TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Heli Meklin

THE EMERGENCE OF FINTECH – THE AML VULNERABILITIES IN THE EU REGULATORY FRAMEWORK

Bachelor's thesis

Programme HAJB08/17 - Law, specialisation European Union and International Law

Supervisor: Jenna Uusitalo, MA

Tallinn 2020

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 12326 words from the introduction to the end of conclusion.

Heli Meklin……
(signature, date)
Student code: 176401HAJB
Student e-mail address: heli.meklin@gmail.com

Supervisor: Jenna Uusitalo:
The paper conforms to requirements in force

……
(signature, date)

Co-supervisor:
The paper conforms to requirements in force
……
(signature, date)

Chairman of the Defence Committee:
Permitted to the defence
……
(name, signature, date)

TABLE OF CONTENTS

ABSTRACT 4
ABBREVIATIONS 5
INTRODUCTION 6
1. THE EMERGENCE OF FINTECH 9
1.1 Background – the emergence of FinTech 9
1.2 The variety of activities under FinTech 10
1.2.1 Comparison to banks 11
1.2.2 Challenges to the regulator and the supervisors 12
2. ANTI-MONEY LAUNDERING REGULATIVE FRAMEWORK IN THE EU 13
2.1 Money laundering and its socio-economic effects 13
2.2 The background for the current AML legislation 14
2.3 The EU AML legislation – an overview 15
2.4 FinTechs in the EU AML Framework 17
2.4.1 Obliged entities 17
2.4.2 Licenses 18
2.4.3 Self-regulation through the chain of supervised entities 19
2.5 Risk-based approach 20
2.5.1 Introduction to the RBA 20
2.5.2 Applying the RBA 21
2.6 Directive-based approach 22
3. FINTECH AML VULNERABILITIES 24
3.1 CDD 24
3.1.1 Registration, ID collection and verification 25
3.1.2 Fake identities 26
3.1.3 Assessing and monitoring the customer behaviour 27
3.2 The FinTech AML vulnerabilities exposure on traditional banks 29
4. MITIGATING ACTIONS 31
4.1 Public-private-partnerships (PPP) 31
4.2 Regulatory sandboxes 31
4.3 Traditional bank - FinTech collaboration 32
4.4 Knowledge-sharing within FinTechs 33
4.5 EU-wide supervisory authority 34
CONCLUSION 36
LIST OF REFERENCES 39

ABSTRACT

This thesis examines the emerging and innovative financial technologies (FinTechs) in the light of the current anti-money laundering (AML) regulative framework in the European Union. The study detects possible financial crime vulnerabilities that the FinTech companies are exposed to due to their constantly and rapidly developing virtual nature. The study also discusses how the risk-based approach enables FinTechs using different and often less stringent requirements for the customer registration vary in comparison to the traditional banks. It detects AML vulnerabilities that the simple customer registration and verification process creates, how that affects the FinTechs knowing their customers, as well as further how the partnering banks are exposed to FinTech AML vulnerabilities. The study further discusses the need for collaboration and knowledge-sharing between the FinTechs, traditional banks, supervisory authorities as well as the regulators, emphasising the need for the growing understanding on the transformation that is taking place in the financial industry. The thesis investigates the challenges that the current licensing system and the diversity in the national AML legislation due to the directive-based approach creates, as well as taking a look at the need for an EU-wide supervisory authority in the matters of AML. The thesis suggests preventive measures to mitigate the risks of the emerging FinTech companies being used as a new means for money laundering and other financial crime.

Keywords: FinTech, anti-money laundering, European Union, financial crime

ABBREVIATIONS

AML – Anti-Money Laundering

AMLD – Anti-Money Laundering Directive

KYC – Know Your Customer

CDD – Customer Due Diligence

CEPS – Center of European Policy Studies

EDD – Enhanced Due Diligence

FATF – The Financial Action Task Force

The Union – The European Union

EU – The European Union

TFEU – The Treaty of Functioning of the European Union

EBA – European Banking Authority

FSA – Financial Supervisory Authority

FCA – Financial Conduct Authority

FinCEN - Financial crimes enforcement network

FIU – Financial Intelligence Unit

SAR – Suspicious Activity Report

PEP – Politically Exposed Person

PI – Payment Institution

EMI – Electronic Money Institution

UBO - Ultimate Beneficial Owner

MS – Member State

NPPS - New Payment Products And Services

MLRO – Money Laundering Reporting Officer

RegTech – Regulative Technology

FinTech – Financial Technology

SupTech – Supervisory Technology

US – United States

INTRODUCTION

Within the past ten years a number of companies rising from financial technology innovations have appeared in the markets around the globe. They have challenged the businesses of traditional financial institutions (FIs) by lowering the accessibility of financial services, bringing the operational costs down, thus providing a large variety of easy-to-use, customer friendly products and services that use new technologies. Although the development of financial technologies is not new per se, the current phenomenon of 'FinTech', seems to take the development to a new level. This has resulted in the finance industry becoming populated with FinTech start-ups as well as global technology and telecommunication companies in addition to traditional FIs such as banks.[1]

Historically, the adaptation of new technologies in the financial industry has taken place during a longer period of time, together with the major central banks and FIs, with the aim of supporting the economic and financial globalisation as well as mitigating occurring risks.[2] Now the situation is different, with FinTech companies developing technologies enabling complete new ways of thinking regarding financial services. This time the change is taking place, not between established FIs, but in companies that may identify themselves as technology companies rather than as operating primarily in the financial industry. As an example of this was the development of digital and mobile financial services in developing countries, which was enabled by the growing accessibility to mobile devices being led mainly by telecommunications companies without the organised supervision of financial regulators.[3] The understanding of the realities and obligations of financial service providers as well as the financial crime risks may not always be as strong as the technological knowledge.

Methods of money laundering (ML), being actions of turning illicit funds to appear as legitimate, are also evolving alongside the new products and services in the market. Previously, the cash derived from criminal proceeds was placed into the financial system via cash intensive businesses, layers of transactions were created, and the funds finally integrated to the economy by a purchase

[1] *Discussion Paper on the EBA's approach to financial technology (FinTech).* EBA. Retrieved from https://eba.europa.eu/sites/default/documents/files/documents/10180/1919160/7a1b9cda-10ad-4315-91ce-d798230ebd84/EBA%20Discussion%20Paper%20on%20Fintech%20(EBA-DP-2017-02).pdf, 23 March 2020.

[2] Arner, D. W., Bargeris, J., Buckley, R.P. (2017). Fintech, regtech, and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business*, 37(3), 379; The Long, Dark Shadow of Herstatt. *The Economist*. (2001). Retrieved from http://www.economist.com/node/574236, 10 March 2020.

[3] Runde, D. (2015) M-Pesa And The Rise Of The Global Mobile Money Market. *Forbes*. Retrieved from https://www.forbes.com/sites/danielrunde/2015/08/12/m-pesa-and-the-rise-of-the-global-mobile-money-market/, 21 March 2020.

of luxury products or real estate thus making the funds appear to derive from legitimate sources.[4] Whilst this still happens, FinTechs provide new sophisticated ways and channels for illicit funds to enter the economy. ML is a serious problem threatening the integrity of the financial system, causing multiple negative socio-economic effects.[5]

FinTechs may have challenges detecting the anti-money laundering (AML) vulnerabilities of their new business-models. Regulators as well as supervisory authorities may also find challenges observing the rapid development and responding. In addition, as the FinTechs also need to partner with traditional banks, such as for example traditional banks processing the FinTech transactions, this means that the traditional banks are also exposed to new AML vulnerabilities.

Whilst The European Union (EU) AML legislation has evolved at a fast pace within the past ten years in order to respond to the development of the finance industry and the growing awareness on the negative effects of ML, improvement is constantly needed.

The hypothesis of this thesis is that the rapid emergence of FinTechs result in new money laundering risks for the finance industry.

The research questions are: What are the FinTech AML vulnerabilities? Does the current EU AML regulative framework enable AML vulnerabilities and if so, in what way? Does the FinTechs' rapid emergence expose other FIs to money laundering and if so, to what extent? Do the regulatory status of FinTechs and their possibly less stringent AML compliance obligations create distortive competition in the finance industry? In addition, what could be the mitigating actions from the perspective of FIs, regulators and supervisory authorities?

