three Latvian banks (Privatbank, ABLV, and Latvijas Pasta Banka). As a result of this scheme, the Moldovan government had to bail out the three banks for a sum equivalent to 12% of Moldova's GDP, throwing the country into political turmoil.[60]

The exposure of these cases had negative consequences for Latvia's international reputation, and it threatened the country's accession to the OECD. In response, the FCMC, under a new direction, stepped up its supervision efforts and, between 2016 and 2018, imposed fines for a total of more than €14 million on 10 banks in Latvia for not complying with AML regulations.[61] This also included fines to five Latvian banks that in 2017 were found to have enabled circumvention of international sanctions imposed on North Korea for the development of nuclear weapons.[62]

In parallel, the FCMC, with the support of audit firms from the US, oversaw a process of "de-risking" of 11 Latvian non-resident banks and encouraged them to reorient their business model towards domestic clients. This resulted in the closure of around 19,000 high-risk accounts and a related 26% drop in the share of non-resident deposits in 2016. In 2017, the branch of Deutsche Bank in the US, the only one still offering correspondent banking services to Latvian banks, decided to terminate the business relationship with them to decrease its exposure to money laundering risks.[63]

In February 2018, FinCEN issued a notice accusing ABLV bank, Latvia's third-largest bank, of carrying out "institutionalised money laundering", enabling corruption and embezzlement in Azerbaijan and Ukraine, bribing Latvian officials and evading international sanctions against North Korea.[64] After a few days, central bank governor Ilmārs Rimševičs was arrested and later investigated on suspicions of soliciting bribes from banks (including ABLV) in exchange for favourable treatment in AML supervision (the investigation was terminated at the end of March 2021 due to lack of evidence).[65]

The two cases struck a blow to the international reputation of Latvia's financial system. Following allegations from FinCEN, ABLV was stripped of its license and, after two months, the government introduced a ban for banks to service shell companies.[66] In the meanwhile, ABLV's management, while denying all accusations, applied for voluntary liquidation, which would allow the bank's shareholders to oversee the process. In July 2018, in a widely criticised move, the FCMC allowed the bank to go ahead, and the liquidation is still ongoing to this day (see box below).[67]

[59] https://www.occrp.org/en/laundromat/the-russian-laundromat-exposed/
[60] https://www.occrp.org/en/investigations/4203-grand-theft-moldova
[61] https://en.rebaltica.lv/2020/09/crime-and-punishment-how-latvia-cleaned-up-its-non-resident-banks/
[62] Transparency International Latvia / Delna (2018), *Connections – Money Laundering in Latvia and the Role of Company Service Providers*
[63] Ibid.
[64] https://www.fincen.gov/news/news-releases/fincen-names-ablv-bank-latvia-institution-primary-money-laundering-concern-and
[65] https://en.rebaltica.lv/2021/05/investigators-fail-to-prove-ex-chief-of-latvian-bank-demanded-bribe-from-ablv/
[66] https://en.rebaltica.lv/2020/09/crime-and-punishment-how-latvia-cleaned-up-its-non-resident-banks/
[67] https://en.rebaltica.lv/2019/03/in-the-shadows-of-ablv-from-regulator-to-a-friend/

The ABLV case

At the time of the FinCEN notice, ABLV was the biggest offshore bank in Latvia. The scale of its business was huge, almost as much as Latvia's GDP in 2016 (€25 billion). In September that year, almost 13,000 non-resident companies had accounts at the bank. Over 12 months beginning in December of 2015, those customers received €22.6 billion via 593,000 wire transfers and paid €23.5 billion to counterparties in 732,000 separate wires. According to FinCEN, 90% of ABLV clients were shell companies in offshore jurisdictions conducting tens of billions of dollars in high-risk transactions from 2012 to 2017.[68]

ABLV had already come to the attention of the FCMC. After a first inspection in 2014, the supervisor found no regulatory breaches. However, after a further inspection the following year, in 2016 the FCMC fined the bank for over €3.1 million for inadequate internal controls and issued a reprimand against the board member responsible for AML. In 2017, following allegations by the US that the bank was circumventing sanctions imposed against North Korea, FCMC carried out another inspection of the bank, and this resulted in an administrative agreement in which the parties agreed to dismiss the matter without imposing any fines, given they had already been given in 2016.[69]

While ABLV had already been associated with the Moldovan Bank Fraud and evasion of international sanctions by North Korea, the FinCEN notice brought new serious allegations. These included facilitating the illicit transfer of assets and funds from a Russia-based bank; funneling billions of dollars on behalf of a Ukrainian billionaire accused of embezzlement; large-scale corruption and money laundering by a top-level official in Azerbaijan; and bribery of Latvian officials to influence their regulatory actions. According to FinCEN, ABLV employees actively supported the schemes by producing fraudulent documentation of the highest quality. [70]

Despite the association with earlier money laundering cases and the severity of the FinCEN allegations, in July 2018 the FCMC allowed the bank to proceed with voluntary liquidation and let its shareholders, who were also its chief officers, oversee the process. The move has been widely criticised by government actors, the FIU and civil society, which argued that voluntary liquidation might lead to the loss of essential information and the cover-up of potential financial crimes. [71] In the same month, the State Police changed the status of an inquiry on the bank it had started in February into a criminal case. [72]

In January 2020, Latvian law enforcement authorities raided the bank headquarters partly in connection with suspicions that at least €50 million may have been laundered between 2015 and 2018.[73] Later that year, in June, the State Police carried out another search at 45 bank-related addresses and detained a number of persons, including employees of the bank suspected of having facilitated the schemes. [74] In March and June 2021, in connection with the case, the State Police also seized shares in several Latvian companies belonging to ABLV's owners and executives.[75] The investigations are still ongoing.

In spite of Latvia having already taken some steps to mitigate money laundering risks, international observers were still not satisfied. In August 2018, MONEYVAL published a report in which it identified several remaining shortcomings in the country's AML system, including (but not limited to) the slow pace of change of business model among non-resident banks.[76] On the basis of the report, the FATF

[68] https://www.occrp.org/en/troikalaundromat/ablv-connection
[69] OECD (2019), "implementing the OECD Anti-Bribery Convention – Phase 3 Report: Latvia", https://www.oecd.org/corruption/anti-bribery/OECD-Latvia-Phase-3-Report-ENG.pdf
[70] https://www.fincen.gov/news/news-releases/fincen-names-ablv-bank-latvia-institution-primary-money-laundering-concern-and
[71] https://en.rebaltica.lv/2019/03/in-the-shadows-of-ablv-from-regulator-to-a-friend/
[72] https://eng.lsm.lv/article/economy/banks/ablv-criminal-case-confirmed-over-money-laundering-suspicions.a294841/
[73] https://eng.lsm.lv/article/society/crime/ablv-bank-raided-as-part-of-50-million-euro-money-laundering-investigation.a346380/
[74] https://eng.lsm.lv/article/society/crime/major-police-search-carried-out-at-ablv-bank-in-latvia.a363735/
[75] https://www.delfi.lv/news/national/criminal/ari-prokuratura-uzlikusi-arestu-ernesta-berna-mantai.d?id=53349007
[76] https://www.coe.int/en/web/moneyval/-/moneyval-publishes-a-report-on-latvia

