Delna
SABIEDRĪBA PAR ATKLĀTĪBU
TRANSPARENCY INTERNATIONAL
LATVIJAS NODAĻA

CONNECTIONS

MONEY LAUNDERING IN LATVIA AND THE ROLE OF TRUST AND COMPANY SERVICE PROVIDERS

Transparency International Latvia (Sabiedriba par atklatibu – Delna) is the 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.

This publication was produced as part of the project "Enhancing the Transparency of Latvia's financial system", funded by the Open Society Foundations in collaboration with Tax Justice Europe – Eurodad.

Author: Antonio Greco

Editor: Liene Gatere

Design: Antonio Greco, Jurgis Kalnins

Acknowledgements: We would like to thank the Open Society Foundations for their financial support that made this research possible. We are grateful for the support and assistance of Tax Justice Europe – Eurodad.

The project team is grateful to all who contributed to the production of this report: Agris Bobrovs, Juan Fuente Bravo, Anita Liepina, Elmars Neimanis, Kristians Sloka, Janis Volberts.

We thank our colleagues Steve Goodrich and Ben Cowdock at Transparency International-UK for their comments on earlier versions of the report.

We are also thankful to Agnese Rudzite and Artis Aizupietis from the State Revenue Service of the Republic of Latvia and Kristaps Markovskis from the Financial and Capital Market Commission of the Republic of Latvia for their comments on the policy recommendations provided in this publication.

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

Published January 2018

Executive summary

As emerged from several journalist and law enforcement investigations, in the course of the last decade the Latvian banking sector was exploited from several individuals and entities across the former Soviet Union and beyond to facilitate the laundering and movement of at least €20 billion in illicit funds originated from corruption, embezzlement and black market, into the international financial system.[1] This often saw the use of complex networks of anonymous shell companies with accounts in Latvian banks, through which the funds were handled in such a way as to systematize chains of fraudulent transactions and obscure the flows of illicit money, hiding the perpetrators.[2]

Much of Latvia's financial sector vulnerability against money laundering has derived from the high money laundering risks inherent to a specific business model developed by Latvian banks – the export of "financial logistics services" to clients in countries of the Commonwealth of Independent States (CIS). This mainly consisted the attraction of clients from those states and the provision of short-term deposits in order to facilitate the transit of their funds into the international financial system.[3] Statistics demonstrated that while the vast majority of Latvian banks' non-resident deposits was made up by individuals and entities from CIS countries with significant corruption problems[4], these owned their deposits via legal entities incorporated in offshore jurisdictions – most of them shell companies lacking information on beneficial owners.[5]

Despite the high money laundering risks inherent to this business model, Latvian banks had not developed the adequate anti-money laundering capacity to handle them. Eventually, it emerged that weaknesses in Latvia's AML system, combined with their extensive correspondent banking network and the untraceable ownership of their client offshore companies allowed for the injection of illicit funds worth billions in the global financial system. This was demonstrated by the 'Russian Laundromat', in which over $20 billions of dirty funds were illegally moved out of Russia and dissipated into the international financial system[6] and the Moldovan Bank Robbery, which saw around $1 billion being fraudulently stolen from three Moldovan banks, and the country deprived of 12% of its GDP.[7]

Significant responsibilities for Latvian banks' anti-money laundering failures lied with the Latvian financial regulator, the Financial and Capital Market Commission (FCMC), which did not have enough resources to ensure their compliance with anti-money laundering (AML) rules. While the number of AML-focused inspections was insufficient, sanctions imposed on banks for non-compliance with AML regulations had been disproportionately small to have a deterrent effect.[8] The OECD expressed particular concern about the fact that, despite the acceptance and customer identification of the majority of non-resident deposits were accepted through Latvian banks' representative branches abroad, the FCMC had conducted no on-site inspections of these overseas offices over the previous years.[9]

This turned out to be one of the major vulnerabilities of the Latvian financial system against money laundering, as many foreign branches of Latvian banks were prominently relying on the services of Trust and Company Service

[1] Re:Baltica (2016), 'US pressures Latvia to clean up its non-resident banks', https://en.rebaltica.lv/2016/02/u-s-pressures-latvia-to-clean-up-its-non-resident-banks/ [accessed 30 Oct 2017]
[2] Stack G. (2015), 'Baltic shells: on the mechanics of trade-based money-laundering in the former Soviet space', Journal of Money Laundering Control, vol.18 Issue: 1, pp. 81-98
[3] Financial and Capital Market Commission (FCMC) (2012), "Non-resident banking business in Latvia", Benefits and Risks, 26 November, available at: http://www.fktk.lv/en/media-room/press-releases/4040-2012-11-26-nonresident-banking-busi.html
[4] International Monetary Fund (2013), 'Latvia: IMF Country Report No. 13/28', available at: https://www.imf.org/external/pubs/ft/scr/2013/cr1328.pdf
[5] 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 Issue: 4, pp. 496-512
[6] Organized Crime and Corruption Reporting Project (2017), 'The Russian Laundromat Exposed', https://www.occrp.org/en/laundromat/ [Accessed October 18, 2017]
[7] Organized Crime and Corruption Reporting Project (2015), 'Grand Theft Moldova', https://www.occrp.org/en/laundromat/grand-theft-moldova/ [Accessed October 18, 2017]
[8] OECD (2015), Phase 2 Report on Implementing the OECD Anti-Bribery Convention in Latvia, pp. 29, available at http://www.oecd.org/daf/anti-bribery/Latvia-Phase-2-Report-ENG.pdf
[9] ibid. p.32

Providers (TCSPs), business introducers and agents, in Latvia and abroad, in order to conduct customer identification and bring in new clients[10], with deleterious effects.

In fact, as emerged, the majority of anonymous shell companies with Latvian bank accounts involved in illegal activity could be traced back to these agents. They were – wittingly and unwittingly – functional in helping money launderers to set up complex offshore structures and open bank accounts for them in partnered Latvian banks relying on their services. In this way, corrupt networks were able to "bypass" customer identification checks, have access to the international financial system and avoid prosecution.[11] The tracing of these actors and the extent of their activities has been difficult due to their loose transnational structures and the shifting collaborations with each other. This was facilitated by their opaque nature and the scarcity of both information and controls, at the national and international level, on the sector, hindering money laundering investigations.

Following international criticism and involvement in large-scale money laundering cases, since the beginning of 2016 Latvian authorities have taken significant steps to end the abuse of the country's financial system. The resources of the Latvian financial regulator were increased resulting in a more effective supervision, unprecedented administrative fines for non-compliance with Anti-Money Laundering rules [12], and a push for the re-orientation of Latvian banks' business towards low-risk domestic clients. Stricter regulations were also issued to mitigate the risks arising from reliance on unsupervised TCSP in Latvia and abroad.[13] These reforms have resulted in a significant decrease of non-resident deposits in Latvia and their related money laundering risks.

However, the 2017 Latvian National Money Laundering Risk Assessment has found a number of vulnerabilities related to the TCSP sector in Latvia – which encompasses legal service providers, tax advisors and external accountants – suggesting a need for enhanced regulation and transparency[14]:

- **Lack of resources, absence of focused risk-assessment and weak supervision by part of the State Revenue Service, which is the competent authority in charge of supervising the sector;**
- **Scarce understanding of anti-money laundering regulations and duties;**
- **Absence of entry requirements and licensing for firms carrying out TCSP services;**
- **Impossibility to ensure that all firms operating in the sector have been educated on anti-money laundering matters**

With the 2017-2019 Anti-Money Laundering Action Plan, the Government has planned to take steps to tackle the problem, including increased supervisory capacity for the State Revenue Service, better assessment of money laundering, development of regulation and licensing, and increased AML trainings for firms operating in the sector.[15] Towards the end of 2017, Latvia has also strengthened its AML legislative framework, transposing the EU 4th Anti-Money Laundering Directive and making access to beneficial ownership of companies in Latvia available to the general public.[16] The public register of beneficial owners is a great step forward towards transparency of corporate entities in Latvia. It will likely facilitate the work of law enforcement authorities in Latvia

[10] MONEYVAL (2012), 'Report on Fourth Assessment Visit – Latvia', pp. 114-116, https://rm.coe.int/report-on-fourth-assessment-visit-anti-money-laundering-and-combating-/1680716b9f
[11] 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 Issue: 4, pp. 496-512
[12] Latvian National Money Laundering/Terrorism Financing Risk Assessment Report (2017), pp.56-57, available at: http://www.kd.gov.lv/images/Downloads/useful/ML_TF_ENG_FINAL.pdf
[13] Financial and Capital Market Commission (FCMC), Regulation No.196/2016, Regulations for Cooperation with Third Parties and Requirements for Business Relations with the Customers whose Identification or Due Diligence is Performed Using Third Party's Services, http://www.fktk.lv/en/law/credit-institutions/fcmc-regulations.html
[14] Latvian National Money Laundering/Terrorism Financing Risk Assessment Report (2017), pp.86-87, available at: http://www.kd.gov.lv/images/Downloads/useful/ML_TF_ENG_FINAL.pdf
[15] Plan of Measures for Mitigation of the Money Laundering and Terrorism Financing Risk for 2017-2019, p.23, http://www.fm.gov.lv/en/s/financial_market_policy/plan_of_measures_for_mitigation_of_the_money_laundering_and_terrorism_financing_risks_for_2017___2019/
[16] Law on Prevention of Money Laundering and Terrorism Financing, https://likumi.lv/doc.php?id=178987

and the rest of the EU, and enhance scrutiny by citizens, public media, civil society organisations and investigative journalists, and it will also help bring more scrutiny in the TCSP sector, deterring money launderers from becoming beneficial owners of these firms.

However, the further challenges posed by an industry which has become increasingly globalised and difficult to control make policies in this field a priority for the mitigation of money laundering risks. Unsupervised and unregulated trust and company service providers, in Latvia and abroad, constitute a significant threat to the resilience of the financial system against money laundering. This calls for a better understanding of the structure of the sector in Latvia, stronger regulations and awareness of anti-money laundering duties by TCSP firms.

Headline Policy Recommendations

- ✓ A thematic review of the TCSP sector in Latvia should be conducted. This should: a) include an analysis of how many firms are operating in the sector as well as the number of their subsidiaries in other countries; b) encompass best-practices in AML procedures in the field and make a comparison with the actual standards in Latvia; c) provide solutions for improving those standards.

- ✓ Appropriate licensing requirements for firms carrying out TCSP services in Latvia should be developed. Before entering the market, these firms should be subject to a 'fit and proper test' (a series of checks, to make sure that they meet the requirements of the National Anti-Money Laundering Laws and Regulations) at the time of licensing and over the period for which they hold a license, applying similar standards of integrity as for financial institutions. Branches and subsidiaries of Latvian TCSPs operating abroad should also be subjected to the same checks and integrity requirements.

- ✓ Trust and company service providers should be prohibited from servicing corporate structures or arrangements facilitating anonymity of beneficial owners and money laundering. Moreover, legal service providers should not be allowed to act as nominee directors for clients.

- ✓ Participation in anti-money laundering training organised by the State Revenue Service should be made a condition for obtaining and keeping a licence.

Table of contents

List of Abbreviations

AML – Anti-Money Laundering

AMLD – Anti-Money Laundering Directive

BO – Beneficial Owner

CDD – Customer Due Diligence

CS – Control Service

CTF – Counter Terrorist Financing

EDD – Enhanced Due Diligence

EU – European Union

FATF – Financial Action Task Force

FCMC – Financial and Capital Market Commission

FIU – Financial Intelligence Unit

ICIJ – International Consortium of Investigative Journalists

ICS – Internal Control System

IMF – International Monetary Fund

LEA – Law Enforcement Authority

LLP – Limited Liability Partnership

ML – Money Laundering

MoF – Ministry of Finance

MoJ – Ministry of Justice

NRA – National Risk Assessment

OCCRP – Organized Crime and Corruption Reporting Project

OECD – Organization for Economic Cooperation and Development

OFC – Offshore Financial Centre

OGBS – Offshore Group of Banking Supervisors

SAR – Suspicious Activity Report

SLP – Scottish Limited Partnership

STR – Suspicious Transaction Report

TBML – Trade Based Money Laundering

TCSP – Trust and Company Service Provider

TF – Terrorist Financing

TI – Transparency International

UBO – Ultimate Beneficial Owner

UN – United Nations

UNODC – United Nations Office for Drugs and Crime

4AMLD – 4th (EU) Anti-Money Laundering Directive

5AMLD – 5th (EU) Anti-Money Laundering Directive

Introduction

This paper gives an overview on how Latvia's financial system was used in the 21st century for money laundering by corrupt networks in the countries of the former Soviet Union and beyond and discusses the role of company service providers and other professional intermediaries therein. The paper also gives an overview of the most recent reforms undertaken in the anti-money laundering field in Latvia and provides recommendations for continued improvement.

Chapter 1 explains what is money laundering, its continued relevance as a global problem, and how anonymous shell companies, offshore financial centres and unscrupulous Trust and Company Service Providers allow the corrupt to hide their illicit assets while avoiding prosecution.

Chapter 2, briefly introduces international and European anti-money laundering standards and the most recent developments in European Union's anti-money laundering legislation, discussing their significance for the global fight against illicit financial flows.

Chapter 3 assesses the role of Latvian banks and anonymous shell companies in enabling complex money laundering schemes carried out by corrupt networks in the post-Soviet space. The main loopholes in Latvia's financial system's anti-money laundering regulatory and supervisory framework are analysed, as well as major reforms undertaken in the last two years in order to tackle the problem.

Chapter 4 focuses on the activities of Trust and Company Service Providers and their role in large-scale money laundering schemes involving Latvian banks. Discussion involves how problems with the regulation and supervision of these actors – as identified by the 2017 Latvian National Money Laundering Risk assessment – has exacerbated the money laundering risks related to their activities, and leaving them with almost no deterrents against working – wittingly and unwittingly – as enablers for corrupt networks

Chapter 5 discusses recent development in Latvia's AML legislative framework and provides policy recommendations for further improvement.

1. What Is Money Laundering and why it matters

Money laundering is the process of concealing the origin, ownership or destination of the profit of corruption, fraud, drug trafficking and other crimes ("dirty money") by hiding it within legitimate economic activities to make it appear legal ("clean").[17]

When illicit financial flows deriving from organized crime and corruption are not detected and confiscated, criminal networks are able to thrive, expand their business and gain resilience against law enforcement authorities who go after them. This can have many other negative effects for societies across the world.

The theft of state funds for private gains depletes resources that would have otherwise gone towards public goods, such as social services and investments in infrastructure and economic development. From an economic point of view, it can distort the market mechanisms, depriving consumers and producers of the benefits of fair, free, safe and secure economic commercial systems; and it can harm the reputation of a country's integrity of banking and financial services market place, turning away potential investors.[18]

There exist various estimates concerning illicit financial flows at the global level. Although they cannot be precise due to the illegal nature of the transactions, they may help to make sense of the relevance of the problem. According to the United Nations, money laundering may reach USD 2 trillion annually (around 2.5% of GDP worldwide) with half of this amount coming from developing countries, a figure which is more than 7 times the total inflows they receive from international aid every year.[19] It has been suggested that as many as 3.6 million deaths could be prevented each year in developing countries if action was taken to tackle corruption and criminality behind these illicit flows and recovered revenues were invested in health systems.[20]

How criminal money is laundered

Money laundering schemes can be carried out in many methods varying in complexity, sophistication and geographic scope, but they usually consist of three main phases.[21]

The first phase is called placement, where the profits of crime enter the financial system in some form (i.e. they are furtively deposited at a bank, smuggled over a state-border or mixed with the financial flows of a legitimate business).

The second phase is the layering, where the illicit funds are "circulated" many times, through a series of financial transfers, either nationally or all over the globe, in order to hide their illegal source and beneficial owner(s). The more often the money gets transferred around the globe in the layering phase, the less traceable its criminal origins are.

In the third phase, called reintegration, the laundered money is reintroduced in the legitimate economy, for example by buying property in the real estate sector, by investing it in the financial market, buying companies or simply buying expensive cars and jewels.

The term "**beneficial owner**" refers to the natural person(s) who ultimately and effectively own(s) or control(s) a company or other legal arrangements and/or the natural person(s) on whose behalf a transaction is being conducted.

In situations of money laundering, the beneficial owner is the person (or group of persons) who has an interest in, or control over, ill-gotten financial assets or property.

Stolen Asset Recovery Initiative (STAR)/World Bank/United Nations Office on Drugs and Crimes (UNODC) (2011), *The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It*

[17] Financial Action Task Force (FATF), "Money Laundering", http://www.fatf-gafi.org/faq/moneylaundering/
[18] ibid.
[19] Pietschmann T. & Walker J. (2011), Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes, United Nations Office on Drugs and Crime, Available at: https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf
[20] https://s3.amazonaws.com/one.org/pdfs/Trillion_Dollar_Scandal_report_EN.pdf
[21] United Nations Office on Drugs and Crimes (UNODC), "Money laundering cycle" https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html

The "layering" phase is often crucial in a typical money laundering scheme. Once the corrupt have stolen the money, they typically wish to make it as difficult as possible to trace the illicit assets to the original theft and prevent law enforcement authorities from being able to discover their identity. This can be done in many ways.

The most common way for is the use of complex networks of anonymous shell companies spanning multiple jurisdictions. The money trail can be concealed even further by using third parties and nominee agents who act on behalf of corrupt individuals.

What is an anonymous company?

An anonymous company is a corporate vehicle registered in a secrecy jurisdiction[1] – a place where details on who owns companies are kept hidden from the public view.

What is a shell company?

A shell company is a corporate vehicle with no active business operations, assets or employees. The US Treasury's Financial Crimes Enforcement Network defines them as 'non-publicly traded corporations, limited liability companies or trusts that have no physical presence beyond a mailing address and generate little to no independent economic value'.[2] Shell companies can be anonymous too, if they are registered in a secrecy jurisdiction, however the terms are not interchangeable.

What is a nominee?

Nominees are individuals (or sometimes entities) who have been appointed to act as directors or hold shares on behalf of someone else, either by contract or other instruments such as power of attorney.[3]

There are two broad categories of nominees: professionals, such as lawyers or Trusts and offshore firms offering nominee services; and informal nominees, such as family members, friends or close associates who play the role of frontmen for the beneficial owner. While some solutions exist to regulate the former category, regulating informal nominee is obviously challenging.

[1] In this paper we define 'secrecy jurisdiction as a country that scores 60+ on the Tax Justice Network's Financial Secrecy Index for 2015 http://www.financialsecrecyindex.com/introduction/fsi-2015-results [accessed 22 November 2017]

[2] https://www.fincen.gov/sites/default/files/advisory/2017-08-22/Risk%20in%20Real%20Estate%20Advisory_FINAL%20508%20Tuesday%20%28002%29.pdf [accessed 22 November 2017]

3 Transparency International EU (2017), 'Under the Shell: Ending Money Laundering in Europe', https://transparency.eu/under-the-shell/ [Accessed 20 October 2017]

In a recent review of 213 instances of grand corruption over the last 30 years, the World Bank found that in more than 70% of the cases the ownership of stolen funds had been disguised through the misuse of corporate entities, half of which were anonymous shell companies.[22] In many cases, these were registered in offshore financial centres offering very little or no cooperation in disclosing relevant information on their beneficial owners.

The definition of offshore financial centre (OFC), implying the artificial movement or use of money across borders, applies to any location that seeks to attract capital from non-residents. By offering politically stable facilities, secrecy, lax regulations, specialized financial instruments, and low/no taxes offshore financial centres have often helped individuals and corporations as well as criminals and tax abusers to get around the rules, laws and regulations of jurisdictions elsewhere, be they related to money laundering, taxation or simply market competition.[23]

In fact, OFCs play a very central role in today's global economy, as suggested by statistics associated with them. A study by Tax Justice network estimated that, in 2010, between $21 trillion and $32 trillion was hiding in more than 80 OFCs, while privileged elites in 139 lower and middle-countries had $7.3 to $9.3 trillion in unrecorded offshore wealth.[24]

The global relevance of offshore financial centres was demonstrated when, on 3 April 2016, journalists from 107 media organizations in 80 countries exposed the so-called 'Panama Papers', the biggest leak of information ever. The 2.6 terabytes of information leaked from the Panamanian law firm Mossack Fonseca contained 11.5 million documents, confidential records of 214.000 offshore companies with connections to around 140 politicians and high-level public officials around the globe.[25]

Apart from massive tax fraud by private persons and firms, a second group of cases shows how officials, ministers, and even heads of state used complex offshore structures to cover up conflict of interest or even corruption and embezzlement, while a third group of cases exposes the use of these structures by outright criminal organizations for laundering the profits of their illegal activities.[26]

[22] Stolen Asset Recovery Initiative (STAR)/World Bank/United Nations Office on Drugs and Crimes (UNODC) (2011*), The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It*, https://star.worldbank.org/star/sites/star/files/puppetmastersv1.pdf

[23] Shaxson N. (2012)., Treasure Islands: Tax Havens and the Men Who Stole the World, London: The Bodley Head

[24] James Henry, 'The Price of Offshore Revisited, Tax Justice Network', July 2012. Available at: https//www.taxjustice.net/cms/upload/pdf/Price_of_Offshore_Revisited_120722.pdf

[25] International Consortium of Investigative Journalists (ICIJ) (2016), "The Panama Papers", https://panamapapers.icij.org, [accessed 16 December 2017]

[26] Obermayer B. & Obermaier F. (2016), The Panama Papers, London (UK): Oneworld Publications

As documented by the Panama Papers, in the creation of complex offshore structures behind complex money laundering schemes, criminals usually purchase fiduciary or intermediary services from a range of financial and non-financial companies and professionals who, wittingly and unwittingly, facilitate the schemes. Among others, these professionals can include, lawyers, accountants, and Trust and Company Service Providers (TCSPs).

A recent review of foreign bribery cases published by the OECD showed that 71% of the incidents involved bribes paid by intermediaries, such as agents, front companies and lawyers.[27] This illustrates how professionals in the legal, finance and accountancy sectors are often critical to supporting a series of financial transactions to give illegitimate wealth a face.