The methods used in the research are qualitative. The EU AML regulatory framework is clarified in relation to the FinTechs and a comparison of the AML compliance requirements on different actors in the finance industry is conducted. A history and the background of the current AML legislation in the EU is examined. The main standard setting bodies influencing the legislation are introduced in order to comprehend the elements, development and the current mindset of the regulatory framework. Viewpoints and articles from scholars are analysed, together with guidelines from EU bodies, non-governmental organizations from the AML field alongside

[4] Dare, P., Thornhill, S., Howarth, W.B. (2019). *ICA International Advanced Certificate in Anti Money Laundering – Course Manual*. (12th ed.) United Kingdom. International Compliance Association ICA, 6.
[5] *The Amounts and Effects of Money Laundering*. A Report for the Ministry of Finance. (2006), 84-95, 160. Retrieved from www.ftm.nl/wp-content/uploads/2014/02/witwassen-in-nederland-onderzoek-naar-criminele-geldstromen.pdf, 2 Jan 2020.

associations specialized in training of AML compliance professionals to give both theoretical as well as 'hands-on' background for the study. Due to the constant, rapid development of the subject of the research, opinions and experiences from different actors in the finance industry operating both in traditional banks as well as FinTech companies are gathered from AML compliance seminars, trainings, as well as non-scientific articles, then analysed in order to create as concrete up-to-date an overview on the topic as possible. In addition, a doctrinal research method is used to suggest a reform on the current directive-based approach in the EU AML legislation.

The first chapter introduces the phenomena of FinTech and defines what is meant by 'FinTech' in the study. The risks associated with financial technologies, a comparison of the business models of FinTechs and traditional banks, as well as a short overview on the development of the financial technology is provided.

The second chapter concentrates on the EU AML regulatory framework after exploring the socio-economic effects of ML, and examining why combating ML is needed. The EU AML Directives, along with the global standards behind them are introduced. The regulatory status of the FinTechs and the challenges this provides to supervisory authorities are examined, as well as the importance and the challenge of the risk-based approach in the current regulatory environment. Finally, challenges related to the current directive-based approach of the EU AML legislation are discussed.

The third chapter explores the identity related AML vulnerabilities associated with on-line-only business models, as well as challenges rising from the FinTech traditional bank interface.

Finally, the fourth chapter explores as well as suggests mitigating actions on the presented FinTech AML vulnerabilities from the perspectives of FinTech service providers, traditional FIs, regulators and the supervisory authorities.

1. THE EMERGENCE OF FINTECH

1.1 Background – the emergence of FinTech

The finance industry is undergoing deep transformation as a variety of innovative alternative financial service providers arise from new technological solutions challenging the current FIs and redefine what is considered as financial services.

"Financial technologies (FinTech) integrate finance and technology in ways that will disrupt traditional financial models and businesses and provide an array of new services to businesses and consumers."[6]

The traditional FIs, such as banks, are also improving technical solutions, such as online banking services and mobile banking apps. However, FinTech companies seem to be a step ahead, providing similar products combined with new business models and 'built-for-digital' new technology with advanced customer experience as well as compatible prices.[7] FinTechs target not only the same customers, but also new customer-bases that are out of reach of traditional banks, thus increasing the financial inclusion in the developing countries and also lowering barriers for entry to efficient banking services for the generation of educated nomad workers commuting between developed countries.[8] This has an opportunity to change the scope and nature of financial services in a ground-breaking way, providing better financial services for everyone.[9]

The overall future impact of the FinTechs on the businesses of the traditional banks is challenging to predict as the change is rapid.[10] In the bigger picture FinTechs represent still a relatively small portion of the financial services on the global markets. However, if looking at specific regional markets, FinTechs already provide a considerably large part of banking services such as M-Pesa

[6] Government Office for Science: FinTech Futures - *The UK as a World Leader in Financial Technologies - A report by the UK Government Chief Scientific Adviser* (2015). Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf, 21 March 2020.
[7] Sironi, P.(2016) My Robo Advisor Was an iPod-Applying the Lessons from Other Sectors to FinTech Disruption. In Barberis, J., Chishti, S. (Eds.) The Fintech Book: The financial technology handbook for investors, entrepreneurs and visionaries, 152-154. Wiley. Referenced in Wu, Y. (2017). Fintech innovation and anti-money laundering compliance, National Taiwan University Law Review, 12(2), 204.
[8] Ibid, 204.
[9] *Basel Committee on Banking Supervision: Sound Practices, Implications of fintech developments for banks and bank supervisors* (2018). Bank for International Settlements, 4. Retrieved from, https://www.bis.org/bcbs/publ/d431.pdf, 14 March 2020.
[10] Ibid, 4.

in Kenya and Tanzania and Alipay in China.[11] Some market observers estimate that especially in retail banking there will be a significant loss in revenue within the coming decade. However some also claim that the traditional banks will absorb or outcompete FinTechs by improving their services and products.[12]

Alternative scenarios for the future for the finance industry include, *inter alia*, the traditional banks growingly digitize themselves in order to enable technology to change their business models, challenger banks such as FinTechs taking over the traditional banks with their advanced cost-effective business as well as obtaining banking licenses, or combinations of the abovementioned such as FinTechs providing advanced customer interfaces for traditional banks or FinTechs with traditional banks sharing the responsibilities on certain services as well as products.[13]

1.2 The variety of activities under FinTech

The trends that are shaping the FinTech landscape currently are resulting from three major evolutionary trends being **"**impacting traditional financial services in global markets, activities in the developing countries, and FinTech start-ups".[14] However, these categorical definitions overlap. The diversity of the innovation is wide and 'FinTech' is considered as an umbrella term, covering a range of business models such as e-wallets, online payment systems, digital bank accounts, virtual currencies, crowdfunding platforms and money transfer services. In this thesis, the term 'FinTech' is used mainly to refer to the so-called 'neobanks' or 'challenger banks' such as FinTech companies operating with a business model providing similar banking services to traditional banks, such as online cross-border accounts, money transfer services or debit cards, with the technology enabled innovations allowing them to operate completely virtually. Service providers

[11] Ibid, 13.
[12] McKinsey & Company: *Global Banking Annual Review* (2015). Retrieved from https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review-2019-the-last-pit-stop-time-for-bold-late-cycle-moves, 14 March 2020.
[13] Basel *Committee on Banking Supervision: Sound Practices, Implications of fintech developments for banks and bank supervisors* (2018). Bank for International Settlements, 4. Retrieved from, https://www.bis.org/bcbs/publ/d431.pdf, 14 March 2020.
[14] Arner, D. W., Bargeris, J., Buckley, R.P. (2016). The evolution of FinTech: A New Post-Crisis Paradigm?, 47 *Georgetown Journal of International Affairs*, 1271, 1272-1219; Arner, D. W., Buckley, R.P. (2011). *From Crisis to Crisis: The global financial system and regulatory failure*. Netherlands: Kluwer Law International. Referenced in Arner, D. W., Bargeris, J., Buckley, R.P. (2017). Fintech, regtech, and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business*, 37 (3), 373.

like this are, for example, Revolut[15], Monzo[16], N26,[17] or Estonian origin Monese[18]. In addition the term FinTech is used to describe the phenomenon of innovative financial technologies.

1.2.1 Comparison to banks

Compared to the traditional banks, FinTechs focus still on a relatively narrow selection of services, although this may be changing as FinTechs rapidly develop their services.[19] To illustrate this, the UK/Belgium based Transferwise of Estonian origin started as an international money transfer service, but soon launched a borderless multicurrency account, with a debit Mastercard linked to it making the business model more towards retail banking services.[20] The company has also launched business services directed at, for example, freelancers and ecommerce firms.[21] Many FinTechs still do not provide services such as loans and investments in the way traditional banks do.[22] Currently, most of the FinTechs do not have banking licences, resulting in the funds not being protected through EU guarantee schemes.[23] Even those that have the banking license or so called 'specialized banking licenses' cannot be considered as banks in the traditional way, for example, as no branches or phone services exist.[24]

It is good to notice that even though the FinTechs may have a power to disrupt the existing business models in the finance industry, the traditional banks and FinTechs are often used in parallel. The use of FinTech does not necessarily result in a customer leaving the bank, but may result in a possible decrease of usage of services and therefore a loss in revenue.[25]

While traditional banks are concentrating on managing the risks at large, investing the customers'