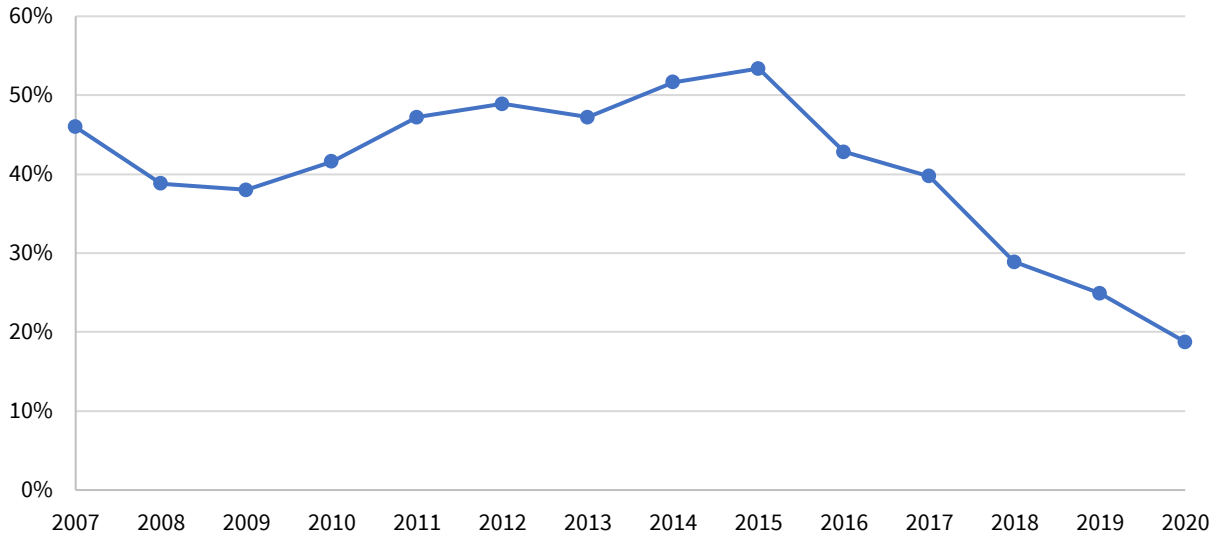
imposed a 1-year observation period, warning that the country would be included in its "grey list" of jurisdictions under increased monitoring if the shortcomings were not addressed.[77]

To avoid the devastating consequences of being included in FATF's gey list, the government acted on several fronts to fix the shortcomings identified by MONEYVAL. Amongst other things, it strengthened capacity and coordination mechanisms among AML institutions, it changed the legal status of the FIU to give it more powers and independence, and it struck off thousands of Latvian companies with no declared beneficial owners. In the meanwhile, the FCMC oversaw the termination of banks' relationships with 27,000 shell companies following the ban.[78]

As a result of these measures, the significance of Latvia as a regional hub for international transactions has waned. The volume of foreign deposits in Latvia's bank system declined by 74% between 2015 and 2019 (from €12.4bn to €3.4bn). At the end of 2020, they accounted for 18,8% of the total.[79] At the same time, the value of cross-border transactions in foreign currencies declined considerably, from €60.2bn in incoming transactions and €50.1bn in outgoing transactions in 2017 to €16.3bn in incoming transactions and €11.2 billion in outgoing transactions in 2019.[80]

At the beginning of 2020, MONEYVAL published a Technical Compliance Report in which it positively assessed Latvia's progress in AML reforms, and the FATF decided not to include the country in the grey list.[81] According to Latvia's FIU, even though nowadays the risk of money laundering through Latvian banks has significantly decreased, there is a need for continued supervision and more attention must be paid to e-money and digital payment systems, which are slowly replacing traditional banking channels for high-risk customers. This issue will be discussed more in detail later in the report.[82]

Chart 1 - Share of non-resident deposits in Latvian banks, 2007-2020



Source: Financial and Capital Market Commission

[77] Financial Intelligence Unit of Latvia, National ML/TF/PF Risk Assessment 2017-2019 (Executive Summary), https://fid.gov.lv/uploads/files/2021/NRA_2017_2019_Executive_Summary%20%28002%29.pdf
[78] Ibid.
[79] https://www.fktk.lv/en/statistics/credit-institutions/quarterly-reports/
[80] Financial Intelligence Unit of Latvia, National ML/TF/PF Risk Assessment 2017-2019 (Executive Summary)
[81] https://rm.coe.int/anti-money-laundering-and-counter-terrorist-financing-measures-latvia-/16809988c1
[82] Financial Intelligence Unit of Latvia, National ML/TF/PF Risk Assessment 2017-2019 (Executive Summary)

Non-resident banking and money laundering in the other Baltic countries

Even though Latvian banks were the major players in the export of banking services to high-risk customers in the FSU, a series of journalist investigations in the last four years revealed that the non-resident banking business model was replicated by banks in Lithuania and Estonia, including Scandinavian banks (i.e., Danske Bank and Swedbank), that were previously believed to be "clean".

In Estonia, Danske Bank came under scrutiny in 2017, when journalists from the Danish newspaper Berlingske, OCCRP and other 15 media organisations across the world, revealed the central role of its Estonian branch in laundering at $2.9 billion for Azerbaijan's ruling elite between 2013 and 2015 (see box below).[83] Part of that money was also used in the so-called "Caviar Diplomacy" case, in which European politicians at the Council of Europe were provided with expensive gifts and favours to turn a blind eye to Azerbaijan's violations of human rights in the country.[84]

The Azerbaijani Laundromat

The Azerbaijani Laundromat was a $2.9 complex money laundering operation and slush fund used by the Azerbaijani ruling elite between 2013 and 2015 to silence human rights violations, create a positive image of the country abroad, buy luxury goods and benefit themselves. The scheme used mainly four anonymous shell companies registered in the UK with accounts in the Estonian branch of Danske Bank. These were used to transfer millions to accounts of companies and individuals across the world.[85]

Almost half of the money (over $1.45 billion) came from an account held in the International Bank of Azerbaijan by a shell company linked to the family of Azerbaijan's president Ilham Aliyev. The remnant came directly from government ministries and agencies as well as large private companies linked to the regime and from a state-owned Russian arms exporter. The money was received by top-level Azerbaijani officials, including a former deputy prime minister, the head of the anti-corruption body and the head of the foreign intelligence and their close circle.

After the Azerbaijani Laundromat revelations, Danske Bank hired the Danish law firm Bruun & Hjejle to investigate AML breaches in its Estonian branch. In September 2018, the bank published the audit report which confirmed that, in a period of over nine years, the foreign banking division of Danske Estonia had carried out systematic money laundering, helping figures from the FSU wash as much as $230 billion.[86] A 2014 audit by the Estonian financial regulator provides a detailed account of the many obvious signs of money laundering and how bank officers blatantly ignored them.[87]

Non-resident banking was a very profitable business for Danske Estonia. As of 2013, foreign customers generated profits of $52 million, representing 99% of profits of the foreign banking unit, and a return on capital of 402%. According to a former account manager at the bank, it was so profitable because non-residents had to pay $90 per cross-border transaction, whereas they normally cost the bank $1.

[83] https://www.occrp.org/en/azerbaijanilaundromat/
[84] https://www.esiweb.org/publications/caviar-diplomacy-how-azerbaijan-silenced-council-europe
[85] https://www.occrp.org/en/azerbaijanilaundromat/
[86] https://danskebank.com/-/media/danske-bank-com/file-cloud/2018/9/report-on-the-non-resident-portfolio-at-danske-banks-estonian-branch.pdf?rev=56b16dfddae94480bb8cdcaebeaddc9b&hash=B7D825F2639326A3BBBC7D524C5E341E
[87] https://www.occrp.org/en/investigations/newly-obtained-audit-report-details-how-shady-clients-from-around-the-world-moved-billions-through-estonia

The only performance measure used to determine bonuses for account managers was the number of transactions handled. As such, they were directly motivated to get as many clients as possible.[88]

In late 2015, Deutsche Bank and Bank of America cut off Danske Estonia branch from their dollar-clearing services, leaving it without access to dollars. Danske Bank's executives tried to sell its Baltic operations without success. Eventually, Danske Bank disbanded the branch's foreign banking division.[89] In 2018 there were devastating consequences for the bank. Its CEO resigned and was later charged for neglect of duties[90], the bank's shares fell by half[91], and ten former employees were arrested[92]. In 2019, the Estonian government mandated the bank to close its Estonian branch.[93]

Partly as a result of Danske Estonia's demise, the share of non-residents in banking in Estonia fell from 19.10% at the end of 2014 to around 7.91% at the end of 2018, with the steepest fall from 8.50% to 0.46% related to deposits from very high-risk jurisdictions, including offshore locations. In late 2018 and early 2019, the Estonian banking supervisor Finantsinspektsioon carried out extraordinary AML inspections at all banks operating in Estonia and concluded that the risks to Estonian banking from serving non-residents had been substantially reduced.[94]

In Lithuania, most of the non-resident banking business was carried out by one bank, Ūkio Bankas, which, together with the Russian investment bank Troika Dialog, was at the centre of the "Troika Laundromat". The scheme, uncovered by OCCRP in 2019, allowed Russian oligarchs and politicians to siphon out of the country $4.8 billion between 2006 and 2013 (see box below).[95] An inspection in early 2013 revealed that the Ūkio had poor asset quality, weak risk management and lack of proper operating data. The bank eventually went bankrupt in the same year. [96]

The Troika Laundromat

The Troika Laundromat was a money laundering scheme, run from 2006 to 2013, which allowed Russian oligarchs and politicians to secretly acquire shares in state-owned companies, to buy real estate in Russia and abroad, purchase luxury yachts, pay medical bills and much more.[97] Journalist investigations on the scheme found links tying almost almost 200 million US dollars to well-known crimes in Russia, including a fuel price scam at Moscow's Sheremetyevo airport in 2012 and a tax rebate scam which ended with the death of a Russian whistle-blower, Sergei Magnitsky, in 2009.