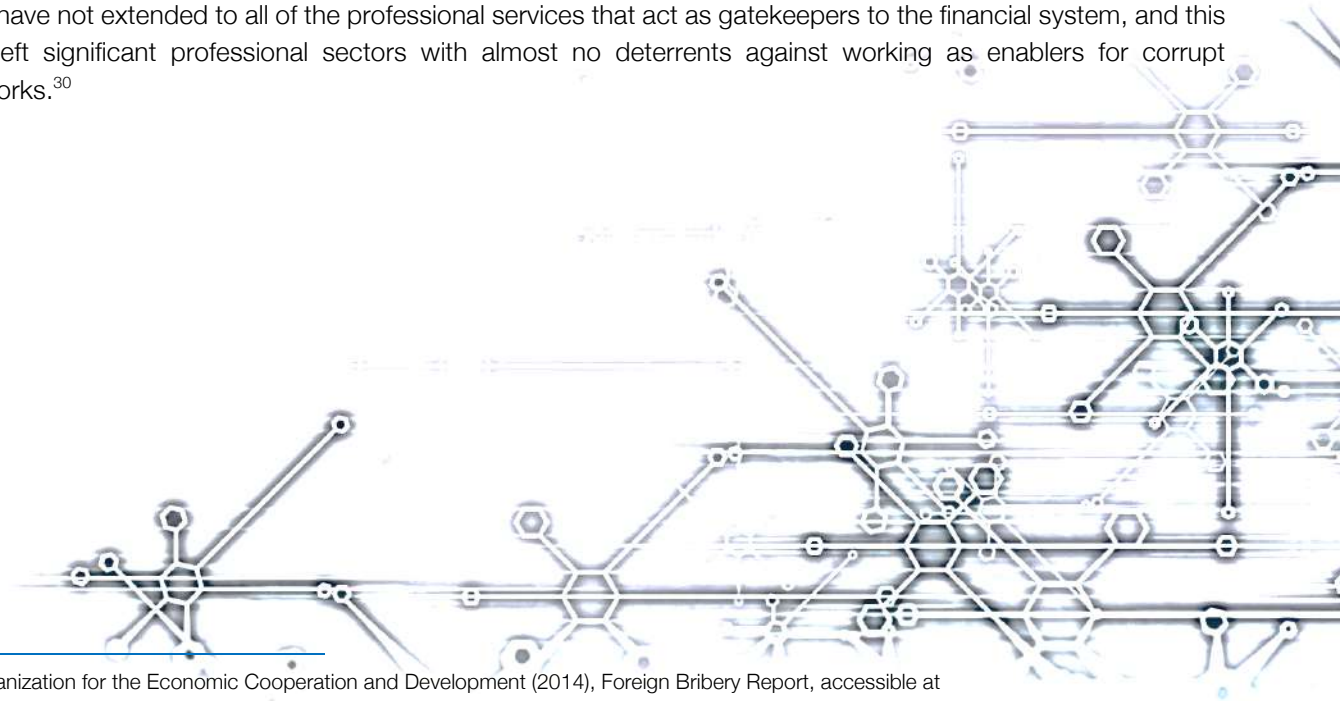
Among professional intermediaries, Trusts and Company Service Providers (TCSPs) and offshore agents such as Mossack Fonseca, are particularly vulnerable to the risk of money laundering, due to the nature of their activities. TCSPs are firms whose core business consists in the incorporation of companies, trusts and other corporate vehicles across multiple jurisdictions and the provision of a wide range of accessory administrative services, including the filing of tax paperwork, the provision of registered addresses and the appointment of nominee directors.[28]

TCSPs can also act as "business introducers", helping new companies gain access to bank accounts around the world. This enables the individuals behind the company to pay funds into it and move the money to other jurisdictions.[29]

There is a large variety of kinds of TCSPs in size and nature. They may be a single individual operating through a website, or a small law or accounting firm. Or they may be well-established organisations, employing hundreds of people and administering thousands of companies at the same time. The level of vulnerability for money laundering posed by TCSPs will usually depend on the relative size of the sector within a domestic economy. However, as online incorporation services make it extremely cheap and easy to incorporate from anywhere around the world, it has been particularly difficult for competent authorities to find effective measures in order to supervise them.

While over the years extensive anti-money laundering responsibilities have been applied to financial institutions, they have not extended to all of the professional services that act as gatekeepers to the financial system, and this has left significant professional sectors with almost no deterrents against working as enablers for corrupt networks.[30]

.



[27] Organization for the Economic Cooperation and Development (2014), Foreign Bribery Report, accessible at http://www.keepeek.com/Digital-Asset-Management/oecd/governance/oecd-foreign-bribery-report_9789264226616-en#page4

[28] Stolen Asset Recovery Initiative (STAR)/World Bank/United Nations Office on Drugs and Crimes (UNODC) (2011), The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It, https://star.worldbank.org/star/sites/star/files/puppetmastersv1.pdf

[29] Transparency International-UK (2017), 'Hiding in Plain Sight: How UK Companies Are Used to Launder Corrupt Wealth', http://www.transparency.org.uk/publications/hiding-in-plain-sight/#.Wj6iTVKZPVr

[30] Judah B. & Li B., Kleptocracy Initiative (2017), 'Money Laundering for 21st Century Authoritarianism: Western Enablement of Kleptocracy', Hudson Institute, https://www.hudson.org/research/14020-money-laundering-for-21st-century-authoritarianism

2. International and European Anti-Money Laundering Standards

Over the years, the international community has set the standards for anti-money laundering (AML) regulation, by adopting several agreements and conventions whose common denominator is criminalization of money laundering and the prevention of the abuse of the financial sector for illicit purposes.

The Financial Action Task Force (FATF) was created in 1989 on the initiative of the G8. The role of this international organization is to issue regularly updated recommendations which aim to set legislative and regulatory Anti-Money Laundering (AML) standards. In 1990, the FATF issued its famous 40 Recommendations, introducing the basic requirements of AML policy. Following the 9/11 terrorist attacks, FATF's mandate was extended to include the combating of terrorist financing, issuing a further nine specially focused recommendations. The FATF 40 Recommendations have over the years represented a blueprint for AML legislation adopted by the European Union. [31]

The EU adopted the first Anti-Money Laundering Directive (AMLD) in 1991, with the aim of protecting the stability of the Single Market and its financial system against the negative and distorting effects of the laundering of criminal funds. Subsequent EU Directives (2001, 2005) were amended to expand the list of predicate offenses for money laundering to terrorist financing.[32]

The 3rd EU AMLD (2005) introduced a major reform in the general approach to the fight against money laundering in the European Union.[33] With the new system in place, called Risk-Based Analysis (RBA) System, significant responsibility for the protection of the financial system against money laundering was given to banks and financial Institutions, making them liable to prosecution for unreported transactions later discovered to be money laundering. In turn, they were allowed to adopt “personalized” risk-assessment programs reflecting their clientele and global position, while government authorities would serve as “watchdogs” through regular inspections.[34]

The indirect character of the current international Correspondent Banking System makes relationships between banks vulnerable to misuse for money laundering. On a general level, it consists in one banks (the correspondent bank) carrying out financial services for another bank (the respondent bank). By establishing networks of a multitude of correspondent relationships at the international level, banks are able to undertake financial transactions in jurisdictions where they do not have offices.[35]

As a correspondent bank may carry out services for clients of another bank, the integrity of which has not had verified beforehand. Thus, it is dependent on regulations and AML standards by all banks in all countries being “equal”. This, however, is not always true, as implementation of AML laws and compliance with regulations by banks is generally not uniform, constituting a weakness for the global financial system and allowing money launderers to exploit the loopholes deriving from different legislation across countries.[36]

Acknowledging this, the 4th EU Anti-Money Laundering Directive – adopted in June 2015 and implemented by EU Member States at the end of June 2017 – reflects the need for better international cooperation, information exchange and transparency in the field of money laundering are reflected in.[37]

[31] Tsingou E. (2010), ‘Global financial governance and the developing anti-money laundering regime: What lessons for International Political Economy?’, International Politics, 47:6, 617-637
[32] ibid.
[33] Directive (EC) 2005/60 of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing
[34] Kegö W. & Georgieff A. (2013), The Threat of Russian Criminal Money: Reassessing EU Anti-Money Laundering Policy, Stockholm: Institute for Security and Development Policy, p.34
[35] Unger B. et al. (2017), ‘Offshore Activities and Money Laundering: Recent Findings and Challenges’, Study commissioned by the European Parliament’s Panama (PANA) Inquiry Committee, pp.16-17
[36] Kegö W. & Georgieff A. (2013), ‘The Threat of Russian Criminal Money: Reassessing EU Anti-Money Laundering Policy’, Stockholm: Institute for Security and Development Policy, p.37
[37] Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

The current international and European AML policy is based on four key pillars: Customer Due Diligence (CDD), reporting obligation; record-keeping obligation; and enforcement, which can be both preventive and repressive character.

Customer Due Diligence (CDD)

The aim of Customer Due Diligence measures is to prevent banks and other financial and non-financial institutions, such as Corporate Service Providers from dealing with unknown customers of businesses which they do not fully understand. For this purpose, they are required to obtain adequate information on the nature of the business their potential client is conducting and verify the identity of their beneficial owner(s).

In order to be more effective, institutions are allowed to perform customer due diligence measures on the basis of the risk-based approach.[38] In case of high-risk clients, such as shell companies, Politically Exposed Persons (PEPs) and clients from high-risk third countries, financial institutions are required to conduct Enhanced Due Diligence (EDD) procedures. These include gathering more specific information on a customer's source of funds or wealth, a closer monitoring of transactions and approval from senior management to conduct business with the high-risk customer in question.[39]

Banks may also decide to rely on third parties such as agents and TCSPs in order to conduct Customer Due Diligence and/or introduce business. However, according to FATF rules, in these cases the ultimate responsibility for CDD measures remains with the financial institution, which has to make sure that the third party is regulated and supervised, and that it has measures in place for compliance with CDD and other AML requirements. Financial institution also must assess the level of AML risk posed by the country where the agent is operating from.[40]

One of the major innovations introduced by the 4th EU AML Directive is the "Central Register of Beneficial Ownership". This means that companies and other legal entities are now required to maintain accurate and current information on their ownership structure, with the obligation to identify the individuals in effective control of the entity and provide such information to government and law enforcement authorities.[41]

Politically Exposed Persons are individuals who are, or have been, entrusted with high-level positions in public service. Their classification may also extend from the person to his or her family members and close associates. PEPs may or may not be corrupt, but nonetheless they represent high-risk customers.

Source: Transparency International, 'Closing banks to the corrupt: the role of due diligence and PEPs', Policy Brief #5/2014

Information on beneficial ownership is to be collected and held by each Member State in a central register accessible to banks, law firms and any person or organisation that can demonstrate a legitimate interest (a formulation that carries its own problems, as it will be discussed shortly below). The Directive also requires all member states to set up centralised national bank and payment account registers, and to make all information on the holders of bank and payment accounts available to governments.[42]

[38] Unger B. et al. (2017), 'Offshore Activities and Money Laundering: Recent Findings and Challenges', Study commissioned by the European Parliament's Panama (PANA) Inquiry Committee, p.28
[39] Transparency International, 'Closing banks to the corrupt: the role of due diligence and PEPs', Policy Brief #5/2014, https://www.transparency.org/whatwedo/publication/policy_brief_05_2014_closing_banks_to_the_corrupt_the_role_of_due_diligence
[40] FATF (2012-2017), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, Recommendation 17, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html
[41] Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing
[42] ibid.

Reporting and record-keeping obligations

The second key element is the obligation for institutions to report - on their own initiative - suspicions of money laundering or terrorist financing to the competent authority, the Financial Intelligence Unit (FIU), which is a central national agency responsible for receiving, analysing and transmitting, to the competent authorities, disclosures concerning potential illicit financial flows.[43] Such disclosures are commonly known as Suspicious Transaction Reports (STRs) or Suspicious Activity Reports (SARs), and the format and criteria they should assume vary according to the jurisdiction in object.

According to Europol, STRs are a core investigative tool. They provide indications not only on the movements of the funds (origin, transfers, destination, beneficiaries), but also to reconstruct the geographic movement of criminals and their current location. Moreover, they allow for the identification for participants in a criminal network and provide the basis for seizure/asset confiscation opportunities. They can also be used for tackling a number of offences such as tax fraud and terrorist financing.[44] For all these reasons, it is important that financial institutions and other reporting entities file high-quality STRs to authorities, and that authorities provide in turn meaningful feedback on the reports received.

The record-keeping obligation entails the obligation for institutions to keep the identification documents and all transaction data stored for a period of at least five years following the carrying out of transactions. The purpose of this requirement is two-fold: on the one hand, it enables supervisory authorities to check compliance with AML rules, while on the other hand it enables law enforcement authorities to gather evidence in case of criminal prosecution.[45]

Preventive enforcement

Under the Risk-Based Analysis system, State authorities must regularly supervise financial and non-financial institutions on their compliance with anti-money laundering obligations, and sanction them in case of non-compliance. The FATF Recommendations stipulate that there must be effective, proportionate and dissuasive sanctions to deal with non-compliance by obliged entities.[46]

Supervisors are also responsible for maintaining awareness of money laundering responsibilities within their sector and should provide clear and consistent signals to firms about the importance of AML measures.[47]

Effective regulation requires adequately-resourced supervisors who can target their resources where they will have the biggest impact, encourage compliance through voluntary measures where it is possible, and provide a significant set of penalties, of monetary or other nature, as a deterrent against non-compliance. Achieving effective implementation of regulations and a business environment that meets the standards set out by law also requires proportionate and transparent enforcement, and a detailed analysis of risk.

The 4th EU AML Directive emphasises the risk-based approach to anti-money laundering at every level. It directs Member States to commission national risk assessments, firms to develop risk-based policies, and practitioners to conduct customer due diligence in a risk-based manner. In addition, firms with majority-owned subsidiaries located in other countries where the minimum AML requirements are less strict than those of the Member State must implement the requirements of the Member State at those subsidiaries.[48]

[43] Unger B. et al. (2017), 'Offshore Activities and Money Laundering: Recent Findings and Challenges', Study commissioned by the European Parliament's Panama (PANA) Inquiry Committee, p.28
[44] Europol (2017), 'From Suspicion to Action: Converting Financial Intelligence into greater operational impact', p.32, https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact
[45] Unger B. et al. (2017), 'Offshore Activities and Money Laundering: Recent Findings and Challenges', Study commissioned by the European Parliament's Panama (PANA) Inquiry Committee, p.29
[46] ibid. pp.29-30
[47] ibid.
[48] Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

Transparency and accountability are particularly important parts of any regulatory system. Like the police, supervisors should be exposed to public scrutiny about what impact enforcement activities are having, and whether these have improved compliance, or remedied the harm cause by regulatory non-compliance. Relevant regulators should publish the details of all sanctions they impose and the details of their enforcement policy, which is a legal document that explains how they intend to use these sanctions in practice.[49]

Repressive enforcement

The repressive part of anti-money laundering policy aims at punishing launderers usually through the use of criminal law and the freezing, seizure and confiscation of assets.[50] This can play a crucial role in fighting organised crime, interrupting its business cycle, protecting the legal economy against infiltration and returning criminal profits to citizens. In recent years, the confiscation of criminal proceeds and criminal assets has been listed as strategic priority by the EU Internal Security Strategy (ISS).[51]

However, despite their importance, prosecution and confiscation of proceeds of crime at the international and domestic level have proven to be very difficult over the years and the existing data paint a bleak picture. According to the United Nations Office on Drugs and Crime (UNODC), less than 1% of global illicit financial flows are currently being seized and forfeited.[52] The figures are very similar with regard to the European Union. From 2012 to 2014 just 2.2% of the estimated proceeds of crime were provisionally seized or frozen, and only 1.1% of the criminal profits were ultimately confiscated at the EU level.[53]

According to Europol, one of the main reasons for the low performance of repressive enforcement has been the fragmented cross-border cooperation and information exchange between FIUs and law enforcement authorities (LEAs) across the world. [54]

The impact of new technologies on the financial system and the development of borderless virtual environment call for reflection on how to adapt policies which are meant to be supervised only at the national level, while the underlying business (and the threats related to it) is already transnational and globalised in its own nature.

[49] Transparency International EU (2017), 'Under the Shell: Ending Money Laundering in Europe', https://transparency.eu/under-the-shell/ [Accessed 20 October 2017]
[50] Unger B. et al. (2017), 'Offshore Activities and Money Laundering: Recent Findings and Challenges', Study commissioned by the European Parliament's Panama (PANA) Inquiry Committee, p.30
[51] Savona E. and Riccardi M. (eds.) (2015), From Illegal Markets to Legitimate Business: The Portfolio of Organised Crime in Europe, Final Report of Project OCP – Organised Crime Portfolio (www.ocportfolio.eu), Trento, Transcrime – Università degli Studi di Trento, p.224
[52] Pietschmann T. & Walker J. (2011), 'Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes', United Nations Office on Drugs and Crime (UNODC), https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf
[53] Europol (2016), 'Does the crime still pay?', https://www.europol.europa.eu/newsroom/news/does-crime-still-pay
[54] Europol (2017), From Suspicion to Action: Converting Financial Intelligence into greater operational impact

The 5th EU Anti-Money Laundering Directive

In July 2016, after the initial public outrage in consequence of the Panama Papers and the revelations of the significant involvement of individuals, firms and banks from the EU in the schemes, the European Commission set up a proposal to amend the 4th Anti-Money Laundering Directive.[55]

Apart from further tightening the screws of the EU anti-money laundering system, this envisages public access to a limited set of information on beneficial ownership of companies and specific kinds of trusts and similar legal arrangements (name, birth date of the beneficial owner, business address, nationality and description of how ownership or control is exercised).

As recognized by the European Commission in its own impact assessment, at present, access to beneficial ownership information is quite restrictive in the EU and left at the discretion of the single Member State, with access granted exclusively to law enforcement authorities, subjects of the AML law and few designed parties with a 'legitimate interest'.[56] This goes against the public interest, as it hampers the EU's long-term objective of ensuring consistent and harmonised practices across the Union, and makes transnational investigations more costly and cumbersome due to slow procedures of Mutual Legal Assistance.

Trilogue negotiations between the European Commission, the Council of Ministers and the European Parliament went on throughout he whole 2017, with the main point of dispute being privacy issues related to the collection and publication of personal information on beneficial owners of trusts, opposed by the Council of Ministers.[57]

A final agreement was finally reached under the Estonian presidency of the EU in late December 2017, according to which national registers of beneficial owners of companies operating in the EU will be interconnected and made freely accessible to the general public.[58] The agreement also includes other proposals which are expected to enhance the resilience of the Union against money laundering. For example, public authorities will have access to real estate ownership; there will be tougher criteria for assessing third countries with an increased risk of money laundering; protection of whistleblowers who report money laundering from discrimination in the workplace and protection of their identity.[59]

If strongly implemented, the agreement will be a major step forward towards a better European AML system. However, some major loopholes will still need to be closed in the future. For example, registers of trusts and other legal arrangements will be accessible only from those with a legitimate interest, while companies and trusts located in third countries but with business ties to the European Union will not be included in the national registers.

The global impact of the Panama Papers can serve alone to demonstrate the benefits of public disclosure of beneficial ownership information: eight months after the scandal, at least 150 inquiries, audits and investigations had been announced in 79 countries around the world and governments were investigating more than 6,500 taxpayers and companies, and had recouped at least $110 million so far in unpaid taxes or asset seizures.[60] There is also a business case for greater beneficial ownership transparency. A survey by the accountancy firm Ernst & Young found that 91% of senior executive believe it is important to know the ultimate beneficial ownership of the entities with which they do business.[61]

[55] European Commission "Proposal for a Directive of the European Parliament and the Council for amending Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing"
[56] European Commission (2016), Impact assessment accompanying the document "Proposal for a Directive of the European Parliament and the Council for amending Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, p.95
[57] http://www.eurodad.org/Entries/view/1546711/2017/02/28/EU-parliament-gets-serious-about-responding-to-the-Panama-Papers-by-fighting-corruption-and-tax-abuse
[58] http://www.sven-giegold.de/2017/lost-and-won-details-of-the-compromise-on-the-european-anti-money-laundering-directive/
[59] ibid.
[60] https://panamapapers.icij.org/blog/20161201-impact-graphic.html
[61] Ernst & Young, Global Fraud Survey 2016, http://www.ey.com/gl/en/services/assurance/fraud-investigation---dispute-services/ey-global-fraud-survey-2016

3. Money laundering in the post-Soviet space and the role of Latvian banks

Systemic corruption has been a particularly persistent problem in the countries of the former Soviet Union in Eastern Europe and Central Asia. It has excluded their populations from enjoying the benefits of economic development, complicating doing business there and impeding engaging in mutually beneficial economic or social partnerships.

In many cases, corruption in the post-Soviet space has seen the emergence of powerful kleptocratic networks operating across states and weaving together public-sector, state-owned enterprises, private businesses as well as outright criminal organizations.[62] The capture of important institutions by powerful political and business elites, and the failure to consistently prosecute those who abuse power for private gains, have seriously undermined the democratic progress, reducing the political and social liberties of their populations.

Much of the resilience of corrupt networks in the post-Soviet space has derived from their ability to effectively accumulate, hide, transfer and use enormous amounts of stolen wealth to expand their control on key state and private institutions. This has entailed the running of sophisticated money laundering schemes to 'layer' funds into the global financial system, often through the use of "money laundering platforms"- These are networks of anonymous shell companies with accounts in a group of collaborative banks, through which the funds are handled in such a way as to systematize complex chains of transactions and obscure the flow of illicit money, hiding the perpetrators.[63]

For investigators and law enforcement authorities across the world it has been more difficult and frustrating to go after money laundering platforms, since they have been usually characterized by the 'mixing' of the illicit funds from different criminal activities and the almost complete lack of any ownership link between the source of funds and the group of shell companies, which allows perpetrators to hide their identity and avoid prosecution.[64]

Given current difficulties in determining the identities of those truly benefiting from offshore corporations and their transactions, banks around the world that take money without carefully examining the ownership structure of the shell companies investing it should probably considered as key enablers of kleptocracies' money laundering schemes, although their involvement may be in many cases unintentional.[65]

As emerged from several investigations, in the course of the last decade and at least up to 2016, Latvian banks played a key role in facilitating the laundering and the movement of massive sums of illicit funds from the former Soviet Union into the international financial system, usually figuring in conjunction with their depositors – platforms of anonymous shell companies registered in multiple offshore jurisdictions.[66]

These platforms were prominently used to carry out 'trade-based' money laundering (TBML), consisting in the use of complex schemes of fraudulent trade transactions in an attempt to legitimize the illicit origins of the funds by means of misrepresentation of price, quantity or quality of imports or exports (also called misinvoicing)".[67] In other instances, they were used to set up complex chains of fictitious loans between the shell companies, so that perpetrators can create an information trail to justify transfers of criminal proceeds through banking channels – without any economic reality.[68]

---

[62] Chayes S. (2016), 'The Structure of Corruption: A Systemic Analysis Using Eurasian Cases', Carnegie Endowment for International Peace, http://carnegieendowment.org/2016/06/30/structure-of-corruption-systemic-analysis-using-eurasian-cases-pub-63991

[63] Stack G. (2015), 'Baltic shells: on the mechanics of trade-based money-laundering in the former Soviet space', Journal of Money Laundering Control, vol.18 Issue: 1, pp. 81-98

[64] ibid.