---

[15] Revolut. Retrieved from https://www.revolut.com 15 March 2020.
[16] Monzo. Retrieved from https://monzo.com 15 March 2020.
[17] N26. Retrieved from https://n26.com/en-eu 15 March 2020.
[18] Monese. Retrieved from . https://monese.com/about, 15 March 2020.
[19] Cabell, J., *Fintechs vs. Traditional Banks: Who Has the Bigger Advantage? Retrieved from https://thefinancialbrand.com/84106/fintech-bank-credit-union-competition-advantages/, 15 March 2020.*
[20] Transferwise. Retrieved from https://transferwise.com, 15 March 2020; Transferwise. Wikipedia. Retrieved from https://en.wikipedia.org/wiki/TransferWise,15 March 2020; Transferwise webpage. Retrieved from https://transferwise.com/gb/borderless/#/card,15 March 2020.
[21] Transferwise for Business (New). Retrieved from https://transferwise.com/gb/business/,16 March 2020
[22] Pinot, A., Fintech: Friend or foe to anti-financial crime? *AcamsToday*. (2019) Retrieved from https://www.acamstoday.org/fintech-friend-or-foe-to-anti-financial-crime/, 18 March 2020.
[23] *Deposit Guarantee Scheme* – European legislation protects banks deposits in case of bank failure. European Comission. Retrieved from https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/managing-risks-banks-and-financial-institutions/deposit-guarantee-schemes_en, 21 March 2020.
[24] Revolut: *How we're different from a bank (and what that means for your business)* https://blog.revolut.com/business-what-makes-us-different-from-a-bank-and-what-that-means-for-your-business/
[25] Pinot, A., Fintech: Friend or foe to anti-financial crime? *AcamsToday*. (2019) Retrieved from https://www.acamstoday.org/fintech-friend-or-foe-to-anti-financial-crime/, 18 March 2020.

deposited funds, as well as being under the pressure of filling stringent regulative environment related to operational, strategic and compliance risks, the FinTechs' attention is on a fluent, seamless customer experience and new technological innovation-based products, making the banks steady but slow, whilst FinTechs are agile but not yet fully trusted.

1.2.2 Challenges to the regulator and the supervisors

In addition to the traditional financial service providers, the rapid emergence of FinTechs challenges the regulators and financial supervisory authorities (FSAs) with previously unknown risks that may escape the existing regulation or supervision. This causes a need for the regulative framework governing the financial industry to evolve to in order to respond to that need.[26] The new products, services and business models do not necessarily fit into the existing regulative framework. In addition, the global nature of the FinTechs and the scale of cross-border activities increase the challenges.

The risks associated with FinTechs and the possible shortages on the regulation are diverse. These include customers' data privacy and security risks, inappropriate marketing practices, discontinuity of banking services, as well as cyber-risks, increased interconnectedness between financial parties, volatility of bank funding sources or liquidity risks. This is because FinTechs do not have the minimum capital requirements unless they have banking licenses.[27] This thesis discusses the risks of ML and the rapid emergence of FinTechs expose to the finance industry.

[26] *Basel Committee on Banking Supervision: Sound Practices, Implications of fintech developments for banks and bank supervisors* (2018). Bank for International Settlements, 4. Retrieved from https://www.bis.org/bcbs/publ/d431.pdf, 14 March 2020.
[27] Ibid, 22.

2. ANTI-MONEY LAUNDERING REGULATIVE FRAMEWORK IN THE EU

2.1 Money laundering and its socio-economic effects

Money laundering, in its simplest definition, is to make illegally gained funds to appear like they would derive from legitimate sources. The vulnerabilities of the financial system are used for this activity, resulting in "(…) hundreds of billions of dollars of criminally derived money is laundered through financial institutions, annually."[28] AML is a set of means and measures to combat ML. AML is often considered when including crimes such as tax evasion, terrorist financing, corruption or fraud.

Previously ML was related to cash. This involved placing the cash derived from criminal proceeds into the financial system, making layers of financial transactions to create complexity and finally integrating the funds into the economy, making them appear as legitimately earned.[29] The whole term 'laundering' comes from the gangster Al Capone funnelling cash via laundry service providers to make the funds appear legal.[30] Whilst cash related laundering has not disappeared, new sophisticated methods of laundering have emerged. New technologies are often soon exploited for criminal and malicious purposes, whilst the developing financial technology may provide unexpected opportunities for ML.[31]

ML is an international problem and should be combated globally.[32] Economy has benefited of the growing globalization and the cross-border money flows since the 1990s and the FinTechs follow that path.[33] AML should impose borders to the growing money flows, however it is a resource consuming activity. A number of mitigating actions are required from FIs, supervisory authorities, law enforcement agencies and regulators. It may be asked if AML measures are cost-efficient and

[28] ICA - International Compliance Association: *What is Money Laundering?*. Retrieved from https://www.int-comp.org/careers/your-career-in-aml/what-is-money-laundering/ , 21 March 2020.
[29] Dare, P., Thornhill, S., Howarth, W.B. (2019). *ICA International Advanced Certificate in Anti Money Laundering – Course Manual*. (12th ed.) United Kingdom. International Compliance Association ICA, 6.
[30] Van Duyne, P. C., (2003). *Money Laundering, Fears and Facts.* In Van Duyne, PC., von Lampe, K., Newell, J.L. (Ed.), *Criminal Finances and Organizing Crime in Europe*, Netherlands, 69. Wolf Legal Publishers.
[31] Kasper, A. (2014) *The Fragmented Securitization of Cyber Threats*. In Kerikmäe, T. ed., *Regulating eTechnologies in the European Union – Normative Realities and Trends*. Germany. Springer, 159-165.
[32] Ionescu, L. (2012). Money laundering directives and corruption in the European union. *Contemporary Readings in Law and Social Justice.* 4 (2), 564.
[33] Alldridge, P. (2008). Money laundering and globalization. *Journal of Law and Society*, 35 (4), 437, 458.

worth the effort, but, as the disadvantages of ML are serious, doing nothing is not an option.[34]

ML causes several direct and indirect socio-economic effects on a global level. Amongst others, it places the stability as well as the integrity of the financial system at risk, lowers the trust on FIs, additionally transferring economic power to criminals and their activities.[35] It also decreases revenues for the public sector entities, increases the tax burden on the honest tax payers, distorts investments and savings, as well as artificially increasing prices resulting in unfair competition.[36] Whilst the economical effectiveness is difficult to measure with the amount of money laundered annually being just an estimation (United Nations estimates 2-5% of the global GDP, Europol estimates that 1,28% of GDP of EU being roughly a minimum of 160,000,000,000 Euros per year is connected to ML), the societal effects of not combating the ML are serious as described above.[37]

2.2 The background for the current AML legislation

Currently the primary approach on combating ML is to establish observing and reporting obligations on the relevant financial and non-financial actors. Customer due diligence (CDD) (with customer identification and monitoring the customer behaviour to detect unusual behaviour), reporting to the relevant FSA and Financial Intelligence Unit (FIU), regulation and supervision as well as sanctions are the key elements of the prevention.[38] In addition, the existing AML policies are considered to have a deterrence effect on potential criminals.[39]

Key global standard setters provide a non-binding regulatory framework for ML. The most influential is the Financial Action Task Force (FATF) promoting regulatory and operational measures. It acts as a policy-making body generating political will and bringing legislative

[34] Unger, B., Ferwerda, J., Van Den Broek, M., Deleanu, I. (2014). The Economic and Legal Effectiveness of the European Union's Anti Money Laundering Policy. United Kingdom. Edgar Elgar Publishing Limited, 2.
[35] *The Amounts and Effects of Money Laundering*. A Report for the Ministry of Finance. (2006), 84-95, 160. Retrieved from www.ftm.nl/wp-content/uploads/2014/02/witwassen-in-nederland-onderzoek-naar-criminele-geldstromen.pdf, 2 Jan 2020.
[36] Ibid.
[37] *Money-Laundering and Globalization.* United Nations Office on Drugs and Crime. Retrieved from https://www.unodc.org/unodc/en/money-laundering/globalization.html, 21 March 2020; Satuli, H., *Rahanpesuongelma jäytää Euroopan taloutta ja tilanne pahenee koko ajan – "Heikoin lenkki on nyt tosi heikko",* (2020). Retrieved from https://www.finanssiala.fi/uutismajakka/Sivut/Rahanpesuongelma-jaytaa-Euroopan-taloutta.aspx, 19 March 2020.
[38] Levi, M., Reuter, P. (2006). Money Laundering – Crime & Justice, Vol. 34, 297
[39] Ferweida, J. (2009) The Economics of Crime and Money Laundering: Does Anti-Money Laundering Policy Reduce Crime? *Review of Law and Economics*, 5 (2), 2.

reforms in the area of AML of its member jurisdictions.[40] FATF '40 Recommendations', and revised Recommendations have set out the basis for AML legislation.[41] The recommendations do not have the force of law, but they are implemented in the legislation in several jurisdictions, including the EU. FATF has also recognized AML risks related to innovative financial technologies and published guidance notes on the topic.[42]

2.3 The EU AML legislation – an overview

The EU can be considered as one of the key players developing regulations on combating AML.[43] At the core of the EU AML legislation are the AML directives (AMLDs) (1-5) of The European Parliament and of The Council. The legal basis for the EU to use the secondary legislation on combating ML is set out in the Treaty of Functioning of the European Union (TFEU), Article 83, stating that The European Parliament and the Council may, by means of directives, establish minimum rules concerning particularly serious cross-border crimes that need to be combated on a common basis. ML belongs to the particularly serious crimes described in the Article.[44]

The AML directives that are strongly influenced by the standards of the FATF are based on the TFEU Article 288 which is separately implemented into national jurisdictions of EU member states (MSs) according to the minimum harmonisation requirements. The relevant parts are then further interpreted as internal working rules within FIs, bringing the global AML standards to the everyday reality of the FIs.