Troika Dialog, once Russia's largest private investment bank, was the operator of the scheme, in partnership with the Lithuanian bank Ūkio Bankas. Troika enabled the flow of $4.6 billion into the system and directed the flow of $4.8 billion out. Troika initially "circulated" the money between different accounts before sending it on to Ūkio, which set up and organized transfers between accounts of at least 35 shell companies. The majority of transfers were represented as allegedly false contracts for the sale of physical goods. Counterparties to these transactions included major Western banks such as Citigroup Inc., Raiffeisen and Deutsche Bank.

[88] https://www.icij.org/investigations/fincen-files/inside-scandal-rocked-danske-estonia-and-the-shell-company-factories-that-served-it/
[89] Ibid.
[90] https://www.reuters.com/article/us-danske-bank-moneylaundering/ex-danske-ceo-borgen-charged-over-money-laundering-case-report-idUSKCN1SD1P3
[91] https://www.bloomberg.com/news/articles/2018-12-27/danske-has-half-its-value-wiped-away-but-will-2019-be-better
[92] https://www.reuters.com/article/us-danske-bank-moneylaundering/estonia-makes-first-arrests-over-danske-money-laundering-idUSKBN1OI0NL
[93] https://www.nytimes.com/2019/02/20/business/danske-bank-estonia-money-laundering.html
[94] https://www.fi.ee/en/news/risks-associated-serving-non-residents-have-declined-estonian-financial-sector
[95] https://www.occrp.org/en/troikalaundromat/
[96] https://voices.transparency.org/lithuanias-money-laundering-problem-c3b3ebba1618
[97] https://www.occrp.org/en/troikalaundromat/

While the share of non-resident deposits in Lithuania fell after the collapse of Ūkio,[98] Lithuania still seems to have significant shortcomings when it comes to AML. In a 2017 evaluation, the OECD concluded that banking supervision in the country appeared to be insufficient and lacking resources.[99] In 2018, the FATF noted some progress on this aspect, but criticised the National Risk Assessment for not addressing the risks around cross-border illicit payments. The FATF also reported that the country's FIU is ill-equipped in terms of staffing and analytical tools.[100]

Other investigations by Swedish journalists and OCCRP in 2019 and 2020 revealed how the Baltic branches of Swedbank were also engaged in the non-resident banking business, enabling political corruption in Russia and Ukraine as well as playing a role in other prominent cases, including the Magnitsky affair and the Azerbaijani Laundromat.

A 2019 report by OCCRP revealed how the Estonian branch of the bank handled massive sums for the Russian oligarch Mikhail Abyzov, who was arrested in March 2019 on accusation of secretly acquiring shares in energy deals while he was minister, defrauding the Russian government and investors of $60 million and running a criminal organisation.[101] According to the investigation, between 2011 and 2016, a total of $860 million went into Swedbank accounts of Abyzov-related companies and roughly $770 million was taken out via more than 3,300 transactions.

Another investigation by the Swedish broadcaster SVT in 2020 revealed that between 2007 and 2015 a total of $5.8 billion of suspicious funds was transferred to around 50 accounts in Swedbank by companies with accounts in Danske Bank's Baltic branches and mentioned in the Azerbaijani laundromat. This included $26 million linked to the Magnitsky affair.[102] SVT also showed that Swedbank's suspicious money also flowed through its Lithuanian branch, including an alleged $4.2 million bribe transferred for the ultimate benefit of Ukraine's ex-president Viktor Yanukovych.[103]

The Swedbank exposé led to an independent inquiry commissioned by the bank and carried out by the law firm Clifford Chance. The final report, published in March 2020**,** found that the bank and its Baltic branches actively sought clients with a high-risk profile and reportedly passed around $40 billion in high-risk transactions between 2014 and 2019, ignoring their AML duties.[104] Swedbank also hid information from authorities during on-site and off-site inspections by Swedish authorities. In March 2020, the Swedish banking supervisor slapped Swedbank with a $386 million fine for AML breaches.[105]

The FinCEN files and ongoing risks

In September 2020, the International Consortium of Investigative Journalists (ICIJ), Buzzfeed and other 108 news organisation reported about the "FinCEN files", a global-scale investigation based on a leak of 2,100 Suspicious Activity Reports (SARs) filed to FinCEN between 2006 and 2017.[106] The files identified at least US$ 2 trillion in transactions potentially related to money laundering, corruption, and other

[98] https://www.lb.lt/en/deposits-by-residency
[99] https://www.oecd.org/corruption/anti-bribery/Lithuania-Phase-2-Report-ENG.pdf
[100] https://www.fatf-gafi.org/countries/j-m/lithuania/documents/mer-lithuania-2018.html
[101] https://www.occrp.org/en/investigations/swedbanks-high-risk-secrets
[102] https://www.svt.se/special/swedbank/english/
[103] https://www.svt.se/special/swedbank/english/yanukovych/
[104] https://internetbank.swedbank.se/ConditionsEarchive/download?bankid=1111&id=WEBDOC-PRODE57526786
[105] https://www.reuters.com/article/us-europe-moneylaundering-swedbank-idUSKBN2163LU
[106] https://www.icij.org/investigations/fincen-files/

crimes. The investigation not only shed light on past and present criminal cases, but it also revealed the role of global banks in enabling the circulation of illicit financial flows.

The investigation also provided additional evidence of the prominent role of Baltic banks in handling suspicious money. According to Re:Baltica, the leaked files show that at least $7.6 billion of suspicious money flowed through 9 Latvian banks between 2006 and 2017.[107] Furthermore, a side-investigation by the ICIJ, based on a leak of Estonian police files, also revealed how officers at Danske Bank Estonia secretly ran a company formation agency that helped clients from Russia and other FSU countries launder billions of dollars through accounts at the bank.[108]

As we discuss in the following sections, such findings raise significant concerns about the ongoing risks related to the abuse of shell companies and uncontrolled company formation activities across the globe.

The shell games

Shell companies, non-resident banking and laundromats

The use of shell companies across multiple jurisdictions offering secrecy for their ultimate owners was an essential component of the non-resident banking business model in the Baltic countries as well as a regular feature of the Laundromats and of other cases. As revealed by the investigations, criminal networks used not only shell companies registered in notorious offshore jurisdictions, such as the British Virgin Islands (BVI), Seychelles, Belize or Panama, but also, first and foremost, shell companies in reputable jurisdictions such as the United Kingdom (UK) and New Zealand.