[65] Chayes S. (2016), The Structure of Corruption: A Systemic Analysis Using Eurasian Cases, Carnegie Endowment for International Peace, p.26, http://carnegieendowment.org/2016/06/30/structure-of-corruption-systemic-analysis-using-eurasian-cases-pub-63991

[66] 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 Issue: 4, pp. 496-512

[67] Financial Action Task Force (2006), "Trade-based money laundering", available at: http://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaundering.html

[68] European Commission (2017), "Supra-national risk assessment (SNRA) of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities", p. 114, available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272

Latvian banks were mentioned, for example, in the "Magnitsky affair", in which, between 2007 and 2008, $230 million were fraudulently stolen from the treasury of the Russian Federation by a criminal network which included Russian top public officials. Of the stolen $230 million, at least $63 million passed through six Latvian banks, where offshore shell companies used for the fraud held accounts. Sergei Magnitsky, the lawyer who discovered the fraud, was eventually arrested by the Russian authorities and died in jail amid alleged violations of human rights.[69] As law enforcement investigations unfolded, it was found that the shell companies used in the fraud were part of a wider network, used for other – unrelated – money laundering schemes around the world also featuring Latvian banks. Among these were the laundering of $40 millions of drug profits from the Mexican cartel Sinaloa, the laundering of around $800 millions in criminal proceeds from a Vietnamese smuggling ring, and a $10.4 millions financial fraud conducted by the US investment firm Rockford. [70]

In other instances, political and financial elites from former Soviet states, endangered by rapid political and social changes in their countries, were able to route their capital through Latvian banks in order to circumvent scrutiny over their transactions and secure their financial assets by wiring them to various offshore jurisdictions across the world.[71] For example, a 2012 report from Global Witness shows how in 2010 the former President of Kyrgyzstan, Kurmanbek Bakiyev, used a shell company registered in Belize with account in a Latvian bank to wire offshore $31.7 millions of embezzled state funds, just before being overthrown by a revolution.[72] Another example relates to the Kazakh banker Mukhtar Ablyazov, who was accused of defrauding over $10 billion from the Kazakh bank he was in charge of through 30 offshore shell companies managed by Latvian nominee directors. According to investigations, about $1 billion dollar went through four Latvian banks.[73]

Latvian banks were also mentioned in some of the biggest and most complex money laundering schemes operating in Eurasia, running over extended periods of time – sometimes years – and involving thousands of shell companies and tens of thousands of transactions. These have been labelled "laundromats" by investigative journalists across the world. In recent years, laundromats have been exposed involving Russia, Moldova[74] and most recently Azerbaijan[75], with illicit funds totalling up to €90 billion from just these countries. The laundromats were used by politicians, public officials, organized criminal groups and ordinary businesses to embezzle funds, disguise the origins of money, evade taxes or sanctions, pay bribes, or move funds from high corruption risk environments to safe markets and secure offshore locations.[76]

[69] Galeotti M. & Bowen A. (2014), 'Latvia and Money Laundering: An Examination of Regulatory and Institutional Effectiveness in Combating Money Laundering', Central European Journal of International and Security Studies, Issue 8:4, p.170
[70] Stack G. (2015), 'Baltic shells: on the mechanics of trade-based money-laundering in the former Soviet space', Journal of Money Laundering Control, vol.18 Issue: 1, pp. 81-98
[71] Galeotti M. & Bowen A. (2014), 'Latvia and Money Laundering: An Examination of Regulatory and Institutional Effectiveness in Combating Money Laundering', Central European Journal of International and Security Studies, Issue 8:4
[72] Global Witness (2012), 'Grave Secrecy: How a Dead Man Can Own a UK Company and other Hair-Raising Stories About Hidden Ownership from Kyrgyzstan and Beyond', available at: https://www.globalwitness.org/en/campaigns/corruption-and-money-laundering/anonymous-company-owners/grave-secrecy/
[73] Galeotti M. & Bowen A. (2014), 'Latvia and Money Laundering: An Examination of Regulatory and Institutional Effectiveness in Combating Money Laundering', Central European Journal of International and Security Studies, Issue 8:4
[74] Organized Crime and Corruption Reporting Project (OCCRP) (2017), 'The Russian Laundromat Exposed', https://www.occrp.org/en/laundromat/the-russian-laundromat-exposed/ [Accessed 22 October 2017]
[75] Organized Crime and Corruption Reporting Project (OCCRP) (2017), 'The Azerbaijani Laundromat', https://www.occrp.org/en/azerbaijanilaundromat/ [Accessed 22 October 2017]
[76] Transparency International-UK (2017), 'Hiding in Plain Sight: How UK Companies Are Used to Launder Corrupt Wealth', http://www.transparency.org.uk/publications/hiding-in-plain-sight/#.Wj6iTVKZPVr

All the investigations also revealed the key role played by a range of intermediaries – such as Trust and Corporate Service Providers, lawyers, lobbyists and middlemen – in enabling money laundering schemes across the world by offering a range of services, including the *en-masse* creation of anonymous shell companies equipped with nominee directors and the opening of bank accounts for them in partnered banks, including Latvian ones.

The level of involvement of these organizations with corrupt networks running money laundering schemes has varied. On the one hand of the scale, they were active and integral part of the networks, providing specific services to the members; at the other end of the scale, they appeared to provide on-demand services to all comers without questioning too much the purposes of the operations they were helping with.

The tracing of these actors and the extent of their activities has been difficult due to their loose transnational structures and the shifting collaborations with each other. This was facilitated by their opaque nature and the scarcity of both information and controls, at the national and international level, on the sector, hindering money laundering investigations.

3.1 Financial logistics services

Upon examination of documented instances of illicit financial flows centred in Latvia, while the period where the biggest money laundering schemes goes from 2009 to 2016, the banking institutions at the centre are almost always domestic banks primarily serving foreign customers. The reasons for this lie in some unique features of Latvia's banking sector and its development after the global financial crisis.

The largest banks in the country are Nordic-owned banks, controlling large part of the overall banking assets and dominating the retail and domestic lending sectors. As such, Latvia-based commercial banks have turned to attracting deposits and business from customers in the countries of the former Soviet Union as their main source of growth.[77] However, differently from other financial hubs such as Switzerland and Cyprus, where banks are focused on attracting non-resident customers' money for long periods and maintaining the value of deposited funds, Latvian banks specialised in short-term, on-demand deposits, used to facilitate the transit of funds from one jurisdiction to another.[78]

In 2012, the Latvian regulator, the Financial and Capital Market Commission (FCMC), acknowledged this business model, referring to it as the provision of "financial logistics services" – the 'export of financial services that improves also the payment of balance sheet in Latvia'.[79] While this business model was pioneered by Latvian banks, it has also existed in countries as diverse as Moldova, Cyprus, Belarus, Kyrgyzstan, Estonia and Lithuania.[80]

The attraction of non-resident deposits from the former Soviet Union in Latvia has been favoured by a combination of different factors. Apart from the strategic geographic position of the country, the stabilising mechanisms put in place in the financial sector in the aftermath of the 2007-2008 global financial crisis, as well as EU membership, allowed Latvia to become a secure financial location, offering legally protected banking services and granting easy access to the banking system of the European Union.[81]

Latvian banks' business in Eurasia has also been facilitated by their ability to provide banking services in Russian language and by the establishment of representative offices in Russia, Ukraine, Moldova, Kazakhstan, Belarus, Uzbekistan and Azerbaijan. Through these offices and their websites, Latvian banks have advertised a wide range

[77] Galeotti M. & Bowen A. (2014), 'Latvia and Money Laundering: An Examination of Regulatory and Institutional Effectiveness in Combating Money Laundering', Central European Journal of International and Security Studies, Issue 8:4, p.160
[78] 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 Issue: 4, pp. 496-512
[79] Financial and Capital Market Commission (FCMC) (2012), "Non-resident banking business in Latvia", Benefits and Risks, 26 November, available at: http://www.fktk.lv/en/media-room/press-releases/4040-2012-11-26-nonresident-banking-busi.html
[80] 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 Issue: 4, pp. 496-512
[81] Galeotti M. & Bowen A. (2014), 'Latvia and Money Laundering: An Examination of Regulatory and Institutional Effectiveness in Combating Money Laundering', Central European Journal of International and Security Studies, Issue 8:4

of corporate services (i.e. company incorporation and remote account management) as well as the extent of their correspondent banking network, the speed of account opening and the speed of transactions' wiring.[82]

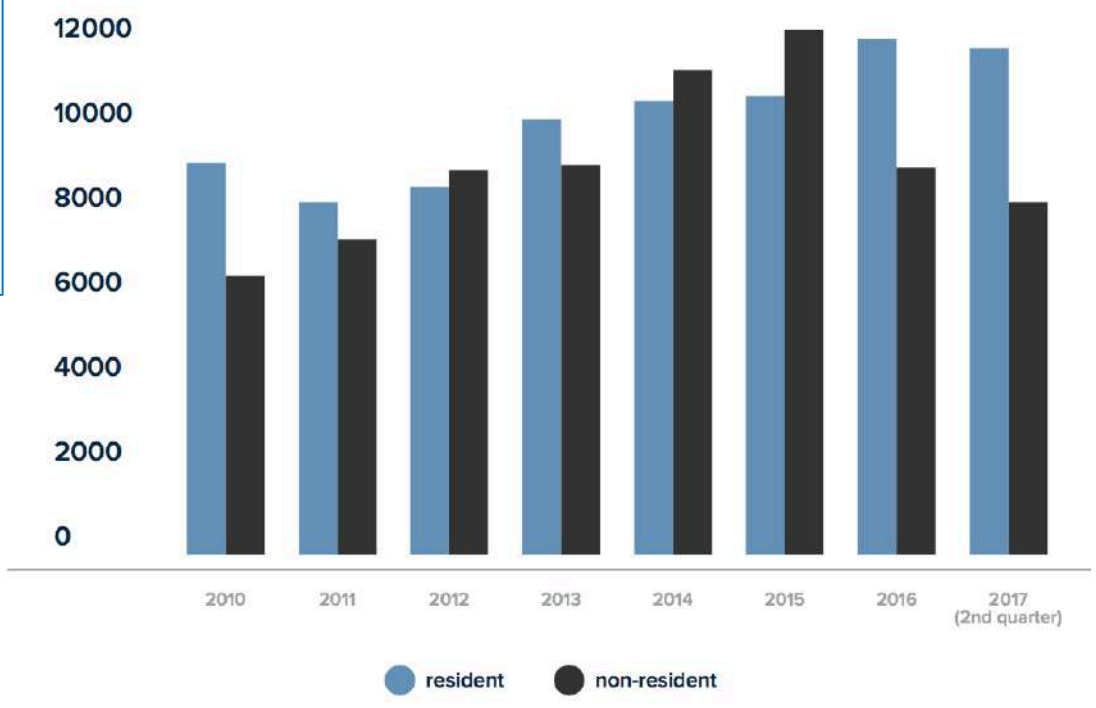
As a result of the export of financial logistics services, non-resident deposits in Latvian banks had increased by 32% from 2010 to 2013, making up 49% of all bank deposits held in Latvia.[83] According to the International Monetary Fund, in 2013, the vast majority (80-90%) of Latvian banks' non-resident deposits was made up by individuals and entities from the former Soviet Union. 90% of them owned their deposits via legal entities – most of them shell companies – incorporated in jurisdictions outside the FSU.[84]

With the acceptance of Latvia into the Eurozone, banking connections and transfers became much easier. Yet, despite this, domestic banks did not concentrate on opening subsidiaries or banking offices in other EU Member States. Instead, they focused on opening offices in Eurasia to court non-resident deposits from those countries.[85]

According to a 2015 OECD report on Latvia and foreign bribery, some banks stated that more than half of their deposits originated from outside Latvia, while others said to have more than 90% of their assets and liabilities linked to non-resident deposits.[86] The same report found loopholes in the regulatory framework which allowed banks to de-prioritize the risk coming from non-resident deposits originated in the former Soviet Union. Moreover, the in-taking of non-resident deposits itself was not listed among financial institutions' activities considered at risk of money laundering.[87] The amount of non-resident deposits reached its peak in 2015, when they constituted 53.1% of overall deposits in Latvian banks, a sum equivalent to 40% of Latvian annual GDP.[88]

Chart 1 – Amount of resident and non-resident deposits in Latvian banks (€ millions), 2010-2017

Source: Association of Latvian Commercial Banks (ALCB)

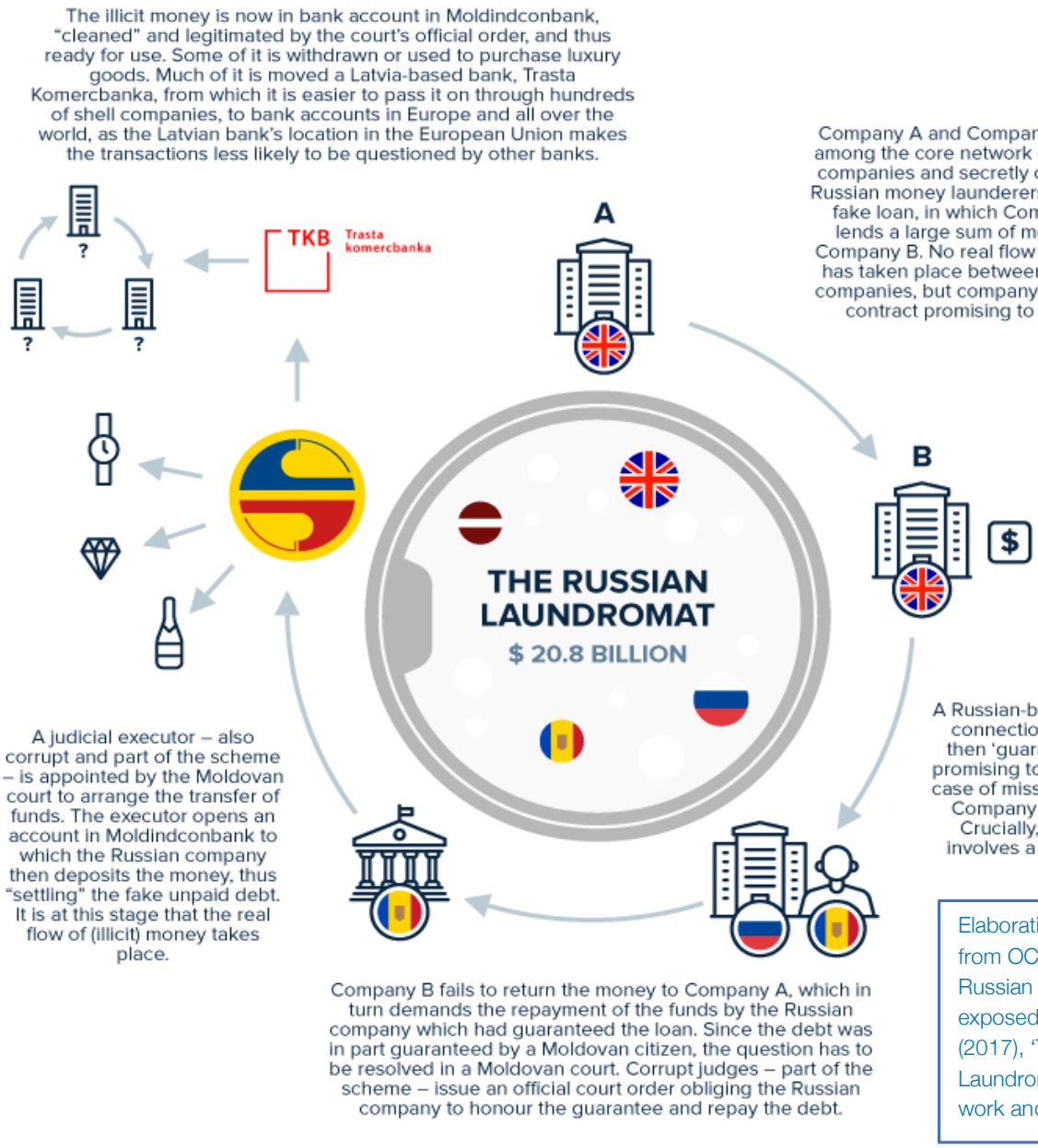


[82] Stack G. (2015), 'Shell companies, Latvian-type correspondent banking, money laundering and illicit financial flows from Russia and the Former Soviet Union', Journal of Money Laundering Control, vol. 18 Issue: 4, pp. 496-512
[83] Galeotti M. & Bowen A. (2014), 'Latvia and Money Laundering: An Examination of Regulatory and Institutional Effectiveness in Combating Money Laundering', Central European Journal of International and Security Studies, Issue 8:4, p.158
[84] International Monetary Fund (2013), 'Latvia: IMF Country Report No. 13/28', available at: https://www.imf.org/external/pubs/ft/scr/2013/cr1328.pdf
[85] Galeotti M. & Bowen A. (2014), 'Latvia and Money Laundering: An Examination of Regulatory and Institutional Effectiveness in Combating Money Laundering', Central European Journal of International and Security Studies, Issue 8:4, p.158
[86] OECD (2015), Phase 2 Report on Implementing the OECD Anti-Bribery Convention in Latvia, pp. 27, available at http://www.oecd.org/daf/anti-bribery/Latvia-Phase-2-Report-ENG.pdf
[87] ibid.
[88] Re:Baltica (2016), 'US pressures Latvia to clean up its non-resident banks', https://en.rebaltica.lv/2016/02/u-s-pressures-latvia-to-clean-up-its-non-resident-banks/ [accessed 30 Oct 2017]

Eventually, it emerged that weaknesses in Latvia's AML system, combined with their extensive correspondent banking network and the untraceable ownership of their client offshore companies allowed for the injection of illicit financial flows worth billions in the global financial system.

This was demonstrated when, between 2014 and 2017, investigative journalists from the NGO OCCRP (Organized Crime and Corruption Reporting Project) and media organizations from 29 countries exposed the details of the so-called "Russian Laundromat", labelled by some as the "biggest money laundering system ever operating in Eastern Europe".[89] The investigations revealed how, between 2009 and 2014, a transnational criminal network of about 500 individuals encompassing Russia, Moldova and Ukraine laundered at least $20.8 billion dollars of illicit funds from 19 Russian banks by using a platform of 21 shell companies registered in the UK, Cyprus and New Zealand – with accounts in the Latvian Trasta Komercbanka and the Moldovan Moldindconbank.

How did the Russian Laundromat work?



Elaboration of the author from OCCRP (2017), 'The Russian Laundromat exposed', and The Guardian (2017), 'The Global Laundromat: how did it work and who benefited?'

[89] Organized Crime and Corruption Reporting Project (2017), 'The Russian Laundromat Exposed', https://www.occrp.org/en/laundromat/ [Accessed October 18, 2017]

The platform of shell companies used in the Russian Laundromat operated 26,746 payments to other 5,140 companies with accounts at 732 banks in 96 countries, allowing for the money to be anonymously dissipated across the global financial system, passing without obstacles even through some of the world's biggest banks. Of these $20.8 billion, nearly $13 billion passed through Trasta Komercbanka.[90]

Between 2012 and 2015, the same period in which the Global Laundromat scheme was taking place, Moldova and Latvian banks were protagonist of another huge fraud. A criminal network with connections to corrupt individuals in Moldovan political parties and government institutions fraudulently acquired ownership of and stole around $1 billion from three Moldovan banks. This was made through a network of UK shell companies with bank accounts in three Latvian banks. [91] The consequences of the robbery were devastating for Moldova, as the banks had to be rescued with money from the public coffers, depriving Moldova of 12% of its annual GDP and throwing the country into political turmoil.[92]

Latvian banks carried many responsibilities in enabling these and several other money laundering schemes over the previous years. Their business model had been characterized by disproportionately high money laundering risk appetite, not corresponding to the capacity of those banks to manage such risks. While Customer Due Diligence officers had not been able to identify complex related relations between customers and analyse activities of participants in group of companies operating through the bank, transaction monitoring systems were outdated and systematically failed in detecting the large number of ongoing illicit activities.[93]

The scandals also exposed major weaknesses in the international and European correspondent banking system. As in that period banks in many EU countries were not required to do large amounts of due diligence procedures on transactions not warranting suspicion from banks within the EU, what occurred is that they trusted the banks they were receiving money from, thus layering enormous amounts of illicit funds, often unknowingly. The speed at which wire-transfers of money was made exacerbated the effect.[94]

The role of Latvian banks in facilitating illicit financial flows has gone even beyond the post-Soviet space, with detrimental effects to international security. In June and July 2017, following an investigation by the FBI, it was revealed that, between 2009 and 2016, five Latvian banks were used by the North Korean regime in circumventing international sanctions targeting its programmes of intercontinental ballistic missiles and nuclear weapons, including related export of goods and equipment.[95]

The illicit transactions, carried out through a complex chain of offshore companies, did not directly involve entities appearing on EU, UN or US sanction lists, which were circumvented by using a network of intermediaries. Despite the transactions contained red flags such as offshore companies sharing the same officers and located at the same address, and cycling payments to the same beneficiaries, Latvian banks failed to detect them due to their weaknesses in internal anti-money laundering systems. [96] This demonstrates how offshore secrecy can have wider repercussions in terms of international security.

[90] The Guardian (2017), 'The Global Laundromat: how did it work and who benefited?' https://www.theguardian.com/world/2017/mar/20/the-global-laundromat-how-did-it-work-and-who-benefited [Accessed October 18, 2017]
[91] Organized Crime and Corruption Reporting Project (2015), 'Grand Theft Moldova', https://www.occrp.org/en/laundromat/grand-theft-moldova/ [Accessed October 18, 2017]
[92] Reuters (2015), 'Billion-dollar bank scam shakes faith in little Moldova's pro-EU leaders', http://www.reuters.com/article/us-moldova-fraud-insight/billion-dollar-bank-scam-shakes-faith-in-little-moldovas-pro-eu-leaders-idUSKCN0QF1KC20150810 [Accessed October 18, 2017]
[93] Latvian National Money Laundering/Terrorism Financing Risk Assessment Report (2017), pp.64-65, available at: http://www.kd.gov.lv/images/Downloads/useful/ML_TF_ENG_FINAL.pdf
[94] Kegö W. & Georgieff A. (2013), The Threat of Russian Criminal Money: Reassessing EU Anti-Money Laundering Policy, Stockholm: Institute for Security and Development Policy
[95] Reuters (2017), 'Latvian banks fined for breaching North Korea sanctions: watchdog', http://www.reuters.com/article/us-latvia-moneylaundering/latvian-banks-fined-for-breaching-north-korea-sanctions-watchdog-idUSKBN1A6217 [Last accessed: 22 October 2017]
[96] Financial and Capital Market Commission (2017), 'FCMC in collaboration with U.S. law enforcement authorities identifies weaknesses and imposes monetary fines on three banks', http://www.fktk.lv/en/media-room/press-releases/6429-fcmc-in-collaboration-with-u-s-law-enforcement-authorities-identifies-weaknesses-and-imposes-monetary-fines-on-three-banks.html [Last accessed 22 October 2017]

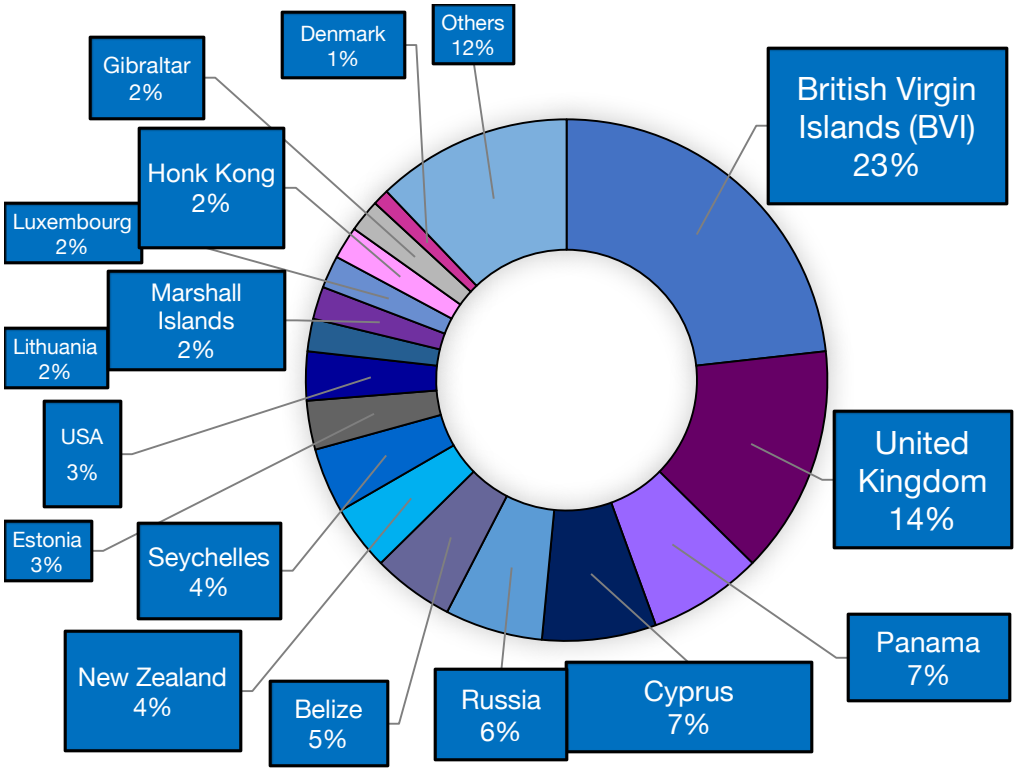
3.2 Latvian banks, shell companies and money laundering

Chart 2, based on statistics obtained by investigative journalist Graham Stack from the Latvian financial regulator, the FCMC, shows the percentage of account holders – divided per jurisdiction – in Latvian banks in 2011.[97] The figure is outdated and very likely does not reflect the current situation; however, it provides evidence that in that period Latvian banks prominently relied on shell companies lacking information on beneficial owners to provide their financial logistic services.