The 1st anti-money laundering directive (1MLD) from 1991[45] introduced the main preventative measures such as customer identification, record-keeping and central methods of reporting suspicious transactions. The 2MLD[46] ten years later in 2001, extended the definition of AML to

[40] FATF: *What we do.* Retrieved from http://www.fatf-gafi.org/about/whatwedo/, 2 Jan 2020.
[41] Dare, P., Thornhill, S., Howarth, W.B. (2019). *ICA International Advanced Certificate in Anti Money Laundering – Course Manual*. (12th ed.) United Kingdom. International Compliance Association ICA, 44.
[42] *Discussion Paper on the EBA's approach to financial technology (FinTech).* EBA, 10-11. Retrieved from https://eba.europa.eu/sites/default/documents/files/documents/10180/1919160/7a1b9cda-10ad-4315-91ce-d798230ebd84/EBA%20Discussion%20Paper%20on%20Fintech%20(EBA-DP-2017-02).pdf, 23 March 2020. FATF: *FATF FinTech&RegTech Initiative.* Retrieved from http://www.fatf-gafi.org/fintech-regtech/fatfonfintechregtech/?hf=10&b=0&s=desc(fatf_releasedate), 27 March 2020.
[43] Van Den Broek, M. (2014). Designing supervision under the Preventive anti-Money laundering Policy in the European Union. *Utrect Law Review*, 10 (5), 151.
[44] Graig, P., De Burca, G. (2015). *EU Law: Text, Cases, and Materials.* 6th ed. United Kingdom. Oxford Press, 966.
[45] Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering
[46] Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering

include underlying offences such as corruption, as well as enlarged the scope to money transmitters and investment firms. The 3MLD[47], made a change towards tightening the EU's AML regime and introduced a risk-based approach (RBA), shifting responsibility to the FIs, demanding a higher outcome of AML effectiveness.[48]

Currently the EU AML regulative framework is built around the 4th and 5th AMLDs. The 4MLD[49], was launched on May 2015 and the update was done shortly afterwards, as a form of the 5MLD[50], specifically with the aim of preventing financial systems being used for terrorist financing (TF), after the Paris terrorist attacks on 2015. From the FinTech point of view the relevant amendment in the 5MLD was that the scope of the directive was increased *inter alia* to cover virtual currency exchanges and virtual wallets. Other main topics in the 5MLD included the register of the ultimate beneficial owners (UBO) and strengthening the cooperation of supervisory authorities and FIUs by improving the exchange of information.[51]

The current EU AMLDs impose obligations on a variety of financial service providers, such as an obligation to identify the customer, verify the identity, obtain information about the nature as well as the extent of the customers' activities including the purpose of using the services and products. In addition to monitoring the use of products and services, detecting unusual behaviour and filing suspicious activity reports (SARSs) to the relevant FIU in case of suspected unusual behaviour referring to ML is also required.[52] The 4MLD also gives emphasis on the RBA which was introduced in the 3MLD. The importance and the challenge of the RBA from the FinTech perspective is discussed further in chapter 2.5.

[47] European Parliament and of the Council of 26 October 2005 Directive 2005/60/EC of the on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

[48] Meklin, H. (2018), AML risks and challenges at the time of crypto currencies. *L'Europe Unie / United Europe*, 13, 61.

[49] European Parliament and of the Council of 20 May 2015 Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

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

[51] Hanley-Giersch, J., Status of the European AML Framework. (2019) *AcamsToday*. Retrieved from https://www.acamstoday.org/status-of-the-european-aml-framework/, 21 March 2020.

[52] Satuli, H., *Rahanpesuongelma jäytää Euroopan taloutta ja tilanne pahenee koko ajan – "Heikoin lenkki on nyt tosi heikko",* (2020). Retrieved from https://www.finanssiala.fi/uutismajakka/Sivut/Rahanpesuongelma-jaytaa-Euroopan-taloutta.aspx, 19 March 2020.

2.4 FinTechs in the EU AML Framework

2.4.1 Obliged entities

According to the EU 4MLD, the AML measures described in the directive apply to all the 'obliged entities' for the purpose of the Article 2 including *inter alia* financial institutions and credit institutions. All service providers belonging under the definition of obliged entities are required to comply with the AML measures of the directives. The Article 2 is further amended in the Article 1 of the 5MLD, increasing the scope of the obliged entities *inter alia* to virtual currency exchanges. The AMLDs do not state a clear regulatory standpoint for FinTechs and they do not distinguish between FinTechs and non-FinTechs.[53] This is understandable when discussing an umbrella term with a variety of different business models.

A challenging point is whether the FinTech business model fits the classification of obliged entities. The classification of 'financial institution' may vary according to the national legislation of the MSs. The FATF has provided guidance on the classification of 'financial institution' and the activities that should be covered for AML purposes. FATF suggests that providers of the new payment products and services (NPPS) would fall within the classification of FI "(…) by conducting money or value transfer services, or by issuing and managing a means of payment."[54] According to the guidance the abovementioned services should be subject to the AML measures such as CDD, record keeping or reporting of suspicious transactions.

The AML obligations each FinTech company has to comply with therefore partly depends on the interpretations of the definition and classification on the previous terms in every MS. The consequence of this is that the some FinTech businesses may or may not be designated as 'obliged entities' in different MSs, even if they provide similar services. This may lead to regulatory arbitrage and create vulnerabilities from AML perspective. In addition, the practice may distort the competition as similar services and products are offered by companies that have or have not certain obligations.[55]

---

[53] *Discussion Paper on the EBA's approach to financial technology (FinTech).* EBA, 10-11. Retrieved from https://eba.europa.eu/sites/default/documents/files/documents/10180/1919160/7a1b9cda-10ad-4315-91ce-d798230ebd84/EBA%20Discussion%20Paper%20on%20Fintech%20(EBA-DP-2017-02).pdf, 23 March 2020.

[54] FATF: *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services.* (2013), 11-13. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf, 23 March 2020.

[55] *Discussion Paper on the EBA's approach to financial technology (FinTech).* EBA, 10-11. Retrieved from https://eba.europa.eu/sites/default/documents/files/documents/10180/1919160/7a1b9cda-10ad-4315-91ce-d798230ebd84/EBA%20Discussion%20Paper%20on%20Fintech%20(EBA-DP-2017-02).pdf, 23 March 2020.

2.4.2 Licenses

FinTechs may not have the same regulatory status as traditional banks and are therefore not obliged to comply with as stringent AML measures. However they do not operate in 'the wild west'. The challenger banks that this study mainly concentrates on are under very similar regulative scrutiny to traditional banks.

In order to provide financial services in the EU, the operators are required to approach a local FSA (for example in Finland "Finanssivalvonta"[56] and in Estonia "Finantsinspektsioon"[57]) to apply for a relevant license and to register themselves as supervised entities. Those registered in another MS need also to submit a notification for the FSA of the country that they provide their services in.

Licenses that FinTechs described in this study currently use are those such as Electronic Money Licenses (EMIs), different Payment Institution (PI) or Payment Service Provider (PSP) licenses. Some FinTechs also have banking licences or 'specialized banking licenses' with, *inter alia*, smaller capital requirements than the regular banking license, but having a banking license does not make FinTech a bank within the meaning of traditional banks.[58]

FinTechs with EMI, PI or specialized banking licenses are in many EU jurisdictions mostly considered as 'obliged entities' within the meaning of the EU AMLDs, and therefore in theory are bound by the same AML obligations as traditional banks. In Finland, for example, the Act on Payment Institutions regulates different payment services, payment institutions, electronic money issuance and electronic money institutions with some exceptions.[59] According to the Act on Financial Supervision[60], the aforementioned authorized service providers are supervised by Finland's FSA Finanssivalvonta, with the Act on Prevention of Money Laundering and Terrorist Financing being applied for all the entities supervised by Finanssivalvonta.[61] The application 'in theory' refers to a different interpretation and application of the required measures due to the RBA. This is further discussed in section 2.5.

---

[56] FIN-FSA, Financial Supervisory Authority: *Authorisations, registrations and notifications in the financial markets*. Retrieved from https://www.finanssivalvonta.fi/en/banks/authorisations-registrations-and-notifications/, 19 March 2020.