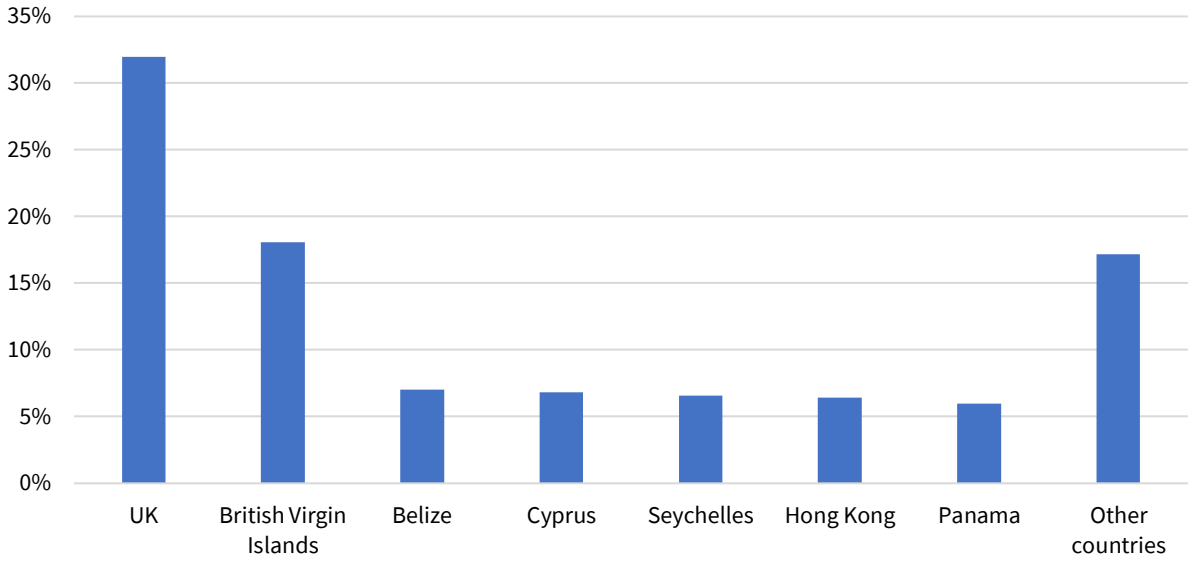
The majority of shell companies in the core platforms used in the Laundromats were registered in the UK.[109] The Russian Laundromat used 440 UK shell companies, 270 with accounts in Latvian banks and 122 with accounts in Estonian banks. The criminal network behind the Moldovan fraud used 48 UK shell companies for its carousel transactions. For its core operations, the Azerbaijani laundromat used mainly four UK Limited Partnerships owned by anonymous shell companies based in the BVIs, Seychelles and Belize. The Troika Laundromat used a platform of 75 UK companies.[110]

According to Transparency International UK (TI-UK), there are at least three reasons why the UK was the jurisdiction of choice for shell companies used in the Laundromats. First, incorporating a shell company in the UK is cheap and easy. It takes as little money as £12 and as little time as three days. Second, UK companies offer a veil of legitimacy and are likely to raise less suspicion in banks compared to shell companies registered in traditional offshore locations. Third, until 2016, there was no requirement for UK companies to declare their beneficial owners, making them effectively anonymous.[111]

[107] https://en.rebaltica.lv/2020/09/what-the-fincen-files-reveal-about-latvia/
[108] https://www.icij.org/investigations/fincen-files/inside-scandal-rocked-danske-estonia-and-the-shell-company-factories-that-served-it/
[109] Transparency International Latvia / Delna (2018), *Connections – Money Laundering in Latvia and the Role of Company Service Providers*
[110] https://www.occrp.org/en/troikalaundromat/
[111] Transparency International UK (2017), *Hiding in Plain Sight – How UK Companies Are Used to Launder Corrupt Wealth*, https://www.transparency.org.uk/sites/default/files/pdf/publications/HidingInPlainSight_WEB3.pdf

Data from the FCMC provides evidence of the shift from traditional offshore jurisdictions to the UK. The share of UK companies with accounts in Latvian banks jumped from 14% in 2011[112] to around 32% in February 2018.[113] It is unclear how many of them had deposits at ABLV; the bank's own audit shows that UK clients were excluded from the high-risk client category. The bank only categorised as high-risk those transactions directly involving CIS countries and/or secrecy jurisdictions, which totalled only roughly one third of incoming and outgoing payments.[114]

Chart 2 - Proportion of shell companies with deposits in Latvian banks* by country of residence, February 2018



*Data refers to 15 banks, excluding ABLV Bank and 5 bank branches in Latvia. The total number of shell companies was 17,107.

Source: Financial and Capital Market Commission

The significance of UK companies for financial crime goes well beyond the Laundromat investigations. In a report published in late 2019, TI-UK identified at least 929 UK companies involved in 89 corruption and money laundering cases across the world, for a total economic damage of around €159 billion. In addition, TI-UK has identified 17,000 legal entities controlled by at least one individual or company that acted as officers for entities involved in economic crime. More than 5,400 of them were still active as of October 2019.[115]

Different types of UK companies were used in money laundering schemes, including Limited Liability Companies (LLCs) and partnership structures such as Limited Partnerships (LPs), Scottish Limited Partnerships (SLPs) and Limited Liability Partnerships (LLPs). While LLCs were required to disclose their

[112] Transparency International Latvia / Delna (2018), *Connections – Money Laundering in Latvia and the Role of Company Service Providers*
[113] Data provided by the FCMC in email correspondence in June 2018.
[114] ABLV Group (2016) *ABLV Group Anti-Money Laundering Enterprise-wide Risk Assessment Report,* available at https://www.regulations.gov/document?D=FINCEN-2017-0013-0024 Exhibit 5, p36
[115] Transparency International UK (2019), *At Your Service – Investigating how UK businesses and institutions help corrupt individuals and regimes launder their money and reputations*

beneficial owners in 2016, partnership structures were not yet subject to this requirement and could even list entities in secrecy jurisdictions rather than real persons as partners.[116]

Not surprisingly, the rate of incorporation of these legal entities increased substantially shortly afterwards. The number of incorporated SLPs rose by 50% in 2016 alone. Investigative journalists at Bellingcat have analysed the incorporation documents of all the 5,216 SLPs incorporated in 2016 and found that 94% of these were controlled by corporate partners, among which 71% were based in secrecy jurisdictions (Seychelles, Belize, Dominica, St Kitts and Nevis, Marshall Islands) and only 5% in the UK.[117]

In mid-2017, pressured by evidence of heavy involvement of UK LPs and LLPs in financial crime, the British government closed the loophole and required both types of entities to disclose their beneficial owners. Thereafter, the incorporation rate of SLPs fell to its lowest level for seven years and it was 80% lower in the last quarter of 2017 than its peak at the end of 2015, which demonstrates the impact of beneficial ownership transparency in mitigating potential abuse of companies.[118]

A 2018 analysis of the UK company register by Global Witness shows that SLPs have been the legal entity of choice for people from the FSU. The proportion of companies whose declared beneficial owner was an individual with residence or citizenship in the FSU (including Baltic states) was as high as 43.15% for SLPs, compared to 6.16% for Scottish LLPs, the second most common type of entity used. Data on 35% of SLPs showed they had not yet completed the steps to find their beneficial owners 8 months after new rules (for other companies, it was 1%).[119]

Despite being responsible for around 40% of incorporations in the UK, as of January 2018 Companies House had only 20 people responsible for monitoring compliance with beneficial ownership declaration rules for over 4 million companies, and it had no responsibility for verification of the information, thus making it easier to file false or fraudulent information without getting caught.[120] In September 2020, the UK government published a reform plan for Companies House envisaging the introduction of a compulsory identity verification mechanism for companies' directors and BOs.[121]

Compounding the problem, Companies House is currently not tasked with verification of beneficial ownership and there is limited proactive follow-up, which not only increases the risk of misleading and inaccurate data, but it also makes it easier for potential criminals to file false or fraudulent information and get away with it. Until February 2018, the UK government had no plan to introduce automatic verification.

[116] Transparency International UK (2017), *Hiding in Plain Sight – How UK Companies Are Used to Launder Corrupt Wealth*
[117] Transparency International UK (2017), *Offshore in the UK: Analysing the Use of Scottish Limited Partnerships in Corruption and Money Laundering*, https://www.transparency.org.uk/publications/offshore-in-the-uk
[118] Global Witness (2018), *The Companies We Keep – What the UK's open data register actually tells us about company ownership*, https://www.globalwitness.org/en/campaigns/corruption-and-money-laundering/anonymous-company-owners/companies-we-keep/#chapter-0/section-0
[119] Ibid.
[120] Ibid.
[121] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/925059/corporate-transparency-register-reform-government-response.pdf

The worrying state of global beneficial ownership transparency

In April 2018, in response to the ABLV case, the Latvian government prohibited banks from servicing shell companies, defined as legal entities having at least one of the following three characteristics: i) lack of justification or evidence of their economic activity; ii) lack of premises for their economic activity; and iii) registration in jurisdictions that do not require filing of financial statements.[122] While this was instrumental to mitigate money laundering risks through Latvian banks, the risk of abuse of shell companies for money laundering elsewhere is still very high.