While the vast majority of non-resident deposits was owned by legal entities registered in popular secrecy offshore locations (British Virgin Islands, Panama, Belize, Seychelles, Hong Kong)[98], a substantial percentage is made up of companies registered in what would be considered "onshore" jurisdictions, such as the UK and New Zealand. As emerged, loopholes in domestic company laws of these latter countries made it possible to achieve a high level of anonymity, through scarce regulation of nominee directors and the provision of specific corporate vehicles not required to disclose their beneficial owners. Indeed, both New Zealand and UK shell companies with Latvian bank accounts have figured prominently in many of the money laundering scandals involving criminal networks from the former Soviet Union. However, this was due not only to the potential anonymity offered, but also to their impeccable reputation and speedy and low-cost incorporation and maintenance.

Chart 2 – Jurisdictions of corporate vehicles owning non-resident deposits in Latvian banks, 2011

Source: Financial and Capital Market Commission data for 2011 provided to journalist Graham Stack, no current data



According to Stack, there appears to be a trade-off between anonymity and the "air of legitimacy" when incorporating shell companies. Money launderers, in order to conduct their business undisturbed, may use corporate vehicles registered in jurisdictions with lower protection of beneficial owners than a classic offshore secrecy haven, but with a better reputation and lower risk profiles, unlikely to trigger red flags.[99] Another key factor of attraction is the ease of administration (cost and speed of setting up a new business and maintaining its files) offered by a determinate jurisdiction. The World Bank's *Doing Business* rating[100] can be a considered a good indicator of this, as it is particularly focused on small businesses and shell companies can be classified as such.

[97] 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 Issue: 4, pp. 496-512
[98] http://www.financialsecrecyindex.com/introduction/fsi-2015-results
[99] 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 Issue: 4, pp. 496-512
[100] http://www.doingbusiness.org/rankings

Corrupt networks, therefore, looking for an ideal combination of anonymity, reputation and ease of administration, may engage in "jurisdictional arbitrage" and take advantage of the discrepancies between company laws and AML regulations across countries in order to incorporate large quantities of anonymous shell companies useful for their purposes.

New Zealand, for example, rates 1st in the World Bank's Doing Business rating and it is one of the easiest place in the world where to set up a business.[101] However, up to 2016, its trusts and companies' regime did not require maintaining beneficial owners' details and allowed nominee directors. The country was criticised by the OECD in 2013 for these deficiencies in its anti-money laundering regulations and the ease with which "shell companies were being established there as fronts for international laundering of drug money, fraud and terrorism.[102]

It was thanks to information related to one New Zealand shell company, Tormex Limited, with account in a small Latvian bank that investigators were able to unfold the network of around 100 anonymous shell companies behind the Magnitsky affair, the laundering of the proceeds of crime from the Mexican cartel Sinaloa and a Vietnamese smuggling ring, as well as a financial fraud from a US firm.[103] A number of NZ shell companies were also mentioned in the Russian Laundromat and had a high number of connections with the Panama Papers and related controversial deals in 2016.[104]

Acknowledging the vulnerability of New Zealand shell companies to abuse for money laundering schemes around the world, the New Zealand government significantly strengthened its anti-money laundering regulatory framework, introducing tougher disclosure requirements for companies and foreign trusts as well as stricter measures for intermediaries, resulting in a 75% decrease in the incorporation of companies and foreign trusts there.[105] This indicates that a jurisdiction may exhaust its reputational advantages when illegal activities are exposed in the media and governments strengthen regulations as a consequence.[106]

[101] http://www.doingbusiness.org/rankings
[102] OECD (2013), 'Phase 3 Report on Implementing the OECD Anti-Bribery Convention in New Zealand', available at: http://www.oecd.org/daf/anti-bribery/NewZealandPhase3ReportEN.pdf
[103] Stack G. (2015), 'Baltic shells: on the mechanics of trade-based money-laundering in the former Soviet space', Journal of Money Laundering Control, vol.18 Issue: 1, pp. 81-98
[104] Australian Financial Review (2016), 'The Panama Papers: Behind Mossack Fonseca's Secret New Zealand Deals', http://www.afr.com/news/politics/world/the-panama-papers-behind-mossack-fonsecas-secret-new-zealand-deals-20160506-gonstp [accessed 30 October 2017]
[105] Stuff (2017), 'NZ foreign trust numbers plummet after post-Panama Papers rules kick in', https://www.stuff.co.nz/business/industries/94403144/foreign-trust-numbers-plummet-after-postpanama-papers-rules-kick-in [accessed 30 October 2017]
[106] 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 Issue: 4, pp. 496-512, p.500

International investigations on the evasion of sanctions by North Korea point at the systematic use of offshore shell companies carrying out complex chains of transactions across multiple countries. This allowed the rogue regime to export its raw goods and obtain payments in US dollars in order to fund its intercontinental ballistic missile and nuclear weapons development programmes. According to a recent report from anti-money laundering specialist ACAMS, 'tracking down the North Korean front companies is tricky business, as these have used 'a series of perpetually evolving sanctions-evasion schemes', and North Korea has 'advanced' these capabilities despite international embargoes.[107]

These schemes include, for example, complex ledger systems tracking debits and revenues between North Korean entities and partnered-Chinese front companies aimed at exporting North Korea's raw goods and obtain profits in US dollars; or the use of shell companies and nominees in secrecy jurisdictions allowing North Korea to pay its imports from other countries in US dollars.[108] This method was used by a Russian company in June 2017 to receive payments from North Korea for the shipment of over $1 million in petroleum products. The scheme involved two shell companies based in Singapore creating the illusion of transactions between Singapore and Russia.[109]

A recent report from the UN Panel Experts on North Korea, has found that Hong Kong – together with the British Virgin Islands – has been one of the business jurisdictions where North Korea has set up the largest share of shell companies used for the evasion of international sanctions.[110] A 2016 report from C4ADS, a Washington-based non-profit firm which conducts data-driven analysis of security issues, identified at least 160 Hong Kong companies indirectly controlled by North Korea through the use of frontmen and/or intermediaries.[111]

Hong Kong appeal for offshore business may derive from its favourable company incorporation laws. The jurisdiction ranks 5th in the World Bank's doing business rating.[112] To start a company in Hong Kong, one needs at least one director (has to be an actual person) and a company secretary (which can either be a person or another company, but must be based in Hong Kong). Though the company's registered office must be in Hong Kong, they are allowed to share an office with their company secretary and neither technically has to operate out of that address, even though doing this is considered a red flag for money laundering investigations.[113]

According to CNN, to service offshore clients, there are plenty of "secretarial services" that provide company directors abroad with assistance. An example of this is represented by Unaforte Limited Hong Kong and its listed company secretary, Prolive Consultants Limited, both accused of helping North Korea access the global financial system. As reported by CNN, while Unaforte's company information shows up in Hong Kong public register of companies, the name of just one individual from the Caribbean island of Dominica appears, with only a passport number, not a phone number.[114]

The link between Latvian banks and the North Korean network is substantiated by the high percentage of BVI companies and the presence of Hong-Kong companies among the depositors, as noted by statistics above. Although it may be that not all of them were involved in the schemes, investigations suggest there is a high risk that a majority of them was.

---

[107] The Epoch Times (2017), 'Banks Begin Hunt for North Korean Front Companies' https://www.theepochtimes.com/banks-begin-hunt-for-north-korean-front-companies_2340899.html [accessed 30 October 2017]
[108] Foundation for Defense of Democracies (2017), 'A legislative proposal to impede North Korea's access to finance', Testimony to the US Congress, Washington DC, 13.09.17, http://www.defenddemocracy.org/content/uploads/documents/09-13-17_AR_HFSC_Testimony.pdf
[109] ibid.
[110] United Nations Security Council, Midterm report of the Panel of Experts established pursuant to resolution 1874 (2009),: http://www.un.org/ga/search/view_doc.asp?symbol=S/2017/742
[111] C4ADS (2017), 'Risky Business: A System-Level Analysis of the North Korean Proliferation Financing System', https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/59413c8bebbd1ac3194eafb1/1497447588968/Risky+Business-C4ADS.pdf
[112] http://www.doingbusiness.org/rankings
[113] CNN (2017), 'Hiding in Plain Sight: Why Hong Kong is a preferred spot by North Korean money launderers' http://edition.cnn.com/2017/10/16/asia/hong-kong-north-korea/index.html?_ga=2.263234382.310622638.1509187684-1794146971.1509187684 [accessed 30 October 2017]
[114] ibid.

Connections with the United Kingdom

In recent years the UK has also become an attractive place for money launderers and corrupt networks around the world to set up shell companies. This is due to the good reputation of the jurisdiction, the ease of setting up a business there and the potential anonymity of its corporate vehicles.

Whereas incorporating a company in the British Virgin Islands may cost around £1,000 and take a number of days, formation of UK companies may cost as little as £12 and take just few hours.[115] Up to June 2016, when the UK government set up the public register of beneficial owners in response to the Panama Papers, it was possible to incorporate most of them without revealing the identity of their true owners.

An open source analysis conducted by Transparency International-UK has identified 766 UK firms used in 52 major high-end money laundering schemes around the world, worth around €90 billion in illicit wealth.[116] As revealed by several investigations over the years, the combination of British shell companies with Baltic bank accounts was particularly common to move illicit funds from the former Soviet States into the international financial system. According to data obtained by OCCRP for TI-UK, of 440 UK shell companies used in the Russian Laundromat, 392 of these had accounts in the Baltics, with 270 firms using Latvian banks and 122 using Estonian banks.[117] In the Moldovan bank robbery, UK shell companies with accounts in three Latvian banks were used in all the phases of the scheme.

Chart 3 - Jurisdictions of the banks where the 440 UK-registered shell companies used in the Russian Laundromat held accounts. In dark grey, number of companies with accounts in Latvian banks; in light grey, number of companies with accounts in Estonia banks.

Source: Transparency International-UK, 'Hiding in Plain Sight: how UK companies are used to launder corrupt wealth'

Among UK shell companies used for criminal activities, of particular concern have been partnership structures such as UK Limited Liability Partnerships (LLPs) and Scottish Limited Partnerships (SLPs), which together made up around 75% of firms identified by TI-UK open source analysis.[118] The reason why these vehicles have been so attractive to money launderers is that loopholes in the UK AML regulations have not required to list real people as their partners, thus allowing them to be anonymously owned by two companies potentially based in secrecy

[115] Transparency International-UK (2017), Hiding in Plain Sight: how UK companies are used to launder corrupt wealth, p.11, http://www.transparency.org.uk/publications/hiding-in-plain-sight/#.Wj6iTVKZPVr
[116] ibid. p.12
[117] ibid. p.30
[118] ibid. p.13

havens.[119] In practical terms, this has meant that money launderers could set up vast networks of hundreds of UK corporate entities and interlinked partners based in secrecy jurisdictions, making it almost impossible for investigators and LEAs to identify the people behind them.

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.[120] Due to their involvement in several money laundering cases related to Latvian banks, the 2017 NRA pointed out that UK companies constitute one of the major threats to Latvia's financial system.[121]

The abuse of UK LPs with Baltic bank accounts was also evident in the so-called "Azerbaijani Laundromat", a complex $2.9-billion money laundering scheme ran between 2012 and 2014 by the Azerbaijani elite to curry influence, pay lobbyists, apologists and European politicians in order to promote a favourable image of Azerbaijan across the world.[122] The scheme was carried out with four UK Limited Partnerships with bank accounts in the Estonian branch of Danske bank. The LPs' partners were all anonymous entities registered in the British Virgin Islands, Seychelles and Belize.[123]

Latvia was also mentioned in connection with the scheme. In what has been called "Caviar Diplomacy" case, one Latvian bank was allegedly used to pay part of a €2.3 million bribe (€220.000), paid by Azerbaijani lobbyists to the Italian politician Luca Volontè, former chair of the centre-right European People's party in the Parliamentary Assembly of the Council of Europe (PACE)[124]. This was made order to influence and distort, in favour of Azerbaijan, resolutions related to the alleged violation of human rights by the government in various political elections held in the country. The rest of the bribe was paid by the UK shell companies with account in the Estonia.[125]

In the last two years, the British government has sought to put an end to the widespread abuse of UK companies for illicit purposes, taking measures to increase transparency of company ownership and control. by setting up a public register of beneficial owners in 2016 and requiring UK Limited Companies and Limited Liability Partnerships to file annual accounts for availability to the public.[126] In June 2017, the UK Government also brought Scottish Limited Partnerships under the beneficial ownership regime, thus closing the loophole which had allowed these corporate vehicles to be owned anonymously by two offshore partners and reducing their vulnerability to abuse.[127]

However, an analysis by Bellingcat and the Scottish Herald shows that risks remain with 16,000 SLPs – 60% of the active partnerships – not complying with the new laws. Of those that have complied, 72% of beneficial owners come from former Soviet states with significant corruption problems.[128]

The abuse of SLPs with Latvian bank accounts for illicit activities was made particularly evident by the Great Moldovan Bank Robbery, in which $1 billion was fraudulently stolen from three banks in Moldova, with devastating consequences for the country.

---

[119] ibid. pp.12-15
[120] ibid.
[121] Latvian National Money Laundering/Terrorism Financing Risk Assessment Report (2017), pp.56-57, available at: http://www.kd.gov.lv/images/Downloads/useful/ML_TF_ENG_FINAL.pdf
[122] The Guardian (2017), 'UK at the centre of secret $3bn Azerbaijani money laundering and lobbying scheme', https://www.theguardian.com/world/2017/sep/04/uk-at-centre-of-secret-3bn-azerbaijani-money-laundering-and-lobbying-scheme [Last accessed 22 October 2017]
[123] ibid.
[124] European Stability Initiative (2012), 'Caviar Diplomacy: How Azerbaijan Silenced the Council of Europe', available at: http://www.esiweb.org/pdf/esi_document_id_131.pdf [Last Accessed 22 October 2017]; European Stability Initiative (2016), 'The European Swamp (Caviar Diplomacy Part 2)', available at: http://www.esiweb.org/index.php?lang=en&id=156&document_ID=181 [Last accessed 22 October 2017]
[125] ibid.
[126] Transparency International-UK (2017), Hiding in Plain Sight: how UK companies are used to launder corrupt wealth, pp.12-15 http://www.transparency.org.uk/publications/hiding-in-plain-sight/#.Wj6iTVKZPVr
[127] ibid.
[128] The Scottish Herald (2017), 'Herald research: Scots tax haven firms bypassing transparency law', http://www.heraldscotland.com/news/crime_courts/15526548.Herald_research__Scots__tax_haven__firms_bypassing_transparency_laws/ [accessed 30 October 2017]

Case study – The Great Moldovan Bank Robbery: how UK shell companies with Latvian bank accounts allowed the 'biggest theft of the century'

Following the scandal which saw around $1 billion vanish from three Moldovan banks at the end of 2014, the National Bank of Moldova hired the US firm Kroll to investigate on the mechanism of the fraud. Kroll's final report was leaked in 2015 by the speaker of Moldova's Parliament Andrian Candu, revealing the central role played by UK SLPs with Latvian bank accounts in all phases of the robbery.[1]

Since summer 2012 till June 2013, the three banks were subject to significant shareholder change, with the effect of transferring ownership to a number of apparently unconnected individuals and entities. The large majority of the funds used to acquire shares in the bank were provided by loans from UK-registered Limited Partnerships with accounts in three Latvian banks (ABLV, Privatbank and Latvijas Pasta Banka).[2]

Public research records by Kroll indicated that the Moldovan shareholders had connections with Moldovan political parties and government institutions, while some of the beneficial owners of the UK-registered companies were reported as being professional nominee directors employed at various Corporate Service Providers. Overall, both individuals and corporate entities had connection with the Moldovan businessman Ilan Shor.[3]

Thereafter, the three banks engaged in a series of lending transactions between each other with 'no apparent economic rationale', facilitated by the use of Scottish Limited Partnerships (20 out of 48 UK corporate entities named in the report). Eventually, the extended and interrelated funding and loan activity within the three banks culminated in a series of events in November 2014 which led to their collapse.[4]

Between 24 and 26 November 2014, a complex series of transactions resulted in new loans of the value of slightly more than $750 million issued by Banca Sociala to Moldovan entities, which then transferred the funds to five UK and Hong Kong-based corporate entities with accounts at Latvia's Privatbank. All five firms had been created in the months leading up to the transactions and had further offshore entities as partners – three were SLPs.[5]

On 26 November 2014, in a shareholder meeting described by the Governor of Moldova's National Bank as "completely fake", the rights to the entire sum owed were transferred to another SLP – Fortuna United LP. [6] From this company, the funds were fraudulently dissipated and disappeared in the offshore maze.

Fortuna United LP was created only months earlier in August 2014 with registered address at 18/2 Royston Mains Street, Edinburgh. Like many SLPs, its partners were corporate entities based offshore, in this instance the Seychelles.[7]

On November 26, the banks went bankrupt and later placed under administration of the National Bank of Moldova. In the meanwhile, orders were given by the management of the banks to archive all the documentation relating to the suspicious transactions with entities connected to Ilan Shor and delete data of these transaction from the databases.[8]

The bank documentation was collected by a van provided by the company Klassica Force SRL. On November 27, the van was stolen and later found burned out. The very same day, the Moldovan government secretly decided to bail out the three banks with $870 million in emergency loans provided by the state's budget. Such a move created a deficit in Moldovan public finances of around 12% of the country's GDP.[9]

Shor was arrested in 2015 on money laundering and embezzlement charges. According to prosecutors, he laundered more than $335 million of the stolen billion. Under arrest, Shor confessed prosecutors about a $250 million bribe he allegedly paid to former Moldova's prime minister Vlad Filat in order to take control of Banca of Economii (one of the three banks involved in the fraud, in which the Moldovan State also had shares).[10]

The authorities investigated the claim and arrested Filat in 2016, sentencing him to 9 years in prison for corruption. Shor also admitted having directed millions of dollars to bank accounts belonging to offshore companies apparently controlled by Veaceslav Platon, one of the minds behind the Global Laundromat scheme.[11]

OCCRP reporters, after having examined various bank records, have found that some of the companies within the Shor Group also received money from the Russian Laundromat. For example, according to RISE Moldova, a OCCRP partner, between 2011 and 2013 six Shor Group companies received a total of $22 million from three shell companies involved in the Russian Laundromat. Other minor transactions between shell companies involved in both frauds were found.[12]

The three Latvian banks involved in the scandal were all issued record fines between 2015 and 2016, while the then head of the Latvian financial regulator handed in his resignations amid criticism for not properly supervising the Latvian banking sector.[13]

---

[1] Kroll (2015), Project Tenor – Scoping Phase, Final Report, available at http://candu.md/files/doc/Kroll_Project%20Tenor_Candu_02.04.15.pdf

[2] ibid. p.9-11

[3] ibid.

[4] ibid p. 11

[5] Transparency International-UK (2017), Offshore in the UK: analysing the use of Scottish Limited Partnerships in corruption and money laundering, p.11, http://www.transparency.org.uk/publications/offshore-in-the-uk/#.Wle69FKB3Vp

[6] http://www.heraldscotland.com/business_hq/13414235.display/

[7] Transparency International-UK (2017), Hiding in Plain Sight: how UK companies are used to launder corrupt wealth, http://www.transparency.org.uk/publications/hiding-in-plain-sight/#.Wj6iTVKZPVr

[8] Kroll (2015), Project Tenor – Scoping Phase, Final Report, http://candu.md/files/doc/Kroll_Project%20Tenor_Candu_02.04.15.pdf

[9] ibid.

[10] OCCRP (2017), 'Two huge scams, one Moldovan businessman', https://www.occrp.org/en/laundromat/two-huge-scams-intersect-at-one-moldovan-businessman/ [accessed 30 October 2017]

[11] ibid.

[12] ibid.