[57] Finantsinspektsioon: *Applying for an operating license in payment services*, Retrieved from https://www.fi.ee/en/payment-and-e-money-services/applying-operating-licence-payment-services, 20 March 2020.

[58] *Lithuanian finance institution – licensing solutions for FinTech companies providing services in single European market*, Ecovis, https://ecovis.lt/lithuanian-finance-institution-the-licensing-solution-for-foreign-companies-providing-services-in-single-european-market/; *Authorisation of Banks.* Bank of Lithuania. https://www.lb.lt/en/authorisation-of-banks#ex-1-2, 9 May 2020.

[59] Maksulaitoslaki 30.4.2010/297 Chapter 1, Article 1.

[60] Laki Finanssivalvonnasta 19.12.2008/8780

[61] Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444

The challenge for both FinTechs and the supervisors are the divergence in the required licenses in MSs. It can be challenging for a FinTech start-up, considering the constant development of the products and the technology used, to be fully aware on what license it should have and what AML measures applies to their exact service. Due to the fact that the local FSA is responsible for the supervision of an entity it has licensed, regardless of the type of the license, it may also provide interpretations of what measures are sufficient for the entity. European Banking Authority (EBA) has noted a need to explore further how the divergence in the classification of the FinTechs for AML purposes influence the risk of ML/TF in the internal market.[62]

For the supervisor, the licensing scheme as well as the cross-border nature of FinTechs causes challenges. The passporting mechanism enables financial service providers that are registered in one state in the European Economic Area (EEA) to operate in other EEA states, either by establishing branches or providing cross-border services.[63] After registering and receiving a license from a local FSA in one EEA Member State, the company is allowed to operate within the whole EEA. This is practical for FinTechs that by nature are cross-border-oriented, as finding a jurisdiction providing an operational environment with less stringent AML legislation can be beneficial from a business point of view. From the perspective of the FSA and the effective supervising, the passporting mechanism causes challenges, as the license may be acquired in one state, the supervisor located in another, with the main activities of the FinTech take place in one or multiple other EEA state(s).[64]

2.4.3 Self-regulation through the chain of supervised entities

Keeping a good reputation may encourage FinTechs to implement stringent AML compliance procedures.[65] As FinTechs need to partner with traditional banks, they may self-regulate themselves using more stringent AML procedures than required from them by legislation in order to attract good co-operating partners. As an example, banks process FinTechs' transactions and the FinTech may use its account in a bank for cash pooling or storing the customer funds. The partner bank may also require it from them. Whilst practical experience from the FinTech field

[62] *Discussion Paper on the EBA's approach to financial technology (FinTech).* EBA, 55. Retrieved from https://eba.europa.eu/sites/default/documents/files/documents/10180/1919160/7a1b9cda-10ad-4315-91ce-d798230ebd84/EBA%20Discussion%20Paper%20on%20Fintech%20(EBA-DP-2017-02).pdf, 4 May 2020.
[63] Law, J. J. (Ed.). (2018). *Dictionary of Finance and Banking.* (9th ed.) United Kingdom. Oxford University Press, 359; EBA: *Passporting and supervision of branches.* Retrieved from https://eba.europa.eu/regulation-and-policy/passporting-and-supervision-branches, 18 April 2020.
[64] Pinot, A., Fintech: Friend or foe to anti-financial crime? *AcamsToday.* (2019) Retrieved from https://www.acamstoday.org/fintech-friend-or-foe-to-anti-financial-crime/, 18 March 2020.
[65] Magnusson, W. (2018). Regulating FinTech. *Vanderbilt Law Review*. 7 (4), 1210.

shows that the self-regulation may be still be "dubious"[66], it can be seen that the effect of the EU AMLDs is also based on the chain of supervised entities, resulting in the AMLDs reaching further than the entities defined within the scope of directives.[67] Even though the FinTech would not directly receive a higher level of regulatory scrutiny from the FSA, it may obtain it indirectly from the partner banks who are obliged to follow more stringent AML regulation.[68]

2.5 Risk-based approach

2.5.1 Introduction to the RBA

RBA is currently the overall design of the AML since the 3MLD.[69] Risk was mentioned already in the FATF 40 recommendations.[70] FATF also published a series of guidance papers on RBA in 2007 to assist different sectors to create a common understanding on the subject.[71] EU introduced RBA to replace the rule-based approach (which produced some insufficient information) at the 3MLD and amended it in the 4MLD.[72] What does RBA mean?

The aim of the majority of crimes is to make money in some way. In order to do that, criminals have to manage the risk of not getting caught while performing the crime or dealing with the proceeds afterwards. A balance between the profit and the risk of getting caught is needed, as is the constant tracking of opportunities to exploit the weaknesses of the financial system.[73] Accordingly, the financial service providers have to be wise and proportionate in managing the risks. In the event that the risks related to certain business model are not properly assessed, the costs of AML would be disproportionate with the requirements for the service provider and its customers overburdensome resulting in the actual risks not being understood and suspicious behaviour not detected.[74]

---

[66] Money Laundering Reporting Officer of SONECT. Pinot, A. Author's interview. Transcript. 25 March 2020.
[67] Chief AML & Sanctions Processing Specialist at Nordea, Vuorinen, M. Author's interview. Transcript. 23 March 2020.
[68] Financial Crimes Risk Specialist at Transferwise, Schnieder, M. Author's interview. 23 March 2020.
[69] Pellegrina, L., Masciandaro, D. (2009). The risk-based approach in the new European anti-money laundering legislation:law and economics view. *Review of Law and Economics,* 5 (2), 931.
[70] Ibid, 932.
[71] FATF: *Risk-Based Approach - 18 publications*. Retrieved from http://www.fatf-gafi.org/documents/riskbasedapproach/?hf=10&b=0&s=desc(fatf_releasedate), 12 March 2020.
[72] Pellegrina, L., Masciandaro, D. (2009). The risk-based approach in the new European anti-money laundering legislation:law and economics view. *Review of Law and Economics,* 5 (2), 932.
[73] Dare, P., Thornhill, S., Howarth, W.B. (2019). *ICA International Advanced Certificate in Anti Money Laundering – Course Manual*. (12th ed.) United Kingdom. International Compliance Association ICA, 101.
[74] Ibid, 101.

"The risk-based approach means a focus on outputs. Firms that apply a risk-based approach to anti-money laundering (AML) will focus AML resources where they will have their biggest impact.

Firms must have in place policies and procedures in relation to customer due diligence and monitoring, among others, but neither the law nor our rules prescribe in detail how firms have to do this. Firms' practices will vary depending on the nature of the money-laundering risks they face and the type of products they sell. For example, a large retail bank with many customers will likely to need to develop or purchase customer monitoring software, but a smaller organisation may be able to monitor its customers using a low-tech solution.

Firms applying a risk-based approach need to be proactive in seeking out information about money-laundering trends and threats from external sources, such as law enforcement, as well as relying on their own experiences and observations. This allows firms to effectively review and revise their use of AML tools to fit the specific risks that they face."[75]

2.5.2 Applying the RBA

RBA requires the financial service providers to be aware of the risks related to the nature of their company, jurisdiction, geographical location, the national risk profile as well as consider the risks that their business idea, services, products and delivery channels are exposed to. Additionally they will need to consider what types of customers are served and how they are acquired.[76] The RBA requires business strategic thinking and continuous evaluation of the emerging criminal trends as well as the senior management's decisions on the tolerated risk level.[77] The challenge is that there are no clear rules or no 'one-size-fits-all' approach, but every company has to continuously assess the risks itself. From the RBA perspective, it is not proportionate to require as stringent a regulatory scrutiny from a small FinTech start up, as it is from a large, established FI.

This is where the dissimilarities in the otherwise similar looking EU AML obligations may rise, creating possible AML vulnerabilities for FinTechs. Criminals search for most favourable and less risky ways to enter to the financial system. In the event that a company applies less stringent AML measures due to its size or does not yet fully understanding the risks associated to its products, a

[75] *Money laundering and terrorist financing*. (2015/2020). Financial Conduct Authority (FCA) UK. https://www.fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing,12 March 2020.
[76] Dare, P., Thornhill, S., Howarth, W.B., *ICA International Advanced Certificate in Anti Money Laundering – Course Manual.* (2019). (12th ed.) United Kingdom. International Compliance Association ICA, 111.
[77] Ibid, 101.

new opportunity for customers wishing to launder their illicit funds appear. It also has to be noted that FinTechs may knowingly seek for this type of customers. They may have a higher risk tolerance, for example when wanting to grow, purposefully applying looser standards for acquiring customers and then only start to get stricter when the company grows.[78] RBA does enable this approach to the point, even though its aim is to prevent ML in the most effective way.