Given the increased alertness among financial institutions to the risks linked to UK companies, it is likely that money launderers will keep systematically searching for other "prestigious" jurisdictions offering easy and low-cost incorporation and *de facto* secrecy of beneficial ownership information, a phenomenon called "jurisdiction mining" by scholar Graham Stack.[123] For example, already for some years there has been evidence of abuse of Canadian companies for money laundering (a practice called "snow washing") for the very same reasons.[124]

The risk of abuse of shell companies across multiple jurisdictions is exacerbated by the worrying situation regarding beneficial ownership regulation worldwide. A 2020 study by the Tax Justice Network found that out of 112 jurisdictions, only 23 had achieved full beneficial ownership transparency. Even fewer (6) published this information online in a centralized register.[125] Furthermore, a 2021 analysis by Transparency International shows that the majority of EU Member States are lagging behind with beneficial ownership transparency and accessibility. Three Member States – Hungary, Italy, and Lithuania – have not even set up a beneficial ownership register yet.[126]

Though the 5th EU AML Directive mandates for public availability of beneficial ownership registers, access and data format is left at the discretion of national authorities. In practice, in many countries this has translated to high paywalls for their use as well as user-unfriendly formats (e.g., PDFs or scanned documents). Some countries have opposed publication of beneficial ownership information on privacy grounds. However, reviews of the UK company register have shown that the impact is minimum and that solid mechanisms can be established to deal with this issue.[127]

Latvia, along with Denmark[128] and Slovakia[129], is a positive exception to this trend. While the public availability of beneficial ownership information was already introduced in April 2018, its accessibility has progressively increased. Even though full access to the register, including the possibility to check company filings and use in-built visualisation tools, is only available to persons with a Latvian ID, in October 2020 the beneficial ownership information register was made available in open format and according to the Beneficial Ownership Data Standard.[130]

---

[122] https://www.mk.gov.lv/en/article/saeima-imposes-ban-servicing-shell-companies
[123] Stack G. (2015), "Shell companies, Latvian-type correspondent banking, money laundering and illicit financial flows from Russia and the Former Soviet Union", *Journal of Money Laundering Control,* vol.18, no.4, pp. 496-512
[124] https://www.theglobeandmail.com/world/article-snow-washing-what-leaked-banking-records-show-about-canadas-role/#:~:text=Subscribe-
[125] Tax Justice Network (2020), *The state of play of beneficial ownership registration in 2020*, https://taxjustice.net/wp-content/uploads/2020/11/State-of-play-of-beneficial-ownership-Update-2020-Tax-Justice-Network.pdf
[126] Transparency International (2021), *Access Denied? Availability and Accessibility of Beneficial Ownership data in the European Union*, https://www.transparency.org/en/publications/access-denied-availability-accessibility-beneficial-ownership-registers-data-european-union
[127] https://www.openownership.org/uploads/oo-data-protection-and-privacy.pdf
[128] Beneficial ownership data for Danish Companies are available on the website of the Central Business Register – https://datacvr.virk.dk/data/?&language=en-gb
[129] In the case of Slovakia, beneficial ownership data is available in open data only for companies with public contracts and not for all companies in the beneficial ownership register – https://rpvs.gov.sk/rpvs
[130] https://data.gov.lv/dati/lv/dataset/plg-bods

While this is expected to mitigate the risk of abuse of Latvian legal entities, in light of the above considerations, the progress at EU level is still too slow and inadequate to deal with the Laundromats and other money laundering scandals revealed in the past few years.

The role of Trust and Company Service Providers

The ease with which legal entities can nowadays be created and dissolved in many jurisdictions, has raised concerns not only about the abuse of "prestigious" shell companies for money laundering, but also about the "enablers" who help to create them, including Trust and Company Service Providers as well as non-financial professionals such as lawyers and accountants. Fast and cheap online incorporation services, while reflecting governments' efforts to facilitate business in their country, have also given rise to the development of a sector that is increasingly difficult to control.

For example, nowadays there are thousands of businesses across the world operating in this area, giving life to a proper market for shell companies, in which they are sold to customers or traded with other TCSPs, along with additional services. Their websites often specify the names of the banks they work with, providing the details of the documents to be submitted on-line, guaranteeing short request processing periods and high confidentiality regarding customer information.

As we shall see in the following sections, these businesses, wittingly or unwittingly, played a role in the Laundromats and other major money laundering cases involving banks in Latvia and other Baltic countries. They helped set up the complex corporate infrastructures to carry out the schemes, by creating hundreds of shell companies across multiple jurisdictions and handling the opening of bank accounts for them, thus providing criminal networks access to the global financial system.

Business introducers and para-bank structures

TCSPs have been a key element of the non-resident banking business in Latvia. In many cases, they struck ad-hoc cooperation agreements with banks and acted as "marketing agents" for them, actively looking for new clients to bring in across countries of the FSU. At times, they also took the form of "para-bank" structures (e.g., sharing premises, telephone numbers, or employees with the bank). In some cases, banks advertising offshore services would address clients to the affiliated TCSPs to arrange bank accounts.[131]

A previous report from Transparency International Latvia describes in detail how TCSPs were behind all of the major money laundering cases involving Latvian banks, including the Magnitsky affair, cases of embezzlement by political elites in Ukraine and Central Asia, the Russian Laundromat, the Moldovan Bank Fraud and several other schemes.[132] Investigations around the Azerbaijani Laundromat, Troika Laundromat and FinCEN files have provided additional evidence and details about their operations and role in the money laundering machinery.

[131] Stack G. (2015), "Shell companies, Latvian-type correspondent banking, money laundering and illicit financial flows from Russia and the Former Soviet Union", *Journal of Money Laundering Control,* vol.18, no.4, pp. 496-512

[132] Transparency International Latvia / Delna (2018), *Connections – Money Laundering in Latvia and the Role of Company Service Providers*

According to Re:Baltica out of the 3,267 UK LLPs and LPs mentioned in the FinCEN files, more than half (1,656) were created by loose but well-organised networks of Trust and Company Service Providers, run by individuals living in the Baltics or Baltic nationals living in the UK**.** These also included "shell company factories" – service addresses or non-descript buildings hosting hundreds of shell companies.[133]

For example, two TCSPs run by Latvian nationals and with operations in the UK and Latvia incorporated at least 492 UK LPs and LLPs. The incorporation documents, financial statements and transaction invoices for such companies were signed either by the owners or officers of the TCSPs or by nominees, including former classmates.[134] According to the ICIJ, the TCSP would write a private power-of-attorney letter secretly transferring full control of the new company to its true owner, who, in exchange would indemnify the manager of the TCSP from any legal threat.

The case of International Overseas Services (IOS), one of the oldest TCSPs in Latvia, is emblematic. IOS was behind the core platform of shell companies and proxy directors used for the Magnitsky fraud.[135] In 2019, OCCRP found that it set up at least 35 of the 75 companies involved in the Troika Laundromat, providing them with nominee directors.[136] Other investigations show it was also behind some of the companies used in the Azerbaijani Laundromat.[137] In 2020, the ICIJ found that it was responsible for setting up and maintaining around 20% (646) of all UK LPs and LLPs in the FinCEN files.[138]

IOS operated under the "franchising principle", establishing agreements with other TCSPs operating in specific jurisdictions in order to attract new clients. In Latvia, IOS and its officers were found to have strong connections with a major UK-Latvian TCSP, Anderson Baltic, which in turn had connections with ABLV Corporate Service Holding, a subsidiary of the bank offering advice on offshore corporate management and other services. A 2019 investigation by OCCRP shows how a IOS legal officer took over part of such business just two months before US intervention (see box below).[139]

IOS & ABLV

Leaked transaction records from the Troika Laundromat investigation show that IOS received $5.3 million from clients and paid out $5.6 million from March 2006 through August 2013. These transactions were labeled as payments for legal or consulting services, and over 60% of them went to Anderson Consulting Company, a TCSP with operations in Latvia and the UK, which shared an address with the IOS office in Riga.[140]

According to a 2019 investigation by OCCRP, at the beginning of December 2017, Anderson Baltic SIA took a 60% stake in ABLV Corporate Services Holding Company, a subsidiary of the bank that advised clients on setting up offshore companies, optimizing tax obligations, and obtaining EU residence permits. Later that month, the 60% was transferred to the owner of Anderson Baltic personally, who in turn transferred 30% of his stake to ABLV's Charitable Foundation, legally independent from the bank but owned by its shareholders. In other words, ABLV Corporate Services Unit moved outside the bank in the run-up to the FinCEN decision, but it was still controlled by the same people.