[13] Re:Baltica (2016), 'US pressures Latvia to clean up its non-resident banks', https://en.rebaltica.lv/2016/02/u-s-pressures-latvia-to-clean-up-its-non-resident-banks/ [accessed 30 Oct 2017]

3.3 Loopholes in Latvia's AML supervision in the financial sector

The Latvian financial regulator, the FCMC, carried significant responsibility with regard to Latvia's AML failures, as its supervisory measures were not adequate to the money laundering risks facing Latvian banks. In particular, FCMC's lack of resources did not allow it to carry out sufficient inspections of banks serving non-resident customers to ensure compliance with the AML rules.[129]

Despite the majority of non-resident deposits were accepted through banks' representative branches abroad, the FCMC stated that it had not conducted on-site inspections of these overseas offices over the previous years, considering them unnecessary since representative branches did not make business decisions, but 'merely collected customer identification information'.[130]

In 2012, Council of Europe's MONEYVAL[131] found that foreign branches of Latvian banks were relying on the services of TCSPs, business introducers and agents, in Latvia and abroad, in order to conduct customer identification. Even though reliance on third parties was regulated by the actual Latvian AML Law, according to MONEYVAL, its effectiveness was weakened by some loopholes.[132]

According to MONEYVAL, the AML Law failed to clearly transpose the requirement establishing ultimate responsibility on banks for customer identification and ongoing monitoring of CDD for clients brought in by third parties. Moreover, despite banks were required to immediately obtain CDD documents on new customers brought in by third parties, they needed the customer's consent in order to get them – for reasons of client's data protection. This resulted in a delay or even cancelation of the process. In addition, there was no provision in place about what measures banks should take if consent was not given.[133]

In practice, the parent bank would ask for a letter of introduction from their foreign branches. During on-site visits, banks stated that when they forwarded a request to their parent-company never got a refusal. In practice, financial institutions closed 2-3 *third party-introduced accounts* every week due to insufficient information on the clients. Such decision was taken at different seniority levels within the bank.[134]

Eventually, this turned out to be one of the biggest vulnerabilities of the Latvian banking system. In fact, the majority of anonymous shell companies with Latvian bank accounts involved in illegal activity could be traced back to international company service provider/business introducer structures, sourcing shell companies wholesale in diverse relevant jurisdictions, usually through partnerships with local company service providers acting as "feeder" structures.[135]

The vast array of different regulations across jurisdictions has allowed corrupt networks to use TCSPs across the world to engage in "jurisdictional arbitrage" between different jurisdictions, exploiting loopholes in domestic laws to create thousands of corporate vehicles ensuring anonymity of the ultimate beneficial owners. At the same time, arm-length arrangements between TCSPs and Latvian banks resulted in a "dilution of customer identification duties, which allowed corrupt networks to "bypass" customer identification checks, giving them access to the global financial system.[136]

Apart from scarce supervision, OECD experts expressed significant concerns also with regard to sanctions imposed on the banks for non-compliance with AML regulations, which had been disproportionately small to have

[129] OECD (2015), Phase 2 Report on Implementing the OECD Anti-Bribery Convention in Latvia, p.31, http://www.oecd.org/daf/anti-bribery/Latvia-Phase-2-Report-ENG.pdf
[130] ibid. p.32
[131] MONEYVAL is a monitoring body of the Council of Europe with the task of assessing compliance with AML international standards
[132] MONEYVAL (2012), 'Report on Fourth Assessment Visit – Latvia', pp. 114-116, https://rm.coe.int/report-on-fourth-assessment-visit-anti-money-laundering-and-combating-/1680716b9f
[133] ibid.
[134] ibid.
[135] 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 Issue: 4, pp. 496-512
[136] ibid.

a deterrent effect.[137] For example, following the Magnitsky case, only one unnamed bank out of six allegedly involved was fined €142.000 – the maximum penalty. In 2014, the liability for banks was capped to 10% of the annual turnover, while liability for senior management and bank officers responsible for AML compliance was introduced (they can be now issued fines up to €5 million for failure in carrying out their AML duties).[138] However, in 2014 only one bank was fined €70.000 and no employees or senior managers had been sanctioned since 2010.[139]

The OECD assessment was also critic of the Suspicious Transaction Reporting System, pointing out that the number of STRs forwarded by the FIU to law enforcement authorities was too low. As a probable reason, the OECD indicated the lack of resources and personnel within the KD – not adequate to cope with the high level of financial activity involving Latvia and the high number of STRs sent by banks.[140] The OECD also pointed out the scarce level of prosecutions and convictions for money laundering underlining the necessity of improving investigative and prosecution authorities' capacity against money laundering crimes.[141] In fact, despite money laundering cases amounting to more than $20 billion in the previous years, none of the criminal procedures commenced in Latvia had resulted in a conviction.[142]

3.4 Mitigation of money laundering risks in the banking sector

Prompted by international criticism and media exposure about the large-scale money laundering cases, since the beginning of 2016 Latvian authorities have taken steps to put a remedy to the anti-money laundering failures of Latvian banks, with the Latvian financial regulator carrying out a number of significant measures aimed at mitigating money laundering risks, strengthening the AML regulatory framework and re-orient Latvian banks towards a different and more sustainable business model.

Capacity building, strengthened supervision and increased sanctions

In 2016, FCMC's staff and resources were increased, resulting in a strengthened supervisory capacity. A new structural unit, the **Compliance Control Department (CCD)**, was set up with the task of performing regular and targeted supervision of Financial Institutions' internal AML systems, carrying out money laundering risk assessment and developing regulatory framework accordingly, and ensuring banks' compliance with international and European regulations as well as international sanctions requirements.[143] Officers within the Compliance

[137] OECD (2015), Phase 2 Report on Implementing the OECD Anti-Bribery Convention in Latvia, p. 32, http://www.oecd.org/daf/anti-bribery/Latvia-Phase-2-Report-ENG.pdf
[138] ibid.
[139] ibid.
[140] ibid. p.31
[141] ibid. p.63
[142] Re:Baltica (2016), 'US pressures Latvia to clean up its non-resident banks', https://en.rebaltica.lv/2016/02/u-s-pressures-latvia-to-clean-up-its-non-resident-banks/ [accessed 30 Oct 2017]
[143] Latvian National Money Laundering/Terrorism Financing Risk Assessment Report (2017), pp.56-57, available at: http://www.kd.gov.lv/images/Downloads/useful/ML_TF_ENG_FINAL.pdf

Control Department increased almost four-fold – from 5 to 18 – in the course of 2016 and a further increase of employees is set to take place in the coming years.

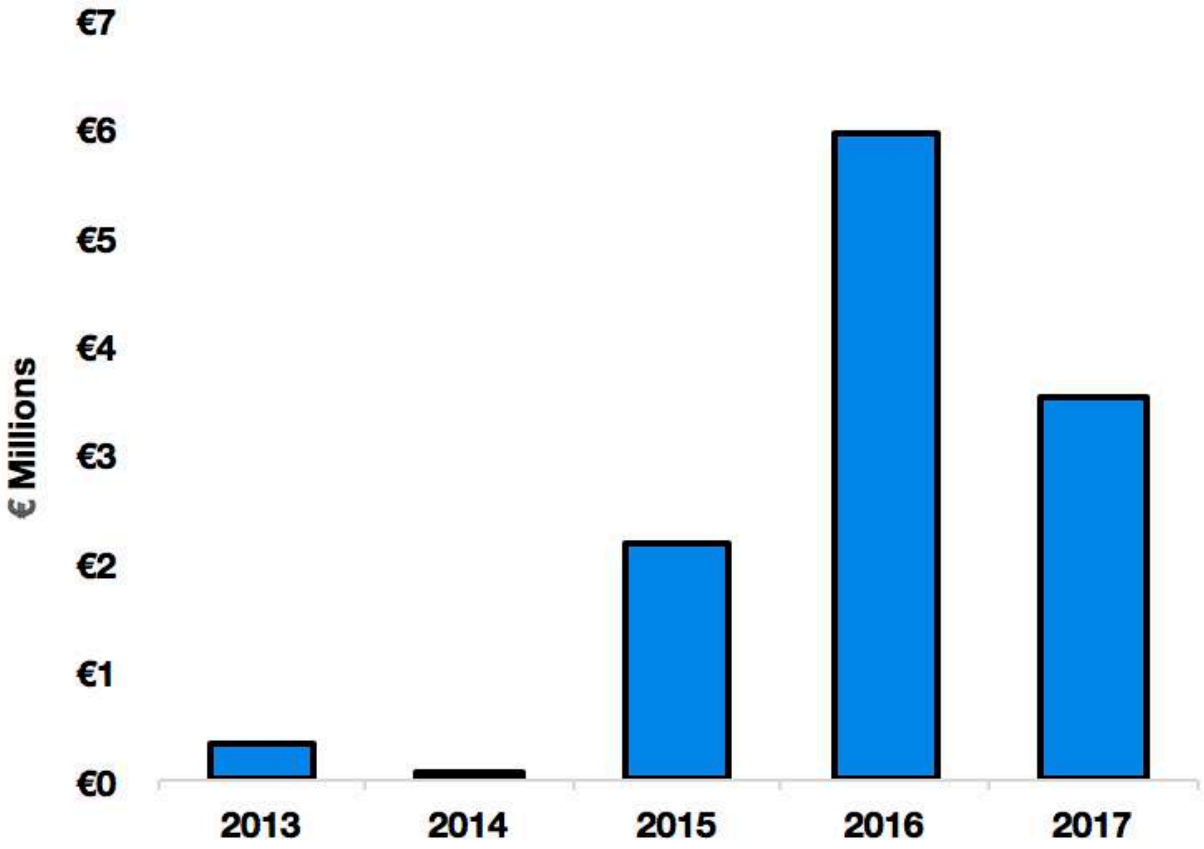
As a result of this capacity building, AML supervision of banks significantly increased, with a special focus on on-site inspections of banks servicing foreign customers, which nearly doubled from 17 in 2015 to 30 in 2016. This included a series of targeted inspections of banks which according to information reported by media had allegedly been involved in money laundering, which led to an unprecedented issuing of administrative fines.[144] Whereas the total amount of administrative penalties for AML failures in the period 2013-2014 was around €400.000, this figure increased by around 20 times in the period 2015-2016 (around €2.2 millions).

In 2015, for the first time, the FCMC issued fines to bank management for their responsibility in AML failures, for a total amount of €145.000. The peak in sanctions was reached in 2016, when the amounts of fines reached almost €6 million. Moreover, in the same year, one bank (Trasta Komercbanka) saw its license being revoked due to severe deficiencies in its AML system. In 2017, administrative penalties amounted to around €3.5 million and were issued in relations to banks' failure to prevent circumvention of international sanctions by North Korea-linked entities and intermediaries.[145]

According to the 2017 National Money Laundering Risk Assessment, banks' level of awareness regarding sanctions for AML non-compliance has increased in the last three years, and banking sector's representatives believe that sanctions have been severe enough to prompt improvement of their AML Internal Control Systems.[146]

Chart 4 – Sanctions for AML breaches issued on Latvian banks by the FCMC, 2013-2017

Source: Financial and Capital Market Commission (FCMC)



[144] ibid. p.57
[145] http://www.fktk.lv/en/market/credit-institutions/2014-10-23-sanctions-imposed-by-fcmc.html
[146] Latvian National Money Laundering/Terrorism Financing Risk Assessment Report (2017), pp.58, available at: http://www.kd.gov.lv/images/Downloads/useful/ML_TF_ENG_FINAL.pdf

Independent external audits and de-risking process

In the course of 2016, the FCMC commissioned and coordinated the performing of external audits by three independent consultants from the United States in 11 Latvian banks.[147] These were aimed at reviewing their compliance with AML laws and regulations as well as the effectivity of their Internal Control and risk management systems, were carried following FCMC's methodology and procedures for ongoing supervision of AML compliance.[148]

All 11 banks received the results of the audits at the end of 2016, and were tasked with developing remediation plans for addressing the deficiencies identified in the course of the assessment. Internal reforms are to be implemented by the end of 2017/first quarter of 2018, and encompass internal control systems, risk management, corporate governance, and training of bank officers and senior management. According to new regulation issued by the FCMC in 2016, banks have now the obligation to subject their Internal Control Systems to external independent audits at least once every 18 months.[149]

The independent assessment process has also entailed a significant process of de-risking among banks clients. About 19.000 high-risk clients have seen their bank accounts closed in 2016 alone, compared to around 11.200 clients de-risked in 2015 (a 39% increase).[150]

The Latvian financial regulator has also recognized the money laundering risks related to banks' collaboration with third parties such as Trust and Corporate Service Providers and agents for customer identification purposes and on-boarding of new clients. As such, it has strengthened regulation in this regard, according to which banks must conduct risk assessment before engaging in a collaboration with third parties, they must conduct Enhanced Due Diligence on clients brought in by agents and ensure that the latter conduct EDD and are aware of their AML responsibilities.[151]

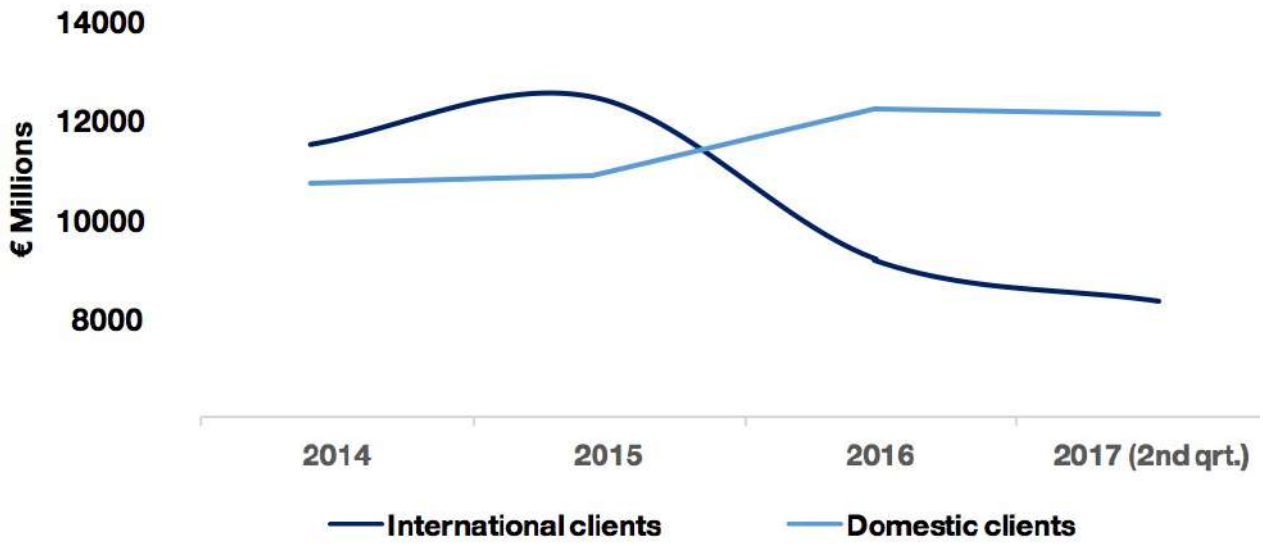
[147] ABLV, Baltic International Bank, BlueOrange, Citadele banka, Norvik banka, Privatbank, RigensisBank, Expobank, Bank M2M, Regionala Investiciju Banka, Meridian Trade Bank
[148] Latvian National Money Laundering/Terrorism Financing Risk Assessment Report (2017), pp.57-58, available at: http://www.kd.gov.lv/images/Downloads/useful/ML_TF_ENG_FINAL.pdf
[149] ibid.
[150] Association of Latvian Commercial Banks (ALCB), Compliance Status Review, September 2017, http://lka.org.lv/en/compliance/
[151] Financial and Capital Market Commission (FCMC), Regulation No.196/2016, Regulations for Cooperation with Third Parties and Requirements for Business Relations with the Customers whose Identification or Due Diligence is Performed Using Third Party's Services, http://www.fktk.lv/en/law/credit-institutions/fcmc-regulations.html

Decrease of non-resident deposits and the need for strengthened regulation and supervision in the TCSP sector

The new AML regulatory framework introduced in Latvia in 2015-2016 and the de-risking process have caused a sharp decline in the proportion of foreign customers' deposits in Latvian banks. Non-resident deposits decreased by 26% in 2016 alone, while the overall proportion decreased from 53.4% in 2015 to 42.8% in 2016 to 41.1% in 2017. [152]

Chart 5 – Amount of resident and non-resident deposits in Latvian banks (€ millions), 2014-2017

Source: Association of Latvian Commercial Banks (ALCB)



This indicates the effectivity of the reform, and a partial reorientation of Latvian banks' business model towards domestic clients. Moreover, as banks implement remediation plans following the independent external audits, the risk coming from non-resident deposits is expected to further decrease.

However, whereas Latvian authorities took significant steps to mitigate money laundering risks in the financial sector, including the reliance on the services of TCSPs, the 2017 Latvian National Money Laundering Risk Assessment (NRA) found a number of vulnerabilities with regard to the TCSP sector in Latvia itself, demonstrating that the money laundering risk posed by these agents has remained high in recent years. These have been mainly related to insufficient capacity of the supervisory and control authorities, absence of entry controls and licensing, and a lack of understanding of money laundering regulations by part of the firms operating in the sector.[153]

This, however, has not been a problem exclusively affecting Latvia, as supervision and regulation of TCSPs has been found to be lacking across many other jurisdictions, in the EU and beyond. While over the years extensive anti-money laundering responsibilities have been applied to banks, they have not extended to all professional intermediaries that act as gatekeepers to the financial system. This has left significant professional sectors with almost no deterrents against working as enablers for corrupt networks.[154]

[152] Association of Latvian Commercial Banks (ALCB) (2017), 'Compliance Status Review, September 2017', http://lka.org.lv/en/compliance/
[153] Latvian National Money Laundering/Terrorism Financing Risk Assessment Report (2017), pp.86-87, available at: http://www.kd.gov.lv/images/Downloads/useful/ML_TF_ENG_FINAL.pdf
[154] Judah B. & Li B., Kleptocracy Initiative (2017), 'Money Laundering for 21st Century Authoritarianism: Western Enablement of Kleptocracy', Hudson Institute

4. Trust and Company Service Providers and money laundering in Latvia

The FATF, as well as banking supervisors across the world, have long acknowledged that inclusion of Trust and Company Service Providers in the regulatory net is important to mitigation of money laundering risks in financial services. However, this has been hampered by significant restrictions in the flow of information related to the industry.[155] These have mainly derived from a lack of universally accepted and understood definition of what constitutes trust and corporate services as well as from the very diverse range of regulatory controls and oversights on these entities across different jurisdictions, many of them weak or ineffective. As a consequence, the TCSP industry has seen not only the proliferation of firms and agents with low level of expertise, knowledge or understanding of key AML matters, but also the presence of persons willing to get involved in criminal activities, and the laundering of their proceeds.[156]

Concerning Latvia, already in 2012 MONEYVAL observed that regulation, supervision and enforcement of money laundering regulations in place were not sufficient to cope with the high money laundering risk posed by the TCSP sector in Latvia, which in that year encompassed around 5.000 firms and individuals, including professionals such as legal service providers, tax advisors and external accountants.[157]

As pointed out by MONEYVAL, the State Revenue Service (SRS) – the designated supervisor for these entities – did not even have a department focused on AML compliance supervision. MONEYVAL also observed a lack of understanding in the sector of the requirements concerning CDD and EDD procedures on high-risk countries and politically-exposed persons, as well as insufficient development of AML Internal Control Systems in general.[158]

This was confirmed when, in 2012, a group of academics conducted an experiment to examine whether international rules on the collection of beneficial ownership information by TCSPs were being implemented in practice. Posing as high-risk customers – including would-be money launderers, corrupt officials and terrorist financiers – the research team emailed 3,700 different TCSPs in 182 countries asking to set up anonymous shell companies that would help mask their identities.[159]

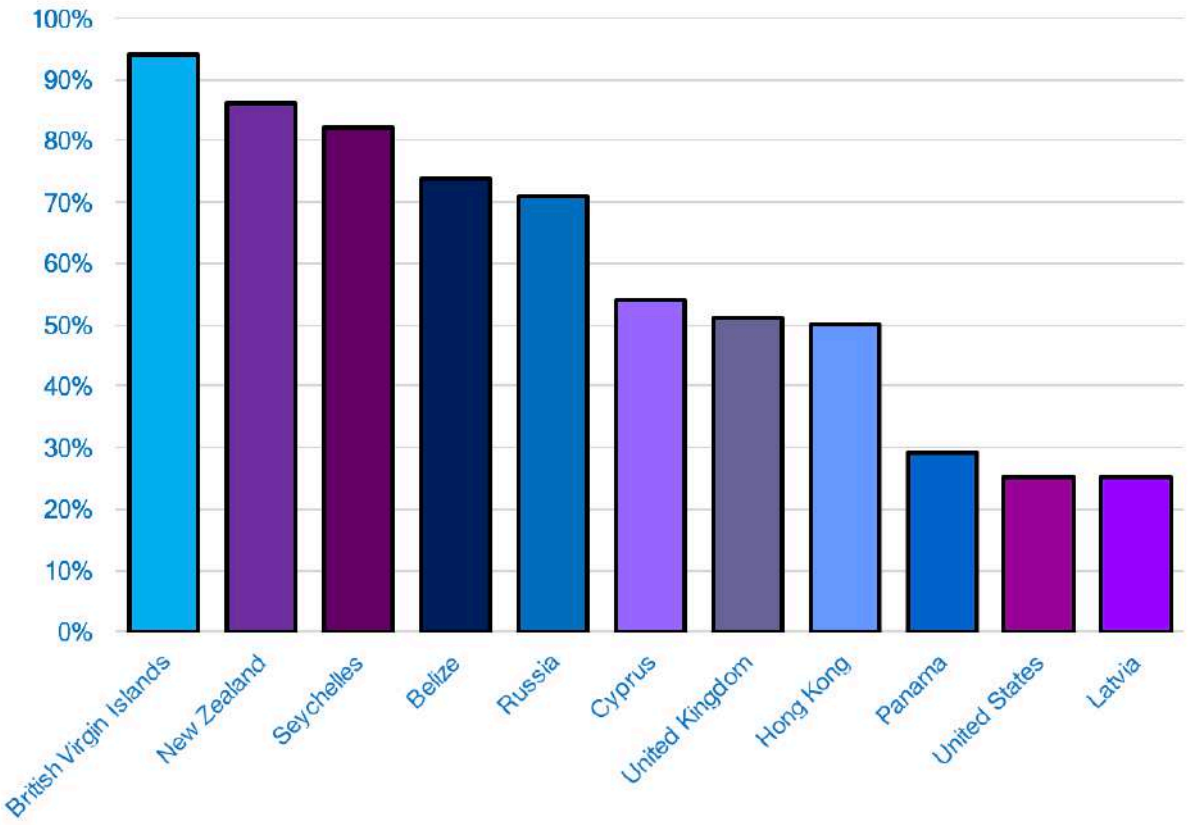
The experiment found that nearly half (48%) of all replies received did not ask for proper identification, and 22% did not ask for any identity document at all to form a shell company. Against the expectations, those selling shell companies from secrecy jurisdictions were significantly more likely to comply with the rules than providers in

[155] FATF (2010), 'Money Laundering Using Trust and Company Service Providers', http://www.fatf-gafi.org/media/fatf/documents/reports/Money%20Laundering%20Using%20Trust%20and%20Company%20Service%20Providers..pdf
[156] ibid.
[157] MONEYVAL (2012), Report on Fourth Assessment Visit – Latvia, pp.26-27, https://rm.coe.int/report-on-fourth-assessment-visit-summary-anti-money-laundering-and-co/1680716ba1
[158] ibid. pp.12 & 207
[159] Findley M. et al. (2012), *Global Shell Games: Testing Money Launderers' and Terrorist Financiers' Access to Shell Companies*, http://www.michael-findley.com/uploads/2/0/4/5/20455799/oct2012-global-shell-games.media-summary.10oct12.pdf

OECD countries like the US and the UK.[160] The experiment found that the compliance rate of TCSPs operating in Latvia was just 25%, one of the lowest among the countries where the study was conducted.[161]

Chart 6 – Compliance rate of TCSPs in Latvia and other 10 jurisdictions in the Global Shell Games study, 2012

Source: Findley M. et al. (2012), Global Shell Games: Testing Money Launderers' and Terrorist Financiers' Access to Shell Companies



As of today, there is large evidence that a number of Latvia-based TCSPs – wittingly and unwittingly – favoured the creation of shell companies for corrupt networks while at the same time giving them access to the financial system, by establishing loose partnerships and implicit cooperation with some of the leading Latvian banks servicing customers across Eurasia.