2.6 Directive-based approach

The current EU AML legislation, as described in section 2.3, is directive-based, establishing only minimum requirements for the legislation in the MS's jurisdictions. Each MS has freedom to decide how to comply with the requirements as a part of its national legislation. This allows national deviation and creates possible loopholes. The same thing can be prohibited, permitted or compulsory, depending on a MS.[79] It is said that "(…) the success of many fintech firms is tied to the firm's ability not only be on head of the technological curve but also to have the flexibility to adapt to an evolving set of laws and compliance obligations."[80] From the FinTechs' perspective, the deviation and the loopholes of the national legislations may be difficult to comply with, but they can also provide beneficial opportunities from the business as well as ML perspective.

Considering the global nature of ML, rapidly developing technological innovations and new FinTech business models, as well as the directive-based approach enabling variation in the AML legislation at the national level (*inter alia*, how the EU AMLDs are interpreted as well as under which licences and legislation FinTech business models are classified), the directive-based approach may not be the best solution for effectively combatting the ML in the EU.

A recent initiative for action towards solving the problem on the deviation in the national AML legislation in the EU has been taken by the Center of European Policy Studies (CEPS), which has established a multinational working group to investigate new measures to combat the ML.[81] One

[78] Chief AML & Sanctions Processing Specialist at Nordea, Sillanpää, P. (17 April 2020). *Training on Payment Service Providers;* Bilkstys G.E., Kanapienis, L., Pinot, A., Schnieder, M. (2020, 5 March) *The Risks and Opportunities of Technology*. ACAMS Anti-Financial Crime Symposium – Baltics, Riga, Latvia.
[79] Satuli, H., *Rahanpesuongelma jäytää Euroopan taloutta ja tilanne pahenee koko ajan – "Heikoin lenkki on nyt tosi heikko",* (2020). Retrieved from https://www.finanssiala.fi/uutismajakka/Sivut/Rahanpesuongelma-jaytaa-Euroopan-taloutta.aspx, 19 March 2020.
[80] Douglas, J. L., (2016) New Wine into Old Bottles: Fintech Meets the Bank Regulatory World. *North Carolina Banking Institute*, 20, 17-66.
[81] Satuli, H., *Rahanpesuongelma jäytää Euroopan taloutta ja tilanne pahenee koko ajan – "Heikoin lenkki on nyt tosi heikko"*, (2020) Finanssiala.fi, Retrieved from https://www.finanssiala.fi/uutismajakka/Sivut/Rahanpesuongelma-jaytaa-Euroopan-taloutta.aspx, 19 March 2020.

topic on their list is whether the EU AML legislation should be changed from directive-based to regulation-based. As in the EU law the regulations are binding, so the regulation-based AML legislation would create more consistency across the MSs.[82]

[82] Ibid.

3. FINTECH AML VULNERABILITIES

The main AML vulnerabilities associated with the FinTechs are those related to the verification of the customer identity. FinTechs, based on the RBA, may decide to use the minimum requirements for the customer identification. The businesses are fully digitalised and an account can be opened in minutes without the company ever meeting the customer. This invites fraudsters and increases the impersonation fraud risk.[83] Fake identities are used also in traditional banks, but the non-face-to-face identification according to the FATF Recommendation 8 is a 'specific' ML risk.[84] To illustrate this, London FinTech FinCrime Exchange Survey 2019 showed that fake identities accounted for 26% of all financial crime risk typologies in virtual banking.[85]

The possibility for a customer to open the services on-line within minutes enables criminals to easily open multiple accounts and rapidly increase the volume of illicit funds entering the financial system.[86] Even if the identity used for registration was real, the easiness in registration, speed of transactions and the increasing amount of service providers in the industry, often used in parallel, creates challenges to monitor the movements of funds.[87] Also, the 'normal activity' of the customer is difficult to define due to the lack of customer data.

3.1 CDD

Proper CDD is the key for every financial service provider in order to prevent ML/TF through their company. CDD enables the financial service provider to rate the risk factors related to a customer and assess if the customer can be accepted.[88]

The EU AMLDs give the framework for CDD. RBA is applied also to CDD, as described before, due to the need for proportionality, to understand risks and to assess possible mitigating actions.[89]

The 4MLD, Articles 10-17 provide general provisions for the CDD. Article 13 describes what the

[83] Dare, P., Thornhill, S., Howarth, W.B. (2019). *ICA International Advanced Certificate in Anti Money Laundering – Course Manual*. (12th ed.) United Kingdom. International Compliance Association ICA, 271.
[84] Ibid, 271.
[85] London FinTech FinCrime Exchange Survey. Retrieved from https://www.fintrail.co.uk/ffe, 17 March 2020.
[86] Ibid.
[87] Dare, P., Thornhill, S., Howarth, W.B. (2019). *ICA International Advanced Certificate in Anti Money Laundering – Course Manual*. (12th ed.) United Kingdom. International Compliance Association ICA, 271.
[88] Dare, P. (2020, 17 March). *ICA International Advanced Certificate in Anti Money Laundering Workshop 2*. Virtual workshop.
[89] Ibid.

CDD of the obliged entities shall comprise. This includes identifying the customer and verifying their identity on the "basis of documents, data or information obtained from a reliable and independent source".[90]

In addition, the requirements comprise *inter alia*: Assessing the customer profile (i.e What is the purpose and the nature of relationship?) The UBO (i.e Can they be identified and do they have a real connection to the customer? What is the source of the funds and wealth? Is it a salary, from another bank, or is it from the business?)[91] Further in the 4MLD, articles 18-24 describe the requirements on the enhanced due diligence (EDD) for higher risk customers, regarding *inter alia* recognizing the politically exposed persons (PEPs) or dealing with customers from high risk jurisdictions and applying stricter measures on them.[92]

3.1.1 Registration, ID collection and verification

The customer registration, ID collection and the verification are the first steps in the CDD process. This is to confirm the identity of the customer and to verify they are who they claim to be. This is also where the questions may rise in relation to the interpretation and practical application of RBA. The AMLDs do not specify how exactly the verification should be done, other than based on relevant reliable documents.[93] The verification can be done based on the risk-assessment of the service provider, traditionally by meeting the customer at the branch office, collecting and verifying the ID-documents face-to-face. FinTechs usually fulfil their customer identification and verification obligation by asking the customer to install the required app, then sending a picture of themselves and their ID. Services are opened on-line from any location. After this, the account is in use via mobile device within minutes.

Currently some traditional banks in the EU also provide remote on-line registration to some extent, often with the help from technology developed by FinTechs providing RegTech solutions, technology used for regulatory processes such as complying with the AML measures, for other FIs.[94]. However, if the customer is not local, the banks require documents such as residency permit,

[90] European Parliament and of the Council of 20 May 2015 Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, Article 13.
[91] Ibid. Articles 10-17.
[92] Ibid Articles 18-24.
[93] Gangull, I., Actelik, O., Kohling, L., Mauhs, FM. (2009). The Third AML-directive: Europe's response to the threat of money laundering and terrorist financing: Part ii. *Banking Law Journal*, 126 (8), 731.
[94] *Fully digitised opening of a bank account is available from anywhere in the world now.* Luminor. Retrieved from https://www.luminor.lv/en/news/fully-digitised-opening-bank-account-available-anywhere-world-now, 2 May 2020.

proof of regular income by an employment contract or account statements from the past six months, or a proof of an address such as paid utility bills. This is to fulfil their obligation to know their customer and the purpose of the customer's need for banking services in the country in question. This may restrict customers that are non-local or recently relocated to a country in opening an account, even though EU-citizens by default have a right to open a bank account in another EU MS.[95] This difficulty has also been an inspiration for FinTech businesses. A founder, of Estonian origin, of FinTech Monese, when moving to UK, was not able to open an account in a bank due to the non-existing credit history and utility bills proving the local address. This inspired him to establish an on-line bank.[96]

Being virtual and cross-border by default, a requirement of being a resident of a specific country does not exist for FinTechs. One can open as many accounts as there are providers, from anywhere in the world, as long as one has an internet connection. In addition to increasing financial inclusiveness and easy access to banking services, this simple registration also increases opportunities for those using the service for criminal purposes. A criminal has a good opportunity to place large amounts of funds rapidly into the financial system without it being easily recognized.[97]

3.1.2 Fake identities

Faking an identity is not only a FinTech related issue as anyone can bring a fake passport to a branch or buy a fake document from the Internet enabling them to pass the Know-Your-Customer on-boarding process of a traditional bank.[98] However, with FinTechs you really never meet the customers face-to-face. When everything from the registration to all transaction activities are done virtually or using ATMs, the FinTech can never be sure who the customers really are and the possibility for the use of fake identities is increased.