[133] Transparency International UK (2019), *At Your Service – Investigating how UK businesses and institutions help corrupt individuals and regimes launder their money and reputations*
[134] https://www.icij.org/investigations/fincen-files/inside-scandal-rocked-danske-estonia-and-the-shell-company-factories-that-served-it/
[135] https://www.reportingproject.net/proxy/en/the-latvian-proxies
[136] https://www.occrp.org/en/troikalaundromat/behind-the-curtain
[137] https://www.irishtimes.com/news/ireland/irish-news/the-fincen-files-the-billion-dollar-a-month-money-trail-1.4358331
[138] https://www.icij.org/investigations/fincen-files/inside-scandal-rocked-danske-estonia-and-the-shell-company-factories-that-served-it/
[139] https://www.occrp.org/en/troikalaundromat/ablv-connection
[140] Ibid.

Despite evidence that IOS-linked companies featured in major money laundering cases, there is no evidence that IOS and their officers knew about the criminal intentions of the clients using the shell companies they provided, even though they did take steps to hide their identity. The now inactive website of IOS says the agents involved would stop working together under its name, however, as of September 2020, data from Companies House shows that they are still active and maintaining hundreds of shell companies.[141]

TCSPs were also used by the Foreign Client Division of Danske Estonia. The Bruun & Hjejle report shows that a large proportion of the 1,200 UK companies that held accounts there obtained them through 25 agents, who received commissions for their efforts in locating customers. An investigation by the ICIJ and Baltic journalists, based on the FinCEN files and a leak from the Estonian police, shows that bankers themselves were secretly running a TCSP that incorporated UK shell companies used in the Azerbaijani laundromats and showed up in thousands of other suspicious transactions.[142]

Danske Estonia's secret TCSP[143]

The Estonian police records, obtained by ICIJ's Italian partner, L'Espresso, reveal that the Danske Estonia bankers — required by law to vet their customers to prevent money laundering — instead ran a secret company that worked with formation agencies to create U.K. LLPs and LPs for Danske Estonia clients. Beta Consult Corp., a company registered in the Marshall Islands and unwittingly owned by a businessman in the Ukraine. Interviewed by ICIJ, the businessman said he knew nothing about Beta Consult and its offshore business.

Beta Consult had its own account at Danske Estonia and other customers of the bank — often UK shell companies incorporated by Beta Consult itself — made dozens of payments into it. There was a secret invoicing system for UK LLPs and LPs, in which the last digit of the invoice number issued by Beta Consult was part of a code that linked sales to at least nine Danske Estonia officers, including the manager of the foreign banking division.

As of 2018, authorities believed that at least 12 former Danske Estonia officers conspired to hide $786.18 million in suspicious transactions ($284.2 million amounted to laundering). Since then, their investigations have widened and investigators are looking into up to $2 billion in suspected money laundering. After Danske Estonia's foreign banking division was shuttered in 2015, former staffers became consultants working with TCSPs forming UK shell companies.

There are indications that at least up to mid-2017 (thus well into the first crackdown on money laundering) the use of company service providers was still relatively common among Latvian non-resident banks. According to MONEYVAL, as of 30 June 2017**,** 5 banks and one branch were using a total of 563 agents with authorization for customer identification in 35 different jurisdictions; 3 banks were using 170 agents with no authorization for customer identification in 21 jurisdictions; 1 bank was using 1 agent with authorization for both; 1 bank was banned by the FCMC to use services of agents.[144]

MONEYVAL identified significant deficiencies in regard to the reliance of non-resident banks on agents, which, partly due to a loophole in CDD regulation, did not ensure adequate and regular control of the quality of customer identification performed by the agents, thus exposing themselves to an unacceptable

[141] https://www.icij.org/investigations/fincen-files/inside-scandal-rocked-danske-estonia-and-the-shell-company-factories-that-served-it/
[142] Ibid.
[143] Ibid.
[144] MONEYVAL (2018), *Fifth Round Mutual Evaluation Report,* https://rm.coe.int/moneyval-2018-8-5th-round-mer-latvia/16808ce61b

level of ML risk. According to MONEYVAL, TCSPs themselves relied on third parties – mainly partner TCSPs from other countries – for customer introduction. However, they had a very remote understanding of their role as providers or receivers of third-party services in particular.

The banks met onsite by MONEYVAL indicated that over the last couple of years the use of agents with or without authorization for customer identification significantly decreased due to both economic and regulatory reasons. This, together with the prohibition for banks to service shell companies, makes it much less likely for TCSPs to be a threat to Latvia's financial system. At the same time, as we shall see below, their vulnerability for money laundering and financial crime is still relevant, and there is need for sustained supervision.

TCSP supervision in Latvia

TCSPs' company formation activities are often carried out across different jurisdictions, and this has posed challenges for their supervision. For example, TCSPs forming companies in the UK have not been bound by UK AML regulation (which mandates them to have a license) if they are not registered in the UK.[145] Even though as part of the reform plan for Companies House only TCSPs registered with UK supervision authorities will be able to form UK companies[146], supervision of AML compliance for TCSPs based in Latvia and incorporating UK companies has so far rested on authorities in Latvia.

In Latvia, company formation services are mainly provided by three categories of businesses – legal service providers, tax advisors and outsourced accountants**.** The State Revenue Service is in charge of their supervision and monitoring their compliance with AML laws. As shown by national ML risk assessments, their vulnerability to money laundering has been medium-high due to a combination of factors, including lack of internal AML capacity and weak compliance with AML rules, lack of licensing, and ineffective sanctions for breaches to the AML law.[147]

According to the latest National Money Laundering Risk assessment, at the end of 2019 there were 1,023 TCSPs under the supervision of the SRS. Around 20% of them served high-risk customers, 13.5% of which were customers from CIS countries.[148] Latvia's FIU has observed that some of their services, including incorporation of shell companies, provision of nominee services, preparation of financial statements, signature of transaction invoices, purchase of properties, are being used for increasingly sophisticated financial crime schemes.[149]

While supervision in this area was initially weak, the SRS has increased its capacity and knowledge in the last couple of years, and supervisory measures have increased in intensity. For example, while in 2018 the SRS suspended activities for one TCSP and applied fines of €2,500 to another four, in 2019 it took 5 decisions of suspension of activity and applied a €52,300 fine to 37 other TCSPs. The most

[145] Transparency International UK (2019), *At Your Service – Investigating how UK businesses and institutions help corrupt individuals and regimes launder their money and reputations*

[146] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/925059/corporate-transparency-register-reform-government-response.pdf

[147] Financial Intelligence Unit of Latvia (2018) – *National Terrorism Financing and Proliferation Financing Risk Assessment Report 2017-2018*, https://fid.gov.lv/uploads/files/English%20version/ENG_TF_PF_report_FINAL_updated_2019.pdf

[148] Information provided by the State Revenue Service in June 2021

[149] Financial Intelligence Unit of Latvia, National ML/TF/PF Risk Assessment 2017-2019 (Executive Summary)

common violations included lack of internal control systems, insufficient understanding of clients' activities and associated risks, failure to identify BOs and report transactions.[150]

At the same time, even though STRs from TCSPs are normally expected to be lower compared to those filed by banks, the rate is still too low when seen in relation to the money laundering risk they pose. While in 2018, TCSPs filed no STRs at all, in 2019 only 2% of entities reported a total of 24 STRs. This might be due to a number of factors, including close relationships with and protection of the identity of the customers served, lack of sufficient knowledge about sophisticated money laundering typologies, and insufficient resources for CDD procedures.[151]

The government has taken steps to improve non-financial intermediaries' capacity to carry out CDD and report suspicious transactions, opening up the beneficial ownership register and setting up "goAML", a system developed by the United Nations that allows regulated entities to easily and swiftly report transactions to the FIU.[152] However, given that at present there is no need for TCSPs to obtain a license for AML capacity and/or quality of the service offered, it will be difficult to raise the bar of compliance of firms and individuals operating in the sector.