For example, journalist investigations found that behind the incorporation of the bulk of shell companies used to carry out the Magnitsky affair, the laundering of drug profit from the Mexican cartel Sinaloa and other crimes related to the same platform there was one of the largest and oldest network of offshore service providers with ties to some of the leading Latvian offshore banks. This dated back to the first decade of the 1990s and had perhaps as much as 25% share in the shell company incorporation business.[162]

According to the German intelligence service Scalaris, the network was centred in the Baltics and encompassed Ukraine, Moldova, Russia as well as the UK and Cyprus, and it appeared to operate across different jurisdictions either through subsidiaries or through partnerships with local TCSPs as well as with affiliated Latvian banks.[163]

[160] ibid.
[161] http://www.globalshellgames.com/results--maps.html
[162] 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 Issue: 4, pp. 496-512
[163] Galli A. (2012), 'Erik Vanagels – The Extent of a Money Laundering Supermarket', Scalaris

Criminal groups across the former Soviet Union and beyond would utilise the shell companies provided by the offshore group, with accounts in Latvian banks, to either move the illicit funds across the global financial system or to stash them offshore. The anonymity of those behind the shell companies was ensured by the use of Latvian nominee directors and shareholders - some of them victims of identity theft.[164]

Part of this network were also other Latvia-linked company service providers, which appeared to be opaque and flimsy, run by either one person or a small group of individuals, and often owned by companies in secrecy jurisdictions veiling the beneficiaries.[165] In 2013, the International Consortium of Investigative Journalist obtained and made available online a leaked database containing confidential information on over 100,000 offshore shell companies, trusts and other corporate entities, which indicated that a number of New Zealand companies used in the money laundering schemes was sourced from a TCSP based in the South Sea by other two TCSPs based in Riga and the Seychelles, both owned by a Latvian citizen. The data also showed that the same TCSPs were responsible for the creation of nearly 1.500 companies in the British Virgin Islands, all featuring the same nominee director.[166]

[164] Kegö W. & Georgieff A. (2013), 'The Threat of Russian Criminal Money: Reassessing EU Anti-Money Laundering Policy', p.29-30 Stockholm: Institute for Security and Development Policy
[165] 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 Issue: 4, pp. 496-512
[166] Bne Intellinews (2013), 'Career of shell-company creator points to banks as culprits', http://www.intellinews.com/career-of-shell-company-creator-points-to-banks-as-culprits-500017931/?source=russia&archive=bne [accessed 30 October 2017]

4.1 The Panama Papers Database

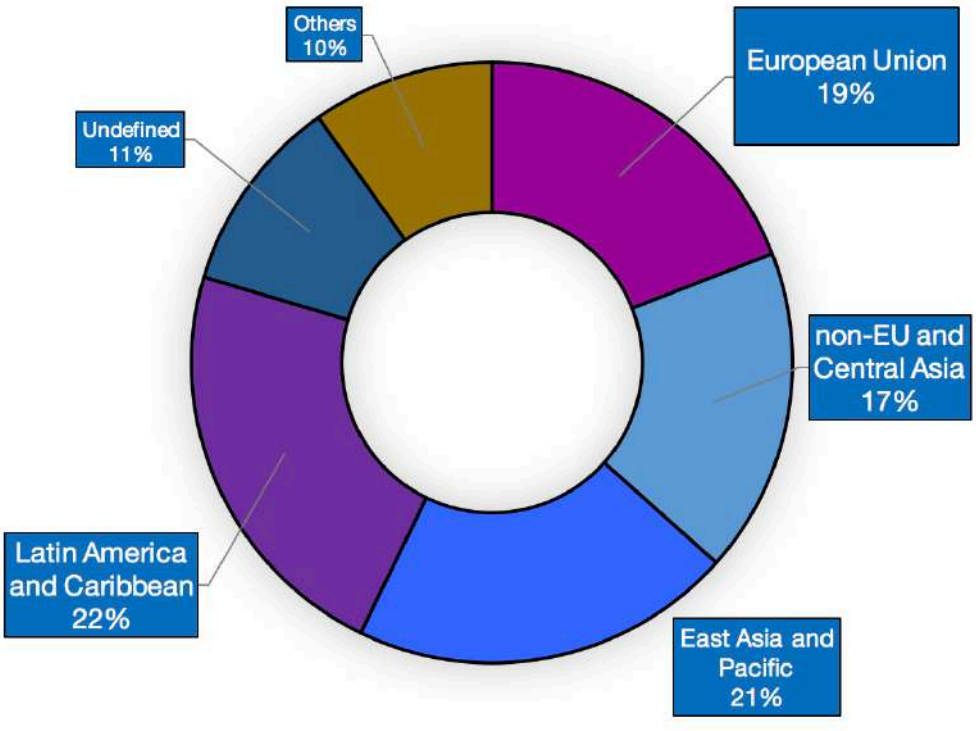
The Panama Papers in 2016 confirmed the scarce compliance with AML rules by TCSPs around the world and many of the loopholes in the global supervision of these entities, already identified by the FATF and other international bodies. The investigations documented a systematic use of illegal practices such as backdating documents and revealed a blatant disregard of basic customer due diligence duties. In some cases, TCSPs even maintained business relations with companies whose nominee directors had been dead for several years). Evidence was also found of banks outsourcing CDD duties to intermediaries identified in the database and to Mossack Fonseca. In several cases, the process was not compliant. [167]

Overall, Latvia's name was associated with 2,951 of the 213,634 offshore legal entities identified in the leak (4th highest number in the EU, after UK, Luxembourg and Cyprus), 162 private individuals, 18 intermediaries and 153 addresses.[168] Despite being in small number, Latvian intermediaries were responsible for at least 1,373 entities, the 5th highest number among EU member states after Luxembourg, the UK, Cyprus and Czech Republic. Almost 90% entities identified in the Panama Papers database were incorporated in just four jurisdictions: BVIs, Panama, Seychelles and Bahamas, with the BVI taking the largest share.[169] As observed above, entities from these jurisdictions together made up 34% of non-resident deposits in Latvian banks in 2011.

The entities present in the leaked database were fed to Mossack Fonseca's predominantly from 14,074 intermediaries, of which 2,696 (19.1%) based in the EU; 2,476 (17,5%) based in non-EU European and Central Asian countries; 2,901 (20.6%) in East Asia and Pacific; and 3.159 (22.4%) in Latin America, Caribbean.[170] This indicates a relatively equal distribution of professional intermediaries cooperating with Mossack Fonseca across the globe. Within the EU, the great majority of intermediaries were found to be in the UK, followed by Luxembourg and Cyprus.

Chart 7 – Location of intermediaries identified in the Panama Papers, 2016

Source: De Groen W.P. (2017), 'Role of advisors and intermediaries in the schemes revealed in the Panama Papers', study commissioned by the PANA Committee of the European Parliament



[167] European Parliament's PANA Committee (2017), Draft report on the inquiry on money laundering, tax avoidance and tax evasion (2017/2013), http://www.europarl.europa.eu/cmsdata/122787/2017-06-30%20Draft%20report.pdf
[168] Lsm.lv (2016), 'Two Latvian officials mentioned in the Panama Papers', http://eng.lsm.lv/article/society/society/two-latvian-officials-mentioned-in-panama-papers.a195785/ [accessed 17 December 2017]
[169] De Groen W.P. (2017), 'Role of advisors and intermediaries in the schemes revealed in the Panama Papers', study commissioned by the PANA Committee of the European Parliament
[170] ibid.

Intermediaries located in the European Union were responsible for 19% of the entities, while intermediaries from non-EU European and Central Asian countries took the largest share (33%), Overall, 2,476 intermediaries from this group of countries where responsible for over 70,704 entities, of which 12,484 of were still active when the data were leaked in 2015. Amongst all intermediaries, Mossack Fonseca had a market share of approximately 5-10% offshore entities and incorporated entities across 21 jurisdictions. [171]

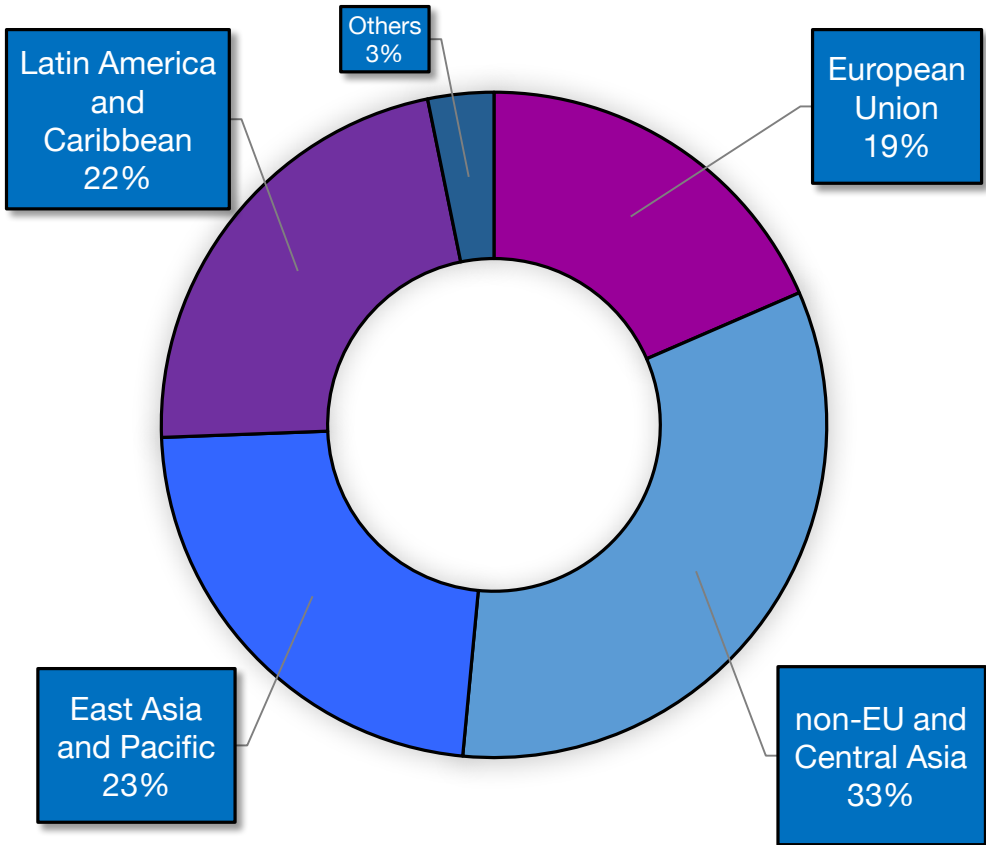


Chart 8 – Percentage of total corporate vehicles identified in the Panama Papers, divided by location of intermediaries responsible for them

Source: De Groen W.P. (2017), 'Role of advisors and intermediaries in the schemes revealed in the Panama Papers', study commissioned by the PANA Committee of the European Parliament

Mossack Fonseca also operated a branch in Riga from 2009 until December 2015, in association with its British subsidiary RM. Though the two firms used a joint name, they had been registered separately from 2009, with a UK citizen listed as owner of both. Two Latvian individuals were found to also own shares in the RM Group Mossack Fonseca Office. It is not clear yet under which circumstances the Mossack Fonseca's Riga branch shut down its activities in Latvia in 2015. Concerning RM, company records only show that the State Revenue Service took a decision to suspend its activities in February 2016.[172]

Despite Latvia's central role in these revelations, there has been little follow-up action by authorities in the form of investigations and prosecutions. According to the Latvian FIU, this was due to a number of reasons. Latvian authorities faced a number of challenges with regard to the processing of personal data, such as lack of basic information, differences in spelling of different languages and outdated information.[173]

[171] ibid.
[172] Lsm.lv (2016), 'Latvia braced for Panama leak info', http://eng.lsm.lv/article/society/society/latvia-braced-for-panama-leak-info.a176426/ [accessed 20 December 2017]
[173] Latvian Ministry of Finance, Information provided to the European Parliament's PANA Committee in the framework of the inquiry on the revelations of the Panama Papers

It has been particularly difficult for authorities in onshore jurisdictions to obtain information on offshore entities through TCSPs, because they often do not have a physical presence in the jurisdiction of the beneficial owner, nor in the jurisdiction of the offshore entities.[174] For example, among the EU entities owned by private persons in the Panama Papers, less than 10% of their ultimate beneficial owners used an intermediary in their home country; another 50% used an intermediary in another EU member state and the remaining 40% used an intermediary in a third country, suggesting that many cases were not covered by legislative requirements.[175]

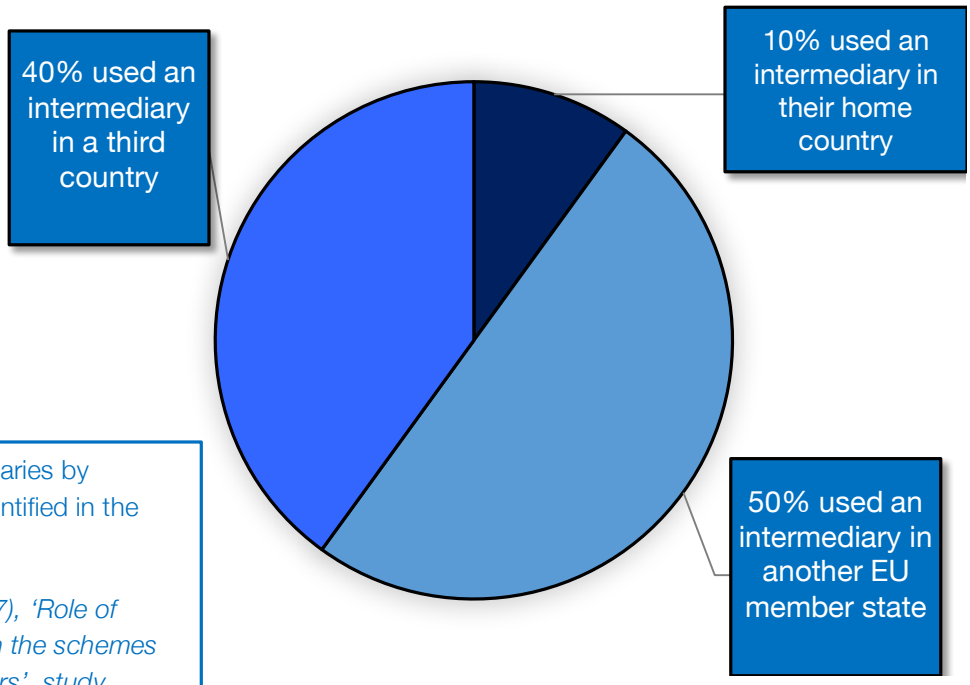


Chart 9 – Usage of intermediaries by ultimate beneficial owners identified in the Panama Papers

Source: De Groen W.P. (2017), 'Role of advisors and intermediaries in the schemes revealed in the Panama Papers', study commissioned by the PANA Committee of the European Parliament

The Panama Papers' database has so far greatly helped to analyse and understand the structure of the offshore financial industry, but some reservations should be made. The leak provided information from only one offshore intermediary that established almost exclusively entities in a small number of offshore jurisdictions. In general, the exact size of the market for offshore structures is still unknown.[176] This indicates the need for strengthened oversight of TCSPs, at the domestic and international level. However, the inherently transnational character of the sector has made the challenge particularly daunting.

A tailored approach to supervision of TCSPs may be more attractive for many jurisdictions, but variations in the approach to defining the sector may also result in a confusing array of laws governing an international industry that is becoming increasingly more globalised, as online incorporation services make it extremely cheap and easy to incorporate from anywhere around the world.[177]

On the other hand, international standards would help to harmonise performance and assessment criteria for TCSPs and, in time, would help close the loopholes and eliminate the opportunities for legal arbitrage. However, this has been problematic, as implementation of standards at the global level has been found to be lacking by the 2016 FATF report to the G20.[178]

[174] De Groen W.P. (2017), 'Role of advisors and intermediaries in the schemes revealed in the Panama Papers', p.34, study commissioned by the PANA Committee of the European Parliament
[175] ibid. p.39
[176] ibid. p.10
[177] FATF (2010), 'Money Laundering Using Trust and Company Service Providers', p.16, available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Money%20Laundering%20Using%20Trust%20and%20Company%20Service%20Providers..pdf
[178] FATF (2016). Report to the G20: Beneficial Ownership (September 2016), http://www.fatf-gafi.org/media/fatf/documents/reports/G20-Beneficial-Ownership-Sept-2016.pdf

4.2 Persistence of the money laundering risk posed by TCSPs operating from Latvia

The 2017 NRA has found a number of vulnerabilities in the TCSP sector in Latvia, due to which the ML risk related to the activities of these firms has remained high in recent years.

Lack of resources

Following MONEYVAL recommendations, at the end of 2012 the Anti-Money Laundering Division of the Tax Control Department of the State Revenue Service was set up with the task of carrying out supervision of AML compliance in the TCSP sector. However, according to the 2017 NRA, this failed to have a significant impact.[179]

As mentioned above, in 2012 MONEYVAL identified around 5.000 TCSP firms operating in Latvia, including legal service providers, tax advisors and external accountants. However, despite the relatively high number of entities, the number of appointed supervisors within the State Revenue Service had remained low up to the end of 2016. Only three officers within the AML department were respectively in charge of supervising tax advisors and external accountants. With regard to legal service providers, up to 2015 the number of employees supervising these entities was only three, and in 2016 it was even reduced to two.[180]

The absence of any focused risk-assessment by part of the SRS and the FIU has not allowed to have a clear overview of the activities in the sector, identify the most sensitive areas of risk and intervene accordingly.[181] This was exacerbated by the fact that, according to the division of functions among SRS' units, only the Tax Control Department carried out on-site inspections of TCSP firms, while the AML Department mostly conducted off-site supervsion. This meant that on-site inspections were more focused on tax evasion risks rather than money laundering, thus preventing the SRS from gaining a full picture on the actual existence and/or effectiveness of AML Internal Control Systems, and whether and how information about customers and transactions has been stored.[182]

Ineffective sanctions

According to the Latvian Administrative Violations Code, the SRS is entitled to impose administrative sanctions on TCSP firms for non-compliance in the AML area. Up to November 2017, the maximum applicable administrative penalty for not following AML requirements amounted to €700, while the applicable penalty for not submitting STRs had been increased to up to €5.000 (or 5% of net turnover for those entities whose annual profit are more than €1 million) in early 2017.[183] The administrative penalties were further increased in late 2017, when Latvia adopted the new AML law, which will be discussed later below.

In practice, in the years 2013-2016 sanctions on TCSP firms were too ineffective and disproportional to have a relevant impact. Due to the structure of SRS' supervisory departments, the SRS often received information on non-compliance too late, and this prevented it from responding in a timely and effective manner.[184] Available data show that from 2013 to 2016, TCSP entities were found in breach of the law only 20 times, and the total amount of sanctions imposed was of around €1.650 (€1.200 on legal service providers and €445 on tax advisors and external accountants together).[185]

Moreover, the SRS could not identify a positive effect of the application of sanctions on TCSPs' attitude towards AML regulations, nor did it collect information on the types of applied administrative penalties and the identity of

[179] Latvian National Money Laundering/Terrorism Financing Risk Assessment Report (2017), pp. 86-87, http://www.kd.gov.lv/images/Downloads/useful/ML_TF_ENG_FINAL.pdf
[180] ibid. p.134
[181] ibid. p.87
[182] ibid.
[183] ibid. p.16
[184] ibid. p.87
[185] ibid. pp.134-135

firms or persons fined. As a result, statistics on applied disciplinary measures on the most common violations were not available,[186] thus preventing a targeted approach on the most sensitive areas.

Lack of understanding of AML rules

The 2012 MONEYVAL report indicated a lack of understanding of ML risks and low compliance with AML rules by part of TCSP entities in Latvia, confirmed by the Global Shell Games study in the same year. Since then, the SRS has taken steps to tackle the problem, including a survey to assess the level of understanding of AML regulations, an increase in the number of voluntary AML trainings and the provision of general advice on AML matters and the publication of AML guidance and educational material on SRS' website.[187]

In a survey conducted in the framework of the NRA, a large number of respondents pointed out that they had developed AML procedures and Internal Control Systems allowing them to timely review potentially suspicious transactions. However, the very low number of transactions reported by legal service providers and practically missing transactions reported by tax advisors and external accountants indicate that these measures have not been sufficient and have so far failed to have a relevant impact.[188]

Despite the overall estimated number of obliged entities in the TCSP sector in Latvia in 2012 was estimated to be relatively high at 5.000, the total number of STRs submitted to the FIU in the period 2013-2016 was just 168, with only 11 reports forwarded to law enforcement authorities for further investigation.[189] Out of 168 STRs, 123 (73%) was submitted only by legal services providers back in 2013-2014. Within the four years covered by the NRA, tax advisors submitted only 24 reports (70% of which only in 2013), while external accountants submitted only one report in 2016 and none in the previous years.

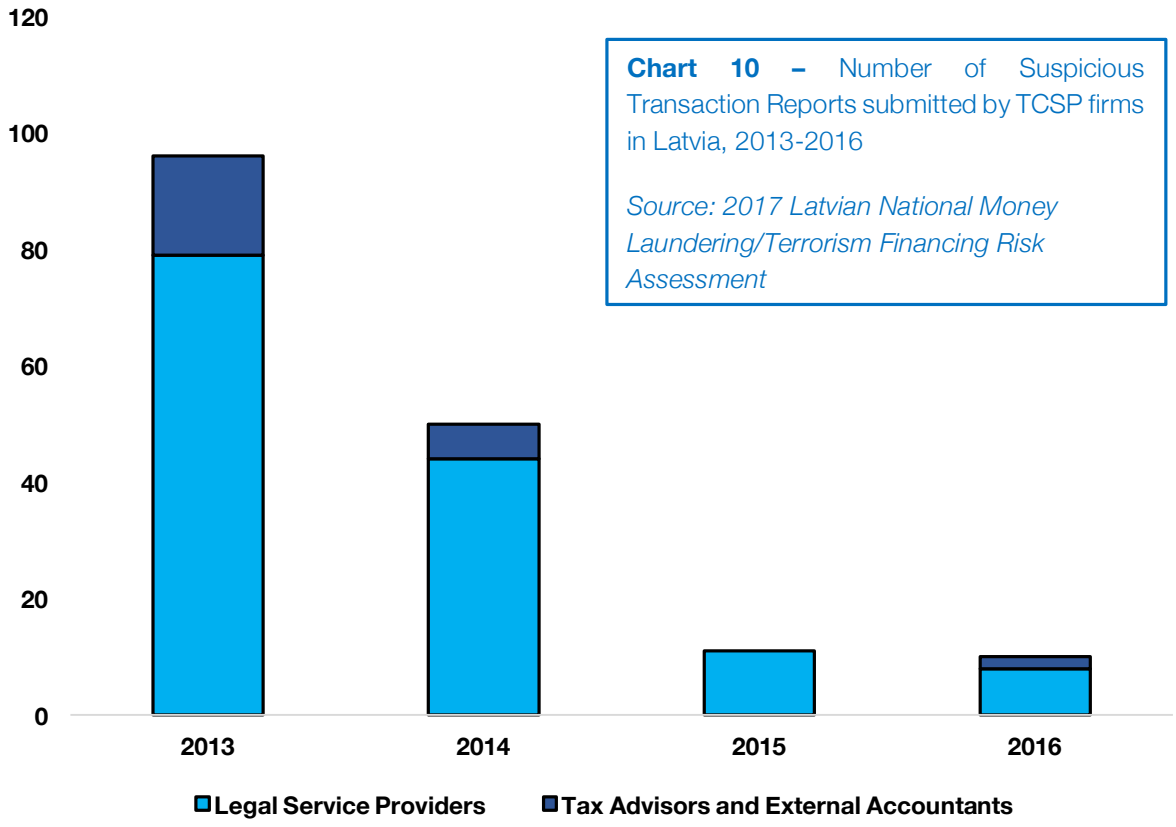


Chart 10 – Number of Suspicious Transaction Reports submitted by TCSP firms in Latvia, 2013-2016

Source: 2017 Latvian National Money Laundering/Terrorism Financing Risk Assessment

[186] ibid. p.88
[187] ibid. p.92
[188] ibid. p.94-95
[189] ibid. p.138

The fact that reports submitted by legal service providers steadily decreased from 79 in 2013 to just 8 in 2016 also should raise alarms in competent authorities. The number of submitted and forwarded reports, although still expected to be lower than that of financial institutions due to the different nature of business, has been clearly not adequate and excessively low in respect to the risk posed by these actors with regard to money laundering. This indicates a strong need to ensure that individuals and firms are aware of their obligations under ML law before starting to operate in the sector and their AML knowledge is fostered over time with regular and comprehensive trainings.