Some identity risks are for example: Counterfeiting involves forged ID or documents, such as use of a same face in multiple documents or combining fake ID and real secondary information. Theft, as a real physical theft of IDs or on-line theft, finding a copy of a passport or stealing personal data online. Identities can also be purchased, for example in the lower GDP countries by offering money

[95] EU: *Pankkitili toisessa EU-maassa*. Retrieved from https://europa.eu/youreurope/citizens/consumers/financial-products-and-services/bank-accounts-eu/index_fi.htm, 29 April 2020.
[96] Monese. https://monese.com/about 29 April 2020.
[97] Pinot, A., Fintech: Friend or foe to anti-financial crime? AcamsToday. (2019) Retrieved from https://www.acamstoday.org/fintech-friend-or-foe-to-anti-financial-crime/, 18 March 2020.
[98] Replace Your Documents Retrieved from https://www.replaceyourdoc.com, 17 March 2020.

for taking a picture of a person and their ID. The purchased identities enable for example an easy, parallel opening of multiple accounts. Virtual phone numbers, office addresses or IPs are also used to mask the real identity.[99]

On the other hand, FinTechs may possess well developed RegTech to acquire additional data of the customers which may improve FinTech CDD processes, and even exceed the traditional bank process at some point.[100] It can still be concluded that currently, the non-face-to-face identification due to the virtual nature of the FinTechs and the use of the minimum requirements for identification, produces an increased risk for the use of fake identities as well as a risk of the FinTechs being used for ML/TF purposes.

3.1.3 Assessing and monitoring the customer behaviour

The outcome of the CDD for the company is to be able to rate the risk factors related to the customer. In addition to verifying the customer's identity, the company, during the on-going business relationship, needs to assess what is considered usual or unusual behaviour for the customer. In case unusual behaviour that does not have business rationale is detected and there is a reason to believe the activity contains ML, the company is required to file a SAR to a relevant FIU.[101] The CDD information also enables the company to assist the law enforcement when the SAR is filed.[102]

The assessing of the customer behaviour is done by monitoring the customer's transactions by automated transaction monitoring systems and manually, in order to detect and asses the unusual behaviour in relation to the customer profile. The risk indicators pointing to the FinTech being used for ML/TF purposes can be for example that the customer profile does not match the products used, such as elderly customers (not known to be particularly technology-savvy) using the service for gaming or purchasing cryptocurrencies which themselves contain high risk due to the anonymity associated to the product.[103] A suspicion may also arise if the customer registered a residence in a certain area, but the technology shows that the device using the service is located

[99] Wright, M. *An insight into virtual banking*. A recording from the International Compliance Association's 2nd APAC conference. Retrieved from https://www.int-comp.org/cpditem/?product=Aninsightintovirtualbanking, 18 March 2020.
[100] Ibid.
[101] International Compliance Association: *What is Customer Due Diligence (CDD)?* Retrieved from https://www.int-comp.org/careers/your-career-in-aml/what-is-customer-due-diligence-cdd/, 18 March 2020.
[102] Ibid.
[103] Dare, P., Thornhill, S., Howarth, W.B. (2019). *ICA International Advanced Certificate in Anti Money Laundering – Course Manual*. (12th ed.) United Kingdom. International Compliance Association ICA, 271.

somewhere completely unrelated, pointing towards possible impersonation fraud. High-value transactions may be a risk indicator, especially if the same customer performs them from multiple accounts.[104] Frequent small value transactions may point to TF, or for the customer or 'a money mule', someone hired or tricked to help the criminal, to enter illicit funds into the financial system, especially if the money is rapidly transferred forward.

The challenge for FinTechs to detect unusual behaviour is that when the service and products are new, the understanding how they can be misused is limited. This, combined with a limited amount of customer data due to a simple registration process, creates a challenge to truly assess what is 'normal' for the customers. When considering FinTechs that provide payment services, the transactions may be moving through different intermediaries, including cross-border, making it difficult to fully track the transactions and recognize patterns related to them.[105]

In the event that the customer acquisition is aggressive (as it could be for a start-up FinTech wanting to grow and gain larger market share), the new customers are taken with limited CDD, then combined with the cross-border nature of the FinTechs, the resulting risk of the FinTechs not knowing their customers, their purpose of using the service, or how their usual business activities look like, is high.

In US, Financial crimes enforcement network (FinCEN) -cases against FinTechs, shows evidence of the FinTechs' reluctancy to comply with required CDD. Ribble Labs Inc., providing payment network for consumers and merchants, received a fine of 700,000 US Dollars for failing to know their customer and letting through certain transactions including for example a transaction of 250,000 US Dollars from a customer that had been convicted on a crime of selling explosives.[106]

A notable risk is FinTechs intentionally focusing on the risky customers that may have been exited from the traditional banks due to the stringent AML measures. In the EU, FinTechs can provide sophisticated solutions for ML for the customers wanting for example to transfer funds from the East to European markets.[107] This is a service, that the traditional banks are not able to provide anymore on a large scale.

[104] Ibid.
[105] Chief AML & Sanctions Processing Specialist at Nordea, Sillanpää, P. (17 April 2020). *Training on Payment Service Providers.*
[106] Wu, Y-T. (2017). FinTech Innovation and Anti-Money Laundering Compliance. *National Taiwan University Law Review*, 12 (2), 234.
[107] Bilkstys, G.E., Kanapienis, L., Pinot, A., Schnieder, M. (2020, 5 March) *The Risks and Opportunities of Technology*. ACAMS Anti-Financial Crime Symposium – Baltics, Riga, Latvia.

3.2 The FinTech AML vulnerabilities exposure on traditional banks

As discussed previously in the section 2.4.3, FinTechs need to partner with traditional banks as the banks need to for example process FinTech transactions and store their funds. The result is that whilst FinTechs may more use stringent AML measures than required, traditional banks may also be exposed to FinTech AML vulnerabilities. Accepting a FinTech as a customer means that the bank moves to an area where it otherwise is reluctant to go. The bank becomes exposed to customers it would not usually accept, such as individuals with no link to the country, or the customers not identified face-to-face.

In general, by providing correspondent banking services for another traditional bank, bank becomes exposed to the risks of the partner bank with customers that the bank itself do not know. In the case of having a FinTech as a customer, the risk is on a different level. The customer-base is new and the uncertainty related to the sufficiency of the other party's AML procedures is increased.

Additionally, due to the constantly developing nature of FinTech businesses, it may happen that the business of the FinTech the bank has accepted as a customer, evolves after the details of the collaboration is negotiated.[108] New products may be introduced and new customer-bases may be acquired, as although involving a bigger risk, being first in a market with a new product, opens a possibility to new customers and bigger returns.[109] Due to the fact that the whole concept of the FinTechs is the re-thinking of the financial services, the provision of choices for the customers, new products, services and the customer-bases may rapidly emerge, resulting in the FinTech company's business model to go beyond the bank's risk appetite.

The relationship with FinTech customers should be evaluated constantly. The product management teams develop new products all the time and the first thing on their mind is not necessarily the financial crime risks the product is exposed to. FinTechs should by default be considered as high risk customers for traditional banks and to be under EDD in order to mitigate the overall risk of money laundering.[110]

A bank needs to ask if there is anything it can do to evaluate the risk coming with the FinTech.

[108] Ibid.
[109] Kobor, E. S. (2013). The role of anti-money laundering law in mobile money systems in developing countries. *Washington Journal of Law, Technology & Arts.* 8 (3), 306.
[110] Bilkstys, G.E., Kanapienis, L., Pinot, A., Schnieder, M. (2020, 5 March) *The Risks and Opportunities of Technology*. ACAMS Anti-Financial Crime Symposium – Baltics, Riga, Latvia.

One option could be to evaluate the corporate culture of the FinTech when negotiating the collaboration with corporate representative such as by asking how does their attitude towards business and financial crime look. Unwanted attitudes and risks coming with it may be recognized in the discussion.[111] Secondly, viewing how the business is built may give a direction, such as asking whether the business answers to a true need that the customer has, what problem does it solve (for example an access to a banking services such as Monese or affordable transfer prices by Transfewise) or whether the business is created just to make profit in any possible way.[112] If the FinTech is focused on a certain customer area, this may also provide help to assess the risk exposure. These measures may give some guidance for a bank to evaluate whether a FinTech fits their risk-appetite and how widely the FinTech expose the banks to new ML risks. One suggested way to recognize a FinTech with proper AML processes is to select one that has already received a fine for not complying as the procedures should be better in place.[113]

[111] Murat, Y. (2020, 5 March) *Correspondent Banking Relationships and De-Risking.* ACAMS Anti-Financial Crime Symposium – Baltics, Riga, Latvia.
[112] Bilkstys, G.E., Kanapienis, L., Pinot, A., Schnieder, M. (2020, 5 March) *The Risks and Opportunities of Technology*. ACAMS Anti-Financial Crime Symposium – Baltics, Riga, Latvia.
[113] Ibid.