The government has recognised the problem and in 2021 amended the "Law on Accountancy" to introduce licensing requirements for outsourced accountants starting from 2023. This is a step forward, but it presents some complications. The law has been criticised by the Latvian Association of Accountants for being too demanding for small businesses and overly focusing on AML rather than quality of service.[153] A further problem is that the law covers only one of the relevant business categories that could also provide company formation services.

At present, there are no plans to extend licensing to tax advisors and legal service providers, though the SRS has stressed that licensing would be desirable.[154] Given the decreased, but still present, money laundering risk posed by uncontrolled TCSP activity, licensing of tax advisors and legal service providers offering company formation services might be an effective solution to mitigate the problem. As with financial actors, the withdrawal of the license would constitute a better deterrent and might also improve confidence among legitimate market operators.

More generally, there is a need for a more systematic, standardized and data-driven approach to TCSP supervision at the EU and global level, including for actions to improve cross-border supervision of their activities. While a tailored approach to the supervision of TCSPs has been more attractive for many jurisdictions, it has also resulted in a confusing array of laws governing an international industry that has become fully globalised. International standards would help to harmonise and catalyze government efforts and performance in this area.[155]

[150] Information provided by the State Revenue Service in June 2021
[151] Ibid.
[152] https://www.fid.gov.lv/en/e-reporting/reporting-system-goaml
[153] https://lvportals.lv/skaidrojumi/325691-arpakalpojumu-gramatveziem-bus-vajadzigas-licences-2021
[154] Interview with State Revenue Service, June 2021
[155] OECD (2021), *Ending the shell game: Cracking Down on the Professionals who enable Tax and White-Collar Crimes*

E-money – a new frontier for high-risk business?

There is widespread agreement that the crackdown on non-resident banking in the Baltic countries from the entire FSU has been an adequate response to the massive amount of money laundering that has taken place over the years. At the same time, there is also a need to reflect on the potential side-effects of the process of de-risking in Latvia, which has seen the mass-termination of Latvian commercial banks' relationships with thousands of high-risk clients in the former Soviet Union, a market segment they had been servicing for years.

Indeed, as revealed by a 2020 investigation by openDemocracy, there are clear indications that the progressive strengthening of AML measures and supervision among Baltic banks has coincided with a gradual migration of high-risk clients from the FSU to Electronic Money Institutions (EMIs) and Payment Institutions (PIs) as a replacement to traditional banking channels for international transactions.[156]

EMIs/PIs usually do not hold licenses for traditional banking operations (e.g., loans, investments, etc.) but facilitate fast payments across the world in Euro or other currencies by using correspondent banks, which hold deposits for them to back customers' accounts. They may serve not only individuals, but also corporate clients, including shell companies, in most cases through remote customer identification and non-face-to-face interactions – features that make them attractive to clients seeking anonymity.

The EMI business not only has parallels with the shell company formation business in the UK discussed earlier but has also become increasingly intertwined with it. The investigation found a number of Russian-language internet trades in UK shell companies with EMI accounts, EMI licences and even anonymous EMI providers on offer for determinate prices. One website even posted a video which explains how clients can set up an SLP and get credit cards issued by an EMI, which are sent to the firm's proxy address in Scotland and from there on to Russia or Ukraine.[157]

Perhaps not surprisingly, the investigation identifies several UK-registered EMIs run by or employing former executives and officers at Latvian non-resident banks that were involved in money laundering scandals or fined for insufficient AML compliance or breaches to the law.[158] All of them have subsidiaries in Latvia. At present, the major provider of correspondent accounts for British EMIs in Latvia seems to be Rietumu Banka. At the time of the investigation, its shareholders owned one of them, Decta, and the bank provided clearing services for it and five more EMIs.

Under the rules of the British Financial Conduct Authority (FCA), managers and directors of EMIs in the UK must prove to have a good reputation and sufficient knowledge of AML regulations in order to get a licence. The FCA has the power to suspend the operations or shut down those that do not comply with or breach the rules.[159] In Latvia, the FCMC monitors Latvian banks' compliance with risk assessment and customer diligence duties in the provision of correspondent accounts to foreign EMIs/PIs. Both FCA and FCMC are aware of the risks and act when needed.

In February 2020, the FCA suspended the operations of ePayments Systems Limited, one of the largest providers of services to FSU customers with correspondent accounts at Rietumu, for insufficient AML

[156] https://www.opendemocracy.net/en/dark-money-investigations/will-e-money-boom-make-uk-hub-money-laundering/
[157] https://offshore.su/blog/offshore_registration/scotland_company.html
[158] https://www.opendemocracy.net/en/dark-money-investigations/will-e-money-boom-make-uk-hub-money-laundering/
[159] Ibid.

controls and exposure to high-risk online business. According to the EMI's website in February 2021 it agreed on a phased re-opening of the business.[160] In June 2021, the FCMC issued a record fine (€5.85 million) against Rietumu Banka after having found it not to adequately address the risks associated with the activities of payment service providers to which it is providing correspondent accounts.[161]

In another recent case, the British EMI AltPay, set up in 2018 by a Latvian national who previously worked at Rietumu Banka, hired a former employee of ABLV who was arrested in early 2020 as part of the €50 million laundering investigation into the bank.[162] AltPay's manager dismissed the case as an unfortunate coincidence, and in interviews carried out by openDemocracy most of the former bankers have stressed that they do not compromise on anti-money-laundering checks and that there is little risk of repeating the bad practices of Latvian non-resident banks.[163]

Challenges in EMIs/PIs supervision in Latvia and abroad

In Latvia, the EMI and payment service industry has been developing in recent years, with a total value of transactions that reached €295 million in 2020 (€60 million more than in 2019).[164] While EMIs/PIs established in Latvia have to obtain a license from the FCMC, the EU Payment Services Directive allows EMIs and PIs in the European Economic Area (EEA) to freely provide services across the EU if they have been given a license to operate by their national regulator.[165] Consequently, nowadays there are dozens of such firms from a wide range of different European countries operating in Latvia.[166]

When it comes to AML, EMIs and PIs from EEA countries operating in Latvia are supervised by authorities in the Member State in which they have received a license. However, following amendments to the Payment Services and Electronic Money Law in 2018, they now have to register with the FCMC.[167] In situations when the FCMC detects potentially suspicious activities of foreign EMIs or irregularities in CDD or transaction monitoring, it exchanges information with the supervisory authorities in the relevant Member State.

Latvia's FIU attributes a medium-high money laundering risk to EMIs and PIs and it explicitly notes that high-risk clients formerly serviced by Latvian banks might move to this industry to carry out their transactions.[168] The FIU notes that following legislative amendments in 2018, which stipulated that EMI/PI customers must be related to Latvia, the number of registered EMIs in the country has dropped. Nevertheless, foreign EMIs free to provide services across the EU still pose a high money laundering risk for Latvia, as they may be established in countries with a weaker supervisory system.

Risks relate not only to financial institutions opening correspondent accounts with EMIs/PIs serving high-risk customers and shell companies, but also to the possibility that Latvian residents open accounts with foreign PIs/EMIs and make their payments opaque to Latvian authorities. The FIU has

[160] https://www.epayments.com/
[161] https://eng.lsm.lv/article/economy/banks/latvias-rietumu-banka-hit-with-record-fine-by-regulator.a409508/
[162] https://eng.lsm.lv/article/economy/banks/former-private-banker-detained-in-ablv-case.a346656/
[163] https://www.opendemocracy.net/en/dark-money-investigations/will-e-money-boom-make-uk-hub-money-laundering/
[164] https://lvportals.lv/norises/327780-maksajumu-iestades-strauja-attistiba-un-naudas-atmazgasanas-riski-2021
[165] https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en
[166] https://www.fktk.lv/en/market/payment-service-providers/electronic-money-institutions/service-providers-from-the-eea/freedom-to-provide-services/ ; https://www.fktk.lv/en/market/payment-service-providers/payment-institutions/service-providers-from-the-eea/freedom-to-provide-services/
[167] https://likumi.lv/ta/id/206634-maksajumu-pakalpojumu-un-elektroniskas-naudas-likums
[168] Financial Intelligence Unit of Latvia, National ML/TF/PF Risk Assessment 2017-2019 (Executive Summary)

observed a rapid increase in Latvian customers (both natural and legal persons) for EMIs/PIs licensed in neighbouring countries, and Lithuania in particular.