Absence of regulation and licensing

At present, in Latvia there are no licensing requirements for firms and individuals providing TCSP services, nor any mandatory control of their compliance with AML regulations. In the 2017 NRA, the SRS indicated that it did not have sufficient capacity to ensure that firms have a proper knowledge of AML rules before starting operating, nor to prevent persons engaged in criminal activities from owning and controlling these businesses. This has considerably increased the money laundering risk surrounding TCSPs in Latvia and their activities.[190]

Irregularity of trainings

According to the Latvian NRA, given that participation in trainings organized by the SRS has not been compulsory for TCSPs operating in Latvia, it has been impossible to ensure that all firms were properly educated on AML matters. In responses provided to a SRS survey, the majority of firms indicated they carried out trainings for their employees in the AML area, who have increased their knowledge over time.[191] However, this should be taken very critically, since, as noted above, the SRS could not get a clear overview of the development of ICSs and the number of STRs has been extremely low.

Following on-site inspections, which included AML checks, the Tax Control Department of the SRS concluded that the majority of supervised entities were compliant with the AML regulations. However, according to the NRA, given that the focus of supervision had been on tax evasion risks rather than anti-money laundering, this information is partially reliable.[192]

***

As shown by the 2017 NRA, unsupervised TCSP firms still represent a relevant threat to the resilience of the Latvian AML system. This, however, is not only due to vulnerabilities in Latvia's domestic AML framework. The challenge is made harder by the inherently transnational character of the operations of these firms, and the confusion resulting from the vast array of different laws regulating their activities across different jurisdictions. This makes it difficult for authorities to control unscrupulous TCSPs, who may incorporate companies in a determinate jurisdiction, under the laws of that jurisdiction, but do so by operating from another jurisdiction, possibly with weak supervision by part of authorities there.

The money laundering risk related to the activities of TCSPs has been particularly evident also in the UK and Cyprus, where most of the intermediaries identified in the Panama Papers were located. As seen above, both these countries were often mentioned in connection with large-scale money laundering scandals involving Latvian banks. These connections may have been made considerably more complex by the intersections with the TCSP sector among the three

[190] ibid. p.94
[191] ibid. p.92
[192] ibid. p.95

4.3 Trade of British shell companies

As seen above, British shell companies were used in all the major money laundering schemes involving Latvian banks and are still considered one of the main money laundering threats to the Latvian financial system. The ease and speed of setting up a company in the UK has meant that the creation and sale of UK corporate vehicles has become a global industry for TCSPs across the world.[193] According to figures provided by the British Companies House to TI-UK, while 39% of the over 640.000 companies registered in the UK between 2016 and 2017 were formed directly through Companies House – which according to TI-UK does not have enough power and resources to ensure the integrity of the customers[194] - the remaining 61% were formed by TCSPs operating in the UK and abroad. As TCSPs operating outside the UK are able to form UK companies and provide additional services for these without actually being located in the UK, Companies House was unable to distinguish between UK and overseas-based incorporation agents.[195]

TCSPs operating from Latvia are also among them. In their websites, apart from UK corporate vehicles and the benefits they can offer, they advertise company formation across a range of jurisdictions (pictures 1 and 2).[196]

Company Formation *(Incorporation and first annual fees)*

Belize	from 890 USD
Seychelles	from 950 USD
Anguilla	from 950 USD
Dominica	from 1,250 USD
British Virgin Islands (BVI)	from 1,290 USD
Marshall Islands	from 1,390 USD
Samoa	from 1,390 USD
Panama	from 1,490 USD
Latvia	from 1,550 USD
Bahamas	from 1,790 USD
St. Kitts and Nevis	from 1,790 USD
Hong Kong	from 1,990 USD
Gibraltar	from 2,580 USD
Dubai (RAK IBC)	from 3,290 USD
Scotland	3,990 USD
Cayman Islands	from 5,300 USD
Liechtenstein	from 5,490 USD
Switzerland	from 5,490 USD
Jersey	from 5,900 USD
Dubai (RAK Freezone)	from 7,500 USD

Picture 1 – Trust and company service provider offering incorporation of companies across different jurisdictions

THE UNITED KINGDOM - a good international image and convenient corporate & tax planning tools. LTD, LLP, LP from € 750. Read more...

UK company formation

A company in Great Britain may be registered in one of the following legal forms:

- **Private company limited by shares, LTD**
- **English limited liability partnership, LLP**
- **English limited partnership, LP**
- **Scottish limited partnership, LP**

Picture 2 – Trust and company service provider offering incorporation of companies in the United Kingdom

[193] Transparency International-UK (2017), Hiding in Plain Sight: how UK companies are used to launder corrupt wealth, p.11, http://www.transparency.org.uk/publications/hiding-in-plain-sight/#.Wj6iTVKZPVr
[194] ibid. p.2
[195] ibid. p.19
[196] Picture1: http://gws-offshore.com/fee-schedule-2/ [last accessed 14 January 2017]; Picture 2: http://www.uniwide.biz/uk-company-formation/ [last accessed 14 January 2017]. Transparency International Latvia is making no allegation of non-compliance with AML rules against the owners of these firms

TI-UK has identified a number of business models within the UK TCSP sector, each with its own incentive structures and money laundering risks. A significant part of the UK TCSP sector operates either on a high volume-low margin business model, forming thousands of companies a year and making small amounts of profit on these formations and the services they provide; or on a low volume-high margin business model, incorporating lower volumes of entities but selling them at higher prices.[197]

The latter is more common for more complex and high-risk vehicles such as LLPs or SLPs, and higher costs are related to the setting up of offshore partners and members as well as the provision of additional services mailing services and bank accounts in a range of different jurisdictions, including Latvia. For example, as reported by TI-UK, at the time of writing, GWS Offshore had seven SLPs owned through Anguillan companies with Latvian bank accounts for sale ranging between $6.490 up to just under $10.000.[198]

The veneer of respectability offered by the UK has also led to the phenomenon of "company factories" – addresses of non-descript building where thousands of UK companies are registered and offering the respectable appearance of a UK company, while in reality representing little more than a mailbox. Company factories all over UK may be behind the mass incorporation of Scottish Limited Partnerships. TI-UK has found that while over 70% of SLPs created in the last 10 years were registered at just 10 addresses, at present there would be 66 company factories operating in the UK with over 1,000 companies registered at each address.[199]

UK-based TCSPs have often links and interactions with TCSPs operating at the global level, and collaboration has come in form of subsidiaries or through informal channels, with transactions and trade of shell companies conducted on occasional bases. This has posed regulatory challenges in terms of understanding the money laundering risks around the supervision of offshore TCSPs and the abuse of UK legal entities. According to UK Law, only TCSPs carrying on business in the UK (including subsidiaries of foreign TCSPs) are bound by money laundering regulations there. In turn, the regulation of individuals and firms setting up UK companies, but with no physical presence there falls to the jurisdiction in which they are physically based.[200]

Partly as a result of the confusion around who money laundering regulations apply to, evidence shows that significant numbers of high-risk corporate vehicles are being formed by unregistered and unsupervised TCSPs. Analysis carried out by David Leask, Chief reporter of the Scottish Herald, found that on a sample of 6.000 SLPs, half had been created by TCSPs which were not registered with the UK supervisor, the HRMC.[201]

As TCSPs operating from Latvia or other countries may trade among themselves UK companies incorporated by themselves or purchased from UK-based agents, these transactions carry a significant money laundering risk due to the likelihood that neither party involved in the transaction is a regulated entity and therefore have no reason to adhere to money laundering regulations, in the UK and abroad.[202] The sale of UK companies - potentially equipped with Latvian bank accounts - between unsupervised offshore TCSPs poses a high risk of money laundering and a challenge to law enforcement agencies.

The case study of Arran Business – involved in the creation of shell companies used for the Moldovan bank fraud and the Russian Laundromat – is an example of how the connections between UK-based, Latvia-linked and international TCSPs trading shell companies and the loose collaboration they may develop with Latvian banks can have deleterious effects.

[197] Transparency International-UK (2017), Hiding in Plain Sight: how UK companies are used to launder corrupt wealth, p.24 http://www.transparency.org.uk/publications/hiding-in-plain-sight/#.Wj6iTVKZPVr
[198] ibid.
[199] ibid. p.26
[200] ibid. p.38
[201] http://www.heraldscotland.com/news/15368778.Analysis__How_controversial_shell_companies_conquered_everything_from_money_laundering_to_Formula_One/
[202] Transparency International-UK (2017), Hiding in Plain Sight: how UK companies are used to launder corrupt wealth, p.24 http://www.transparency.org.uk/publications/hiding-in-plain-sight/#.Wj6iTVKZPVr p.42

Behind the Moldovan Bank Robbery

The Kroll investigative report on the Moldovan bank robbery showed that a total of 48 UK shell companies – 20 registered in Scotland, 28 elsewhere – was used in all key phases of the schemes.[1] According to investigative journalist Graham Stack, the bulk of Scottish shell companies could be traced back to two company service providers, Arran Business Services and Royston Business Consultancy, both registered at the Edinburgh address of 18/2 Royston Mains Street and linked by personal and corporate ties to other feeder structures at around a dozen different addresses.[2]

These addresses allegedly provided shell companies not only for the Moldovan bank fraud, but also for the Russian Laundromat and other money laundering schemes. Fortuna United LP, the Scottish firm to which $750 million were made disappear had its registered address at 18/2 Royston Mains Street, together with almost 250 other SLPs registered there in the last 10 years.[3] According to the UK company register, Arran Business Services has no beneficial owner, but one of its manager since 2011 has been a Latvian national resident in the UK, Vitalijs Savlovs. In May 2016 Arran Business Services moved to the Suite 2 of 44 Main Street, Douglas, Scotland.[4] According to TI-UK open source analysis, this was the address of 21 companies identified as having been involved in illegal activities.[5]

At the time of the scandal, Arran Business Services formed part of Arran Consult, a corporate service provider operating across CIS countries.[6] The Arran Consult Russian-language website, which appears to be no longer active, publicises its partnership with leading Latvian banks, among which is ABLV – named in the investigation into the Moldovan bank scandal as having business relationship with 14 of the UK companies involved. While investigating, Graham Stack contacted Arran Consult in Russia, and they said they are no longer connected to Savlovs, nor they had any connection with the Moldovan case.[7]

In Latvia, Savlovs was owner of the "legal services" firm Arran Latvia, operating from December 2011 to September 2015 with registered address in Riga. Investigative journalists found indications of Savlovs' close connections to Latvia's banks. He formerly served on the board of Latvia's former biggest bank – Parex – and had close connections to Baltikums Bank (now BlueOrange Bank), in particular in 2010-2012, for which he is said to have formed Scottish Limited Partnerships.[8]

Baltikums Bank was not one of the banks mentioned in the Kroll report as having clients who transited funds stolen from Moldova, and is also not a bank featured on the Arran Consult website as a partner. According to the Latvian company register, Savlovs had a seat on the board of one Latvian affiliate of Baltikums Bank, BB Trust Consultancy Ltd, until 2012. As Baltikums Bank told reporters, BB Trust Consultancy Ltd "was not Baltikums Bank's subsidiary in legal terms". The bank also denied having had any business relationship with Savlovs or his Arran companies.[9] According to the September 2017 LKA Compliance Status Review, in 2017 the bank 'has discontinued cooperation with partners in the area of client identification and now performs client identification only by meeting with clients face-to-face.[10]

Apart from the Moldovan Bank fraud and the Russian Laundromat, Savlovs was also cited as a company service provider for companies involved in a separate money laundering case in a London High Court decision on fraud case amounting to around £130 million.[11] While Savlovs may not have knowingly been involved in the scandals, the companies he helped to create provided ideal vehicles for money laundering.

In a 2015 interview, he acknowledged acting as business introducer for foreigners to Latvian banks, but he denied moving to Scotland to launch a "company factory" incorporating Scottish shell companies for the banks.[12] He also claimed his business was not so big, as he earned only a tiny fee per company and used to incorporate just over 100 firms per year for clients. As he pointed out, it takes only 15 minutes to incorporate a UK company online: "many business people in post-Soviet countries don't know English, and we help them", he said. "Apart from this, we don't do anything." Savlovs also claimed he had received no police requests to check his customer files.

---

[1] Kroll (2015), Project Tenor – Scoping Phase, Final Report, available at http://candu.md/files/doc/Kroll_Project%20Tenor_Candu_02.04.15.pdf

[2] Bne Intellinews (2015), 'Latvia banks fuel Scotland's shell company 'factory' linked to Moldova fraud', http://www.intellinews.com/latvia-banks-fuel-scotland-s-shell-company-factory-linked-to-moldova-fraud-500446872/?archive=bne [accessed 30 October 2017]

[3] Transparency International-UK (2017), Hiding in Plain Sight: how UK companies are used to launder corrupt wealth, http://www.transparency.org.uk/publications/hiding-in-plain-sight/#.Wj6iTVKZPVr

[4] https://beta.companieshouse.gov.uk/company/SC332769

[5] Transparency International-UK (2017), Hiding in Plain Sight: how UK companies are used to launder corrupt wealth, http://www.transparency.org.uk/publications/hiding-in-plain-sight/#.Wj6iTVKZPVr

[6] BneIntellinews (2015), 'Mystery Latvian linked to Scottish shell companies denies role in $1bn Moldova bank fraud' http://www.intellinews.com/mystery-latvian-linked-to-scottish-shell-companies-denies-role-in-1bn-moldova-bank-fraud-83352/ [accessed 30 October 2017]

[7] ibid.

[8] ibid.

[9] ibid.

[10] Association of Latvian Commercial Banks (ALCB) (2017), 'Compliance Status Review, September 2017', http://lka.org.lv/en/compliance/

[11] BneIntellinews (2015), 'Mystery Latvian linked to Scottish shell companies denies role in $1bn Moldova bank fraud' http://www.intellinews.com/mystery-latvian-linked-to-scottish-shell-companies-denies-role-in-1bn-moldova-bank-fraud-83352/ [accessed 30 October 2017]

[12] ibid.

4.4 Business introducers

Incorporation and trade of corporate vehicles across jurisdictions constitute the core business of many TCSPs. However, most of them can also act as "business introducers", opening accounts at partnered banks across the world for potential bank clients and taking responsibility for compiling client due diligence files and documents. As discussed above, reliance on these agents was a common among overseas branches Latvian banks offering financial logistics services.

Contacts between introducers and potential clients largely take place via Internet and through secured lines of communication assuring privacy and confidentiality. Some TCSPs' websites list partnership status with individual banks, and some banks may detail in their annual reports partnership status with individual business introducers and may instruct potential clients to go through them to open an account at the bank.[203]

A quick search on the internet reveals that, among a range of options available, Latvia is often advertised for its ease of accessibility and the possibility to remotely open a bank account with no client interview at the bank needed. Pictures 3 and 4 show examples of international, UK and Latvia-linked TCSPs advertising Latvian banking services.[204] As can be noticed, the price for opening a bank account in Latvia ranges between €350-600 depending on the partnership status. with the bank and the connections with affiliated local TCSPs.

Picture 3 – Business introducer offering opening of bank accounts in Latvia, Switzerland and Lichtenstein

№	Name of bank	Country	How long it takes to open an account (working days)	Cost of opening an accoun	Minimum deposit	Client interview at the Bank
1	Norvik Bank	Latvia	10-14	550 EUR	not required	not required
2	C.I.M. Banque	Switzerland	10-14	1 200 EUR	10 000 EUR/USD	not required
10	Valartis Bank	Liechtenstein	10-14	1 200 EUR	300 000 USD	not required

Picture 4 – Business introducer offering opening of bank accounts in Baltic banks

Baltic States banks (Latvia, Lithuania, Estonia)

Type of Bank account: Corporate Account/Personal Account

Fee – 350 € + bank tariff

If you are looking for a European Bank which provides multi-currency accounts, internet banking service and the major payment cards, then you should consider banking in the Baltic States.

Due to our privileged relationship with our partners in the Baltic States, we are able to benefit from simplified administrative formalities when opening a bank account.

We offer corporate accounts only for companies which were incorporated through our service.

[203] 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 Issue: 4, pp. 496-512

[204] Picture 3: http://www.goodwin-gmc.com/en/uslugi/otkrytie-scheta-v-banke/ [last accessed 14 January 2017]; Picture 4: http://mail.cmc-providers.com/en/our_services/bank_accounts/baltic_states_banks/ [last accessed 14 January 2017]. Transparency International Latvia is making no allegation of non-compliance with AML rules against the owners of these firms, and the banks in the picture.

Indeed, this 'introducer' role has many legitimate functions. However, according to FATF, primary responsibility for Customer Due Diligence remains with the bank, which also needs to ensure that the introducer complies with AML regulations and that the information they keep is immediately made available to banks under request.[205]

When banks over-rely on business introducers, this may have deleterious effects for beneficial ownership transparency and money laundering risks. For example, a unique 2013 audit on the Cypriot banking sector by MONEYVAL found that an estimated 75% of business at the banks analysed had been brought in by introducers, often passing through whole chains of company service providers before reaching the banks.[206]

In connection with the heavy use of introducer structures, 70% of the customers files audited had nominee shareholders, with an average of three layers distancing the customer vehicle from the beneficial owner, while on average 27% of deposit client files were found to contain inaccurate information on beneficial owners. In addition, approximately 10% of customers were found to be politically exposed persons, but had not been flagged as such.[207]

The MONEYVAL report on Cyprus shows how reliance on business introducers and corporate service providers can have serious negative impacts on the identification of the ultimate beneficial owners holding accounts in financial institutions.

As seen above, there is evidence that, over time, Latvian banks relied on the services of business introducers with deleterious effects for money laundering through their channels. In response to that, the Latvian financial regulator strengthened the regulation related to banks' cooperation with third parties for customer identification and on-boarding of new clients.[208]

The regulation requires that before engaging with agents, banks must substantiate the need for such services and assess the money laundering risks related to countries and territories where they operate. Moreover, the decision

[205] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html
[206] MONEYVAL (2013), 'Special assessment of the effectiveness of customer due diligence measures in the banking sector in Cyprus', available at: https://rm.coe.int/special-assessment-of-the-effectiveness-of-customer-due-diligence-meas/168071611d
[207] ibid.
[208] Financial and Capital Market Commission (FCMC), Regulation No.196/2016, Regulations for Cooperation with Third Parties and Requirements for Business Relations with the Customers whose Identification or Due Diligence is Performed Using Third Party's Services, http://www.fktk.lv/en/law/credit-institutions/fcmc-regulations.html

of collaborating with a determinate agent of firm must be approved by the bank's Senior Management responsible for AML compliance.[209]

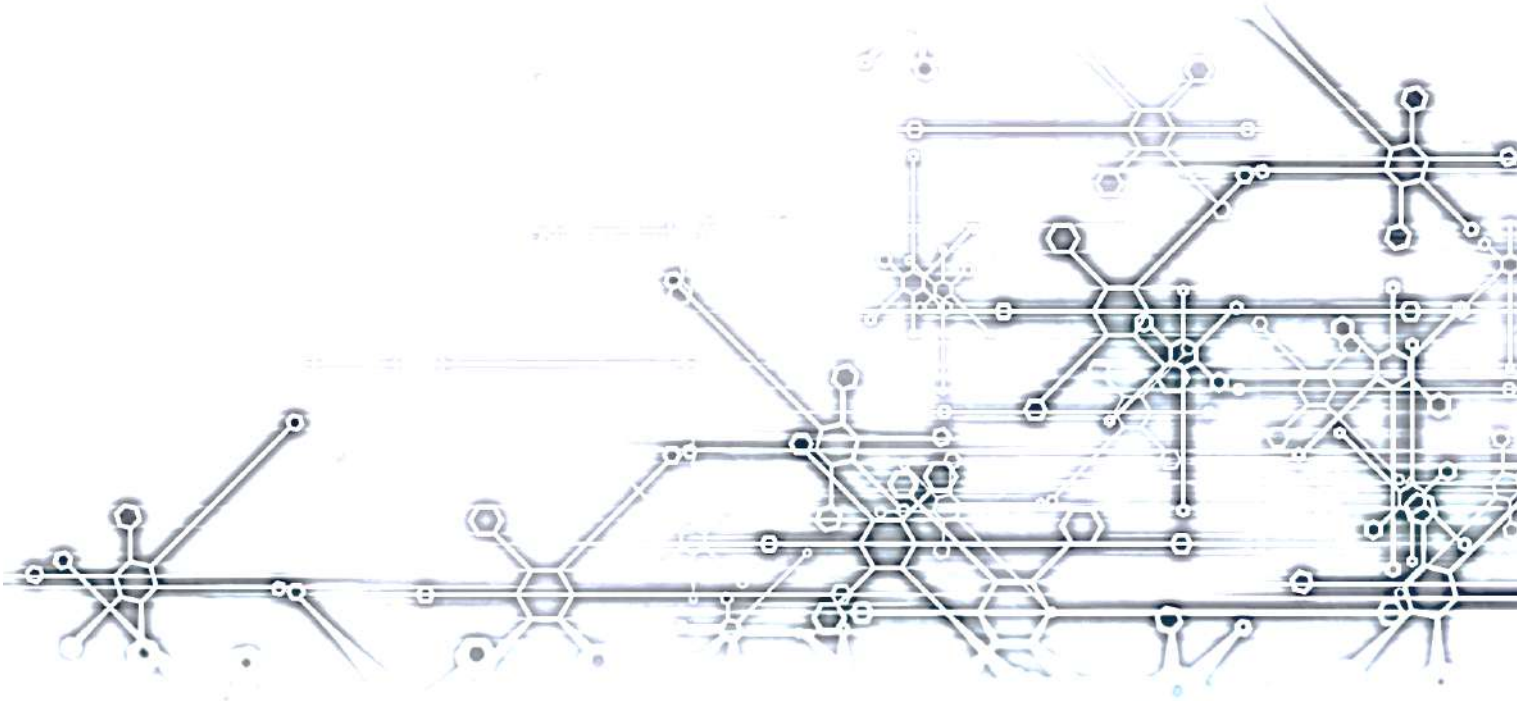
Banks are also required to establish and update a Register of Agents containing all the relevant information and details on the collaboration agreements, keeping record of their decision to establish business relations with customers brought in with the agents.[210]

When collaborating, banks must ensure that the agents conduct face-to-face customer identification and that they have not subcontracted such duties to third parties.[211] The Regulation also emphasises the importance of agents' awareness of money laundering typologies and risk mitigation, obliging banks to develop AML training programmes for them and ensure that such trainings are carried out at least once a year.[212]

The Regulation also implements Enhanced Due Diligence measures for clients on-boarded through agents. In particular, banks must establish a mechanism in their ICSs which enables them to identify the customers whose identification has been carried out by third parties. If the customer brought in by the agent is a shell company or a PEP, the bank itself must conduct face-to-face identification no later than three months after the establishment of the business relation.[213]

This is a major step towards protecting the Latvian financial system against unscrupulous TCSPs. However, the lack of supervision and regulation for these actors across the world suggests the need for a focused monitoring on these relationships.