Following Brexit, many UK-licensed EMIs/PIs have begun opening subsidiaries in Lithuania, which offers relatively simple procedures for opening and licensing of EMIs.[169] Indeed, due to its business-friendly regulatory environment, Lithuania is currently one of the most attractive locations for FinTech firms (it ranks 10th in the Global FinTech Index[170]), and, partly due to the straightforward licensing process, it has become a leader in Europe when it comes to the number of EMIs/PIs operating in the country, with a payment volume of €115.8 billion in 2020.[171]

The growth of the industry has prompted the Lithuanian government to establish the Centre of Excellence in Anti-Money Laundering, whose purpose is to mobilise public and private efforts in tackling illicit financial flows.[172] However, a recent report from Transparency International Lithuania on the money laundering prevention capacity of FinTech firms, based on surveys to industry representatives, raises several concerns, especially when it comes to transparency of the sector, assessment of its risks and cooperation between public and private sector bodies.[173]

For example, a proportion of less than one in every ten companies publish their financial statements, and some companies do not even have a website. There is also a dearth of data and statistics on money laundering risks in the sector. In addition, as noted earlier in this report, Lithuania has not yet set up a beneficial ownership register, which makes scrutiny of the owners and operations of these firms even more difficult. This is worrying considering that since the beginning of 2021 corporations are also allowed to open accounts with e-money institutions.[174]

Apart from specific country cases, it might be argued that, while they are certainly promising in terms of financial inclusion and business growth, EMIs/PIs might also constitute the "worst of both worlds" in relation to money laundering risks. On the one hand, due to their small scale, sheer number, and cross-border operations, they resemble the TCSP industry and present similar problems of supervision and control. On the other hand, their potential to perform fast payments across the world in different currencies makes them akin to Latvian non-resident banks that used to offer the very same service.

As such in the future it will be of extreme importance, in the Baltic region and Europe at large, to improve cross-border cooperation on the supervision of these actors, harnessing new technologies and data analytics to mitigate risks and monitor transnational activities.

The EU's new AML package

Prompted by the growing concerns on money laundering, on 20 July 2021, the EU Commission presented an ambitious package of legislative proposals to strengthen the EU's anti-money laundering system. This includes the creation of a new EU AML authority (AMLA); a new regulation on AML containing directly applicable rules, including in the areas of Customer Due Diligence and beneficial

[169] https://www.lb.lt/en/news/steady-growth-big-names-and-a-focus-on-aml-lithuanian-fintech-in-2020
[170] https://gfi.findexable.com/?utm_source=Medium&utm_medium=Email&utm_campaign=Launch%20Report&utm_term=Findexable%20
[171] https://www.lb.lt/en/news/steady-growth-big-names-and-a-focus-on-aml-lithuanian-fintech-in-2020
[172] Ibid.
[173] https://www.transparency.lt/en/during-the-pandemic-the-scale-of-fraud-using-fintech-companies-has-likely-increased/
[174] https://www.njordlaw.com/njord-lithuania-now-companies-being-set-can-open-accounts-e-money-institutions

ownership; a 6th AML Directive containing provisions for the new rules to be transposed into national law; and a strengthening of AML rules for the crypto sector.[175]

The main task of the new AMLA will be to establish a single integrated system of AML supervision across the EU based on common supervisory methods and convergence of high standards. AMLA will not only monitor and coordinate national supervisors of financial and non-financial entities but will also directly supervise high-risk financial institutions operating in a large number of Member States. Furthermore, AMLA will enhance cooperation among FIUs, facilitating coordination and joint analyses between them.[176]

The package also includes significant measures that are expected to increase the availability, transparency and accuracy of beneficial ownership information across the EU. These will aim to establish a harmonised approach to the identification of beneficial ownership across EU countries, and to introduce disclosure requirements for nominee shareholders and directors as well as for non-EU legal entities that either enter into a business relationship with EU regulated entities or acquire real estate in a Member State.[177]

The legislative package seems to address several of the problems identified in this report, many of them, such as high-risk correspondent banking and abuse of shell companies, caused by the lack of a cross-border approach in supervision and investigation. Assuming a speedy legislative process and dialogue with the EU Parliament and Council (both institutions have already expressed themselves in favour), the new AMLA will be established in 2024 and be fully operational in 2026, when the new rules will enter into force.

While this is a much-welcomed move, it will still be a long time before Member States can fully adapt to the new framework and reap the benefits of enhanced cross-border AML monitoring and control by AMLA (assuming this body will have adequate resources and governance). As such, governments in Latvia and in the other Baltic countries should not only fully support the EU Commission proposal in Council negotiation, but already take some steps to tackle the most pressing problems identified in this report and to prepare themselves and facilitate the transition to the new rules.

As we propose in the next section, this should include a mutual understanding of the impact of de-risking among Baltic banks and of the challenges stemming from it, an upgrade of company registers, including measures to ensure interoperability among them and better verification measures, licensing and improved supervision of company formation activities, and, last but not least, the setting up of mechanisms to improve monitoring of EMIs/PIs.

[175] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3690
[176] https://ec.europa.eu/finance/docs/law/210720-proposal-aml-cft-authority_en.pdf
[177] https://ec.europa.eu/finance/docs/law/210720-proposal-aml-cft_en.pdf

3. Policy recommendations

As shown in this report, there are reasons to believe that the money laundering risks affecting banks in Latvia and in the other Baltic states is nowadays much lower than it was in the past decade. Nevertheless, the worrying state of global beneficial ownership transparency, the difficulty of controlling company formation activities across jurisdictions and the gradual shift of high-risk customers to the growing and increasingly sophisticated e-money sector suggest that increased cross-border efforts are needed to understand evolving money laundering threats in the region and how they could be tackled.

As such, we recommend the Latvian government to fully support current EU efforts to establish a supranational supervision and reporting mechanism for cross-border transactions, and work in concert with the FIU, the FCMC, the SRS, the Enterprise Register, and members of the Financial Sector Development Board to implement the following measures:

- Ensure the regular publication of detailed statistics about banks' relationships with TCSPs and EMIs/PIs, including at least: i) the number of TCSPs with whom they have a cooperation agreement and the number of EMIs/PIs to whom they provide correspondent banking accounts; ii) jurisdictions in which those TCSPs and EMIs/PIs are based and operate; iii) information about the different types of cooperation agreements and correspondent banking services

- Take steps to further strengthen the monitoring and transparency of the provision of corporate services in in Latvia, by: i) developing licensing requirements for TCSPs, regardless of the specific business category to which they belong; ii) setting up a public register of all TCSPs under the supervision of the SRS; iii) publishing a list of disqualified TCSP owners' and directors.

- Engage with competent authorities in Estonia and Lithuania to ensure interoperability among corporate registries in the three countries and harness their AML intelligence value, by: i) adopting common open data standards; ii) developing common tools and indicators to detect suspicious TCSP activities (e.g., bulk-formation of companies); iii) developing technical solutions that allow for cross-border verification of basic beneficial ownership information (e.g., verifying whether information provided by a Latvian national setting up a company in Estonia corresponds to information held by Latvian authorities about that person).

- Seek to upscale financial intelligence cooperation and information sharing related to EMIs/PIs, across the three Baltic States, by: i) undertaking a joint cross-border risk assessment or thematic study focused on current money laundering threats posed by EMIs/PIs operating in the three countries and targeting high-risk customers from the FSU; ii) establishing regional Expert Groups to share intelligence with the largest private EMIs/PIs operating in the three countries; and iii) consider the introduction of mandatory targeted transaction and record-keeping requirements on EMIs/PIs serving legal entities owned by high-risk customers

Citadeles iela 8, Riga, LV-1010, Latvia

+371 67285585

ti@delna.lv

www.delna.lv