The case study of France Offshore, in which one Latvian bank was allegedly involved in mass tax evasion and money laundering in France, demonstrates how reliance on third parties for customer identification may result in the unwitting involvement of financial institutions in cases of financial fraud, and trigger lengthy and consuming investigations due to difficulties in the attribution of the ultimate responsibility for the crimes.



[209] ibid. p.1
[210] ibid. p. 5
[211] ibid. pp.1-2
[212] ibid. p. 4
[213] ibid. pp.6-7

Case Study – France Offshore

France Offshore was a France-based trust and company service provider which presented itself as a network of more than 120 lawyers, jurists and accounting experts from different European countries providing their clients with the necessary know-how for the creation of offshore entities and the opening of bank accounts in various jurisdictions, including Latvia, Switzerland, Hong Kong, Singapore and Cyprus. The firm was formed in the 2000s by the French citizen Nadav Bensoussan, who was proud to announce his ambition to provide "offshore for all".[1]

He was even protagonist of a 2011 French television piece recorded in Latvia, in which he shows the reporter an advertisement of France Offshore at the Riga airport offering the creation of offshore bank accounts and similar financial services. He then goes to visit Rietumu's offices in Riga, where he meets the bank's then vice-president.[2] In a later interview, Bensoussan claimed the target customers of France Offshore were small companies who wanted to "pay taxes, but little, and elsewhere".[3]

Investigation by the French authorities on the activities of France Offshore began in July 2011 and spanned six years. According to investigation files, France Offshore had facilitated tax evasion and money laundering on a massive scale, with initial estimates amounting to around €760 million.[4]

Among France Offshore's clients were not only ordinary taxpayers and small businesses in France, but also outright criminals involved in frauds related to Value Added Tax, Carbon Tax and foreign exchange market, about which Bensoussan claimed to be unaware.[5]

The scams typically operated by setting up complex networks of shell companies in various offshore jurisdictions, for which France Offshore had set up a total of some 700 bank accounts at Rietumu Bank, in Latvia.[6] Later on, France Offshore was also found to be a partner of the Panamanian law firm Mossack Fonseca, at the centre of the Panama Papers scandal.[7]

On 6 July 2017, the French Criminal court sentenced Bensoussan to five years in jail, while Rietumu was handed a €80 million fine and a ban on its activities in France for 5 years. To put figures in perspective, the audited profit of Rietumu in 2016 was €80.3 million and the largest fine ever imposed on a Latvian bank (ABLV) was €3.17 million. Rietumu's chairman of the board and its representative in France were also sentenced to respectively 4 years of conditional imprisonment and 1 year of probation period.[8] At the hearing, the presiding judge said the proven amount of money laundered from 2008 to 2012 was at least €203 million, but investigators believe the amount is much higher, up to €850 million.[9]

The bank's lawyers appealed to the judgment, defending the absence of illegal conduct from the bank and stating that Rietumu was fully compliant with Latvia's law, that all the international requirements and recommendations had been observed and that there does not exist any evidence in the materials held by the prosecution to prove the personal involvement of the bank's senior officials in the activities of France Offshore or its clients. The bank also noted that until the judgment comes into effect, it is not obliged to pay any fine. "Given all the upcoming instances, the process can continue for a long time - up to 2-3 years and longer," said the bank's representatives. Until the end of the litigation process, Rietumu Bank will refrain from commenting in this case.[10]

---

[1] Le Figaro (2012), 'Un patron d'un site offshore en examen', http://www.lefigaro.fr/flash-actu/2012/12/19/97001-20121219FILWWW00587-un-patron-d-un-site-offshore-en-examen.php [accessed 30 October 2017]

[2] https://www.youtube.com/watch?v=kWkN838VxCk

[3] Le Monde (2017), 'France Offshore: "Le paradis fiscal pour tous" face au tribunal', http://www.lemonde.fr/police-justice/article/2017/02/27/france-offshore-le-paradis-fiscal-pour-tous-face-au-tribunal_5086080_1653578.html [accessed 30 October 2017]

[4] ibid.

[5] ibid.

[6] Lsm.lv (2015), 'Details emerge of massive French tax evasion scam using Latvian bank', http://eng.lsm.lv/article/economy/economy/details-emerge-of-massive-french-tax-evasion-scam-using-latvian-bank.a154945/ [accessed 30 October 2017]

[7] Lsm.lv (2016), 'Wall of silence on activities of Mossack Fonseca Riga office', http://eng.lsm.lv/article/economy/economy/wall-of-silence-on-activities-of-mossack-fonseca-riga-office.a177541/

[8] Lsm.lv (2017), 'Rietumu handed massive French fine' http://eng.lsm.lv/article/economy/banks/latvian-bank-handed-80-million-euro-fine-in-france.a242443/ [accessed 30 October 2017]

[9] http://www.dailymail.co.uk/wires/ap/article-4671842/Latvian-bank-fined-heavily-laundering-scheme-France.html#ixzz52YhQbwnJ [accessed 28 December 2017]

[10] Ir (2017, 'Rietumu bankai naudas atmazgasanas lieta francija piespriests 80 miljonu naudassods' http://www.irlv.lv/2017/7/6/rietumu-bankai-naudas-atmazgasanas-lieta-francija-piespriests-80-miljonu-naudassods [accessed 30 October 2017

5.Recent measures in Latvia's AML regulatory framework and policy recommendations

Public-private partnership in the AML field

The year 2017 has seen a further strengthening of AML rules in Latvia, as well as an unprecedented self-regulatory push by part of the Latvian banking sector. This has come mainly from Association of Latvian Commercial Banks (ALCB), which has taken a more proactive stance on the issue of money laundering and offshore banking. Apart from monitoring the implementation of banks' remediation plans following the US external audits, the ALCB has fostered public-private partnership to more effectively tackle financial crime at the national level and has sustained banks' business re-orientation towards low and medium risk clients and products.[214]

In autumn 2017, the ALCB has issued for the first time a set of policy guidelines on Anti-Money Laundering, Terrorist Financing and Enforcement of Sanctions.[215] The guidelines policies of no-cooperation with high-risk jurisdictions, stricter requirements for cooperation with shell companies in order to ensure corporate transparency among clients and zero tolerance regarding intentional violations of AML/CFT law and regulation. Importantly, the guidelines also mention an explicit policy of vigilance against and no cooperation with non-authorized and not supervised company service providers, thus acknowledging the potential high-money laundering risk constituted by the scarce regulation of these firms.[216]

According to the latest ALCB's Compliance Status Review, as of September 2017, eleven Latvian banks had implemented 81% of remediation plans drafted following the independent US audits carried out in 2016.[217] Among them, 10 pointed out they exited high-risk jurisdictions, 9 pointed out they changed their business model ad strategy and 6 banks have pointed out that they established Enhanced Due Diligence and stricter on-boarding requirements for clients acquired through agents.

The general improvement of Latvia's AML framework and the reduced risk of money laundering in the financial sector was demonstrated by the results of the 2017 Basel Anti-Money Laundering Index, published by the Basel Institute of Governance since 2012. The Index covers 146 countries and provides risk ratings based on the quality of a country's framework for AML and related factors such as perceived levels of corruption, financial sector standards and public transparency. In just one year, from 2016 to 2017, Latvia improved its score and climbed 14 positions, from 28th in 2016 to 14th in 2017.[218]

New Law on the Prevention of Money Laundering and Terrorist Financing

At the end of October 2017, Latvia adopted the new Law on the Prevention of Money Laundering and Terrorist Financing, transposing the EU 4th Anti-Money Laundering Directive and making the country fully compliant with the latest European and international anti-money laundering standards.[219]

The amendments envisage more transparency in the financial sector, public access to beneficial ownership information, improved international cooperation on financial crime, a focus on the mitigation of risks, and a more robust supervision and sanctioning system of the law subjects. By making information on beneficial owners of companies publicly available, changes to Latvia's AML legislation have gone even beyond the EU 4AMLD.

In Latvian AML Law, the beneficial owner is generally defined as the natural person who ultimately owns or control a company or legal arrangement and in whose name a transaction in the interest of a client is carried out.[220] In the

[214] http://lka.org.lv/en/compliance/
[215] Association of Latvian Commercial Banks (ALCB) (2017), Policy Guidance and Guidelines on Anti-Money Laundering, Countering Terrorism Financing and Enforcement of Sanctions, https://www.lka.org.lv/wp-content/uploads/2017/12/LKA_politika_ENG-1.pdf
[216] ibid. p.4
[217] Association of Latvian Commercial Banks (ALCB) (2017), 'Compliance Status Review, September 2017', http://lka.org.lv/en/compliance/
[218] Basel Institute of Governance (2017), Basel AML Index 2017, https://index.baselgovernance.org/sites/index/documents/Basel_AML_Index_Report_2017.pdf
[219] Law on Prevention of Money Laundering and Terrorism Financing, https://likumi.lv/doc.php?id=178987
[220] ibid., section 1

case of companies, the beneficial owner is at least a natural person who holds, directly or indirectly, more than 25% of the (voting) shares in a legal person or controls the entity, directly or indirectly. In the case of legal arrangements, the beneficial owner is 'the person in whose interest the legal arrangement is established or operates, or any other natural person who actually exercises control over the legal form, by ownership or other means, including the settlor, the supervisor or beneficiary of such arrangement'.[221]

Even though this definition of beneficial owner of companies is comprehensive, the control threshold set at 25% of total shares or voting rights which is too high and easy to circumvent for people looking to stay under the radar, as stated by the European Commission in its own impact assessment on the 5th AML Directive proposal.[222] As a solution, the commission proposed to lower the threshold to 10% in respect of legal entities with specific AML risks.

In case a beneficial owner cannot be identified using the primary criteria of ownership and control, then the person with the highest management role in the given entity can be identified as the beneficial owner instead. This, however, leaves open the possibility to list nominee directors as beneficial owners, which is misleading and will prevent public authorities and others from detecting anomalies and raising red flags.[223] This loophole is still largely present among EU Member states, though it has been closed with EU institutions' agreement on the future 5th AML Directive at the end of 2017.[224]

According to the new AML Law, by March 2018, legal entities will be required to submit an application indicating their ultimate beneficial owner to the Latvian Register of Enterprises (RE).[225] The new rules also introduce a public register of beneficial owners to be launched in April 2018. Information in the register will be accessible to the public online (on the RE website) and in open data format for the payment of a fee.[226]

The public register of beneficial owners is a great step forward towards transparency of corporate entities in Latvia. It will likely facilitate the work of law enforcement authorities in Latvia and the rest of the EU, and enhance scrutiny by citizens, public media, civil society organisations and investigative journalists. It will also help bring more scrutiny in the TCSP sector, deterring money launderers from becoming beneficial owners of these firms.

However, the fee may represent a barrier against the public demand for this information. In the UK, for example, there is no fee for access to beneficial ownership information contained in the Companies House Register. Since the UK removed a small paywall in 2016, data use has grown exponentially to over 2 billion searches a year, up from 6 million access requests during 2014-15.[227] This demonstrates there is significant demand for this data, and that even a small fee will create a barrier.

- ✓ **The threshold for the identification of beneficial ownership should be lowered to 10%, or alternatively, appropriate thresholds at the national level requiring a good understanding of the ownership structures of companies in the country should be set. This would make it more difficult to appoint a few trusted individuals as shareholders. A more differentiated approach could also be considered, for instance by setting sector-specific thresholds or subjecting PEPs to different threshold policies.**

[221] ibid.
[222] European Commission (2016), Impact assessment accompanying the document "Proposal for a Directive of the European Parliament and the Council for amending Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, p.95
[223] Transparency International EU (2017), 'Under the Shell: Ending Money Laundering in Europe', https://transparency.eu/under-the-shell/ [Accessed 20 October 2017]
[224] http://www.sven-giegold.de/2017/lost-and-won-details-of-the-compromise-on-the-european-anti-money-laundering-directive/
[225] Law on Prevention of Money Laundering and Terrorism Financing, Section 18, https://likumi.lv/doc.php?id=178987
[226] ibid.
[227] Global Witness (2017), '10 Lessons from the UK's public register of the real owners of companies', https://www.globalwitness.org/en/blog/10-lessons-uks-public-register-real-owners-companies/

- ✓ **A mechanism should be established that allows for the identification of senior managers in the public register of beneficial ownership, in those cases in which the beneficial owner cannot be found.**
- ✓ **Any fee that is currently levied on the general public in order to get access to beneficial ownership information should be removed.**

Action Plan for the mitigation of the money laundering risks in the TCSP sector

New State Revenue Services' Anti-Money Laundering Department and increased sanctions

With the Latvian Anti-Money Laundering Action Plan for the years 2017-2019, the Government has expressed the intention of enhancing the supervisory and risk assessment capacity of the State Revenue Service in the area of money laundering. As such, the plan has envisaged the institution of a new, money laundering-focused structural unit within the SRS, composed of 21 officers and provided with the necessary resources to carry out their duties.[228]

With the new AML Law, the Latvian Government has also addressed the loophole regarding low sanctions and scarce information regarding the enforcement work of the SRS. With the new Law, a clear framework on the power of the SRS to issue sanctions has been implemented, and the SRS will be required to publish timely, comprehensive and detailed statistics about the number of inspections carried out, the nature of breaches found and their consequences. Moreover, the SRS will be able to apply sanctions up to €1.000.000, depending on the seriousness of the breach.[229] This is expected to constitute a solid deterrent against firms which may be wittingly involved in money laundering.

As of November 2017, the new AML unit of the SRS had already recruited 13 employees and was expected to reach full capacity by the end of January 2018. The unit is composed of two divisions, respectively focusing on risk assessment and on-site supervision.[230] This is expected to raise the effectiveness of the supervisory process and reduce the possibility for TCSPs to get involved in money laundering and other financial crimes. On-site supervision will also likely enhance the capacity of the unit to gather relevant information on the development of internal AML procedures and improve the quality of risk assessment.

These measures are expected to have a positive money laundering risk-mitigation impact. However, as seen above, the increasing complexity of the sector and its inherent transnational nature call for an in-depth assessment of the TCSP sector in Latvia and its intersections with other jurisdictions, a strong implementation of international standards in the field, and high-quality guidance on AML rules to TCSPs and other professional intermediaries.

- ✓ **A thematic review of the TCSP sector in Latvia should be conducted and published. This should: a) include an analysis of how many firms are operating in the sector as well as the number of their subsidiaries in other countries; b) encompass best-practices in AML procedures in the field and make a comparison with the actual standards in Latvia; c) provide solutions for improving those standards. The results of the study could also be used to update the guidance issued.**

[228] Plan of Measures for Mitigation of the Money Laundering and Terrorism Financing Risk for 2017-2019, p.24, http://www.fm.gov.lv/en/s/financial_market_policy/plan_of_measures_for_mitigation_of_the_money_laundering_and_terrorism_financing_risks_for_2017___2019/
[229] Law on Prevention of Money Laundering and Terrorism Financing, Section 78, https://likumi.lv/doc.php?id=178987
[230] Delna in consultations with the SRS, 29 November 2017

The need for licensing and regulation

The Latvian government has acknowledged the high risk posed absence of licensing and lack of regulation, and in the ML Action Plan 2017-2019 it has pointed out the need to develop proposals for the licensing of sectors currently not regulated by the subjects of the AML Law, including firms carrying out TCSPs services. The Ministry of Finance, in coordination with the Ministry of Economics, the Ministry of Justice and the SRS are currently in charge of developing proposals for licensing of TCSPs and, if necessary, amendments to the legal framework.[231]

The new AML Department of the State Revenue Service has expressed its support and reiterated the need for licensing of TCSPs, as this would enable appointed supervisors to have a better and clearer overview of the sector and enhance their supervisory capacity. However, it has also indicated that the development of proposals will require at least one year. This is due to both the complexities of the sector and potential resistance to regulation by part of the firms themselves.[232]

Regulation and licensing subject to a AML test should be made a priority by competent authorities. It would allow competent authorities to better assess and supervise firms in the sector, and It would ensure that all TCSPs operating in Latvia are aware of AML regulations and understand the ML risks they incur providing their services. Moreover, for legitimate firms in the TCSP sector, it is also expected to improve the quality and professionality of the services provided, while at the same time protecting the consumers.

The development of licensing in the TCSP sector should be accompanied by stronger regulation in the specific activities that these firms carry out from Latvia. As discussed above, the services offered by TCSPs have often helped individuals engaged in illegal activities in setting up complex offshore arrangements hiding their identity from law enforcement authorities. This calls for stronger regulatory measures prohibiting firms from – wittingly and unwittingly – servicing corporate structures or arrangements facilitating anonymity of beneficial owners and money laundering. In the future, breaches with this regulation may also include losing the license.

- ✓ **Appropriate licensing requirements for firms carrying out TCSP services in Latvia should be made a priority. These firms should be subject to a 'fit and proper test' (a series of checks, to make sure that they meet the requirements of the National Anti-Money Laundering Laws and Regulations) at the time of licensing and over the period for which they hold a license, applying similar standards of integrity as for financial institutions. Branches and subsidiaries of Latvian TCSPs operating abroad should also be subjected to the same checks and integrity requirements.**
- ✓ **TCSPs should be prohibited from servicing corporate structures or arrangements facilitating anonymity of beneficial owners and money laundering and act as nominee directors for clients. Non-compliance with rules may also include losing the license to operate.**

Regularity of trainings

The Government has also acknowledged the need for obliged entities to improve their knowledge regarding AML obligations as well as the quantity and quality of suspicious or unusual transactions submitted to the FIU. To this purpose, the SRS will be required to organise regular trainings for the supervised entities, paying special attention to the identification and reporting of suspicious transactions. The trainings will also include the case study analysis,

[231] Plan of Measures for Mitigation of the Money Laundering and Terrorism Financing Risk for 2017-2019, p.23, http://www.fm.gov.lv/en/s/financial_market_policy/plan_of_measures_for_mitigation_of_the_money_laundering_and_terrorism_financing_risks_for_2017___2019/

[232] Delna in consultations with the SRS, 29 November 2017

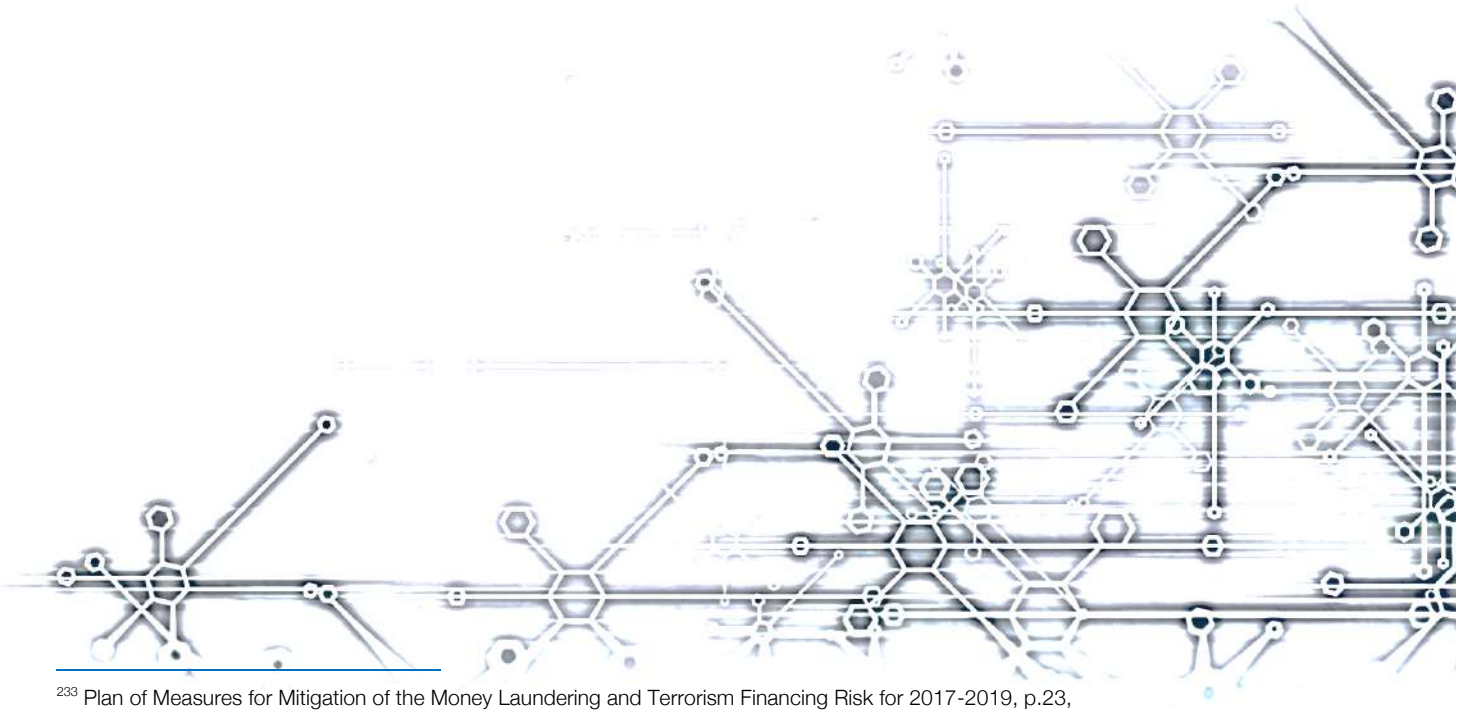
paying attention to cases reported in the media.[233] The SRS' AML Department has confirmed that the number of trainings will be increased, and that seminars will be organised regularly every 1-2 months.[234]

Trainings, however, will not be compulsory, and this may represent a weakness, as a certain number of obliged entities may not participate and be covered. On the other hand, the AML Department has pointed out the difficulty of applying such requirement, due to the high number of firms operating in the sector. In remediation, the Department is planning to develop an e-training platform, through which TCSP firms would be able to train remotely. In order to encourage participation of TCSPs in e-trainings, the Department has expressed the intention of implementing rewarding mechanisms rather than administrative fines for non-participation.

The use of an e-platform with rewarding mechanisms for participating firms is likely to encourage more TCSPs to regularly participate in trainings. However, supplementary mechanisms should be implemented in order to obtain specific information on the rate of participation in e-trainings, allow trained firms to give their feedback on the quality of the training and express the need of education on specific issues related to AML compliance. This would likely improve the capacity of the SRS to progressively enhance the quality of the trainings issued (both online and offline) and better understand ML risks firms encounter in carrying out their activities.

In the future, participation in AML trainings could also be made a precondition for obtaining and keeping a license. This would ensure that all firms operating in the sector are regularly educated on AML matters.

- ✓ **E-trainings for TCSP firms should be supplemented by mechanisms allowing for feedback by part of trained firms and collection of useful information on the activities in the sector by part of the supervisor.**
- ✓ **Participation in anti-money laundering training organised by the State Revenue Service should be made a condition for obtaining and keeping a license.**



[233] Plan of Measures for Mitigation of the Money Laundering and Terrorism Financing Risk for 2017-2019, p.23, http://www.fm.gov.lv/en/s/financial_market_policy/plan_of_measures_for_mitigation_of_the_money_laundering_and_terrorism_financing_risks_for_2017___2019/

[234] Delna in consultations with the SRS, 29 November 2017

Transparency International Latvia

Citadeles iela 8, Riga,

LV1010, Latvia

+371 6785584

ti@delna.lv

www.delna.lv