4. MITIGATING ACTIONS

4.1 Public-private-partnerships (PPP)

When mitigating the risks related to the AML vulnerabilities of FinTechs the key elements are 'understanding', 'knowledge-sharing' and 'collaboration'. New technological innovations, disruptive ways of thinking of financial services, FinTech interfacing with traditional banks, increasing financial inclusiveness, cross-border services, regulations that need to change to serve the new business models, and supervisors trying to get an overview on different business models taking place in several jurisdictions provide a challenge for all parties such as regulators, supervisors (private and public sector authorities), traditional banks and FinTech companies when aiming to combat ML. "Coordinating is important - to get the right people to discuss with each other", as the head of Latvian FIU, Ilze Znotina states it.[114] All parties have different perspectives and access to the needed information so well-functioning PPPs are in a key position.

4.2 Regulatory sandboxes

From the FinTech perspective, working with a regulator that understands the FinTech industry is a key for a less risky environment.[115] Due to the fact that the FinTechs are pioneering the new forms of financial industry and developing ideas that no-one has yet experience in, it is understandable that rules of conduct are still being established.[116] In order to be able to design effective regulations as well as supervise efficiently, the regulators and supervisors need to constantly be able to evaluate, identify as well as assess risks related to not only the business models and technology of the evolving FinTechs, but also to the whole phenomenon being the disruptive transformation that is taking place within the finance industry.[117]

The 'sandbox' concept originates from a report of UK's Financial Conduct Authority (FCA) from the year 2015 that proposed an idea of creating a testing environment for new businesses before

[114] Znotina, I., (2020, 5 March) *Regulatory Roundtable on Financial Crime Prevention*. ACAMS Anti-Financial Crime Symposium – Baltics, Riga, Latvia.
[115] Bilkstys, G.E., Kanapienis, L., Pinot, A., Schnieder, M. (5 March, 2020) *The Risks and Opportunities of Technology*. ACAMS Anti-Financial Crime Symposium – Baltics, Riga, Latvia.
[116] Magnusson, W. (2018). Regulating FinTech. *Vanderbilt Law Review.* 7 (4), 1209.
[117] Ibid.

entering the market.[118] The regulatory sandboxes provide financial service providers with an environment where the new innovative solutions can be tested with the support of an authority with the aim of giving business owners and developers time to evaluate as well as validate their business models.[119] The concept also works the other way round for regulators and supervisory authorities in order to gain understanding of the evolving businesses.

Lithuania has managed to create a FinTech friendly regulative environment with the active cooperative role of the Bank of Lithuania which combines both central bank and FSA functions. It has launched also a successful regulatory sandbox for FinTechs aiming to establish businesses in Lithuania, to try out their business ideas and to gain general knowledge on "financial ecosystem, legal issues and regulation".[120] The central bank has also simplified the regulatory procedures for FinTechs.[121] Operating as a supervisory authority and managing the sandbox, the bank gets a good overview on the FinTechs it is supervising, as well as learning to understand their business models. However, the question still remains as to whether the resources of a central bank are really sufficient for effective supervision for the growing FinTech field.

An addition to FinTech regulatory sandboxes is 'SupTech' which is a specific supervisory technology. This is seen as something that could further improve the efficiency on the regulatory rulemaking process, making the regulatory sandboxes 'supervisory control boxes'.[122] The idea is new and is open for further research.

4.3 Traditional bank - FinTech collaboration

There is a question as to whether traditional banks should be in the role of trainers for smaller financial service providers and whether this would mitigate the risks on both sides. Banks could provide their currently superior and more thorough knowledge on AML that they have gained due

[118] FCA: *Regulatory sandbox.* (2015). Retrieved from https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf, 2 May 2020.
[119] *Discussion Paper on the EBA's approach to financial technology (FinTech).* EBA, 10-11. Retrieved from https://eba.europa.eu/sites/default/documents/files/documents/10180/1919160/7a1b9cda-10ad-4315-91ce-d798230ebd84/EBA%20Discussion%20Paper%20on%20Fintech%20(EBA-DP-2017-02).pdf, 23 March 2020.
[120] Turp, G.: Emerging Europe: *Sandbox success cements Lithuania's reputation as fintech hub.* Retrieved from https://emerging-europe.com/new-industry/sandbox-success-cements-lithuanias-reputation-as-fintech-hub/, 4 May 2020.
[121] *Lithuanian finance institution – licensing solutions for FinTech companies providing services in single European market*, Ecovis, https://ecovis.lt/lithuanian-finance-institution-the-licensing-solution-for-foreign-companies-providing-services-in-single-european-market/, 2 May 2020.
[122] Tsang, C. (2019). From industry sandbox to supervisory control box: Rethinking the Role of Regulators in the Era of FinTech. *University of Illinois Journal of Law, Technology & Policy*, 2019 (2), 355.

to stringent regulations and longer history of financial crime prevention. The bank, based on the training related communication with FinTech, would be more able to assess the risks associated with the business models of their FinTech customers.

In collaborations, the reputation is considered the most effective measure to comply with the common rules. However, this can be done only when the expected behavior and the rules to be followed in order to collaboration to happen are clearly communicated.[123] When the rules are unclear, co-operation in order to gain reputational gains is less likely to happen as the costs of breaking unclear rules are lower.[124] With an educative approach, due to a training collaboration, the banks could be able to create a more straightforward understanding on what measures FinTechs should follow in order to be able to collaborate with them and also to communicate that clearly.[125]

A successful example of banks training their collaborators, can be taken from the field of trade finance: Standard Chartered Bank has taken a successful educational approach and launched a 'Correspondent Banking Academy', organizing workshops among their collaborators to educate and share best practices for AML.[126] This model could also be worthwhile to examine for the FinTech field.

4.4 Knowledge-sharing within FinTechs

Collaboration and knowledge-sharing within the FinTech companies will also mitigate the ML risks. The companies need to understand the industry, products, the business they are conducting and also know the required license as well as the regulatory regime where they operate.

Although it is the senior management's responsibility to define the risk appetite for the company, the team designing the products and services should also add a financial crime risk perspective to the designing process. A clear business strategy created with RBA by the senior management helps

[123] Axelrod, R. (1986). An Evolutionary Approach to Norms *The American Political Science Review*. 8(4), 1095, 1105; Cooter, R.D. (1996). Decentralized Law for a complex economy: The Structural approach to adjudicating the New Law Merchant. *University of Pennsylvania Law Review*. 144(5), 1643-1645, 1670.
[124] Axelrod, R. (1986). An Evolutionary Approach to Norms *The American Political Science Review*. 8(4), 1105
[125] Bilkstys, G.E., Kanapienis, L., Pinot, A., Schnieder, M. (2020, 5 March) *The Risks and Opportunities of Technology*. ACAMS Anti-Financial Crime Symposium – Baltics, Riga, Latvia.
[126] Standard Chartered Bank: *De-risking through education: a powerful tool for raising industry standards*. Retreived from https://www.sc.com/en/explore-our-world/correspondent-banking/, 4 May 2020; Murat, Y. (2020, 5 March) *Correspondent Banking Relationships and De-Risking.* ACAMS Anti-Financial Crime Symposium – Baltics, Riga, Latvia.

the production team to design products which fit the defined risk limits. Communication in both directions builds understanding on what the company actually does, what are the ML risks it is exposed to, and how the risks are mitigated.

4.5 EU-wide supervisory authority

EU AMLDs require MSs to ensure that obliged institutions are adequately regulated and supervised. There are no clear instructions how this is to be done, meaning that the requirement is filled by MSs with minimum harmonisation so therefore supervision is strongly regulated on the national level thus from the institutional perspective the policies differ considerably. The current supervisory models MSs are using are: FIU model, having the national FIU as a supervisory body with ultimate responsibility on supervision; External model, meaning the use of external, generally existing supervisory structures with no direct professional relationship to the supervised entities; Internal model, where the supervision is usually performed with many different professional associations; and Hybrid model, combining elements from the aforementioned models.[127]

Using the Nordic and Baltic states as an example Lithuania uses the FIU model. Finland, Sweden and Denmark use external/internal models whilst Estonia (external/internal/FIU) uses the hybrid model.[128] All the models have their strengths and weaknesses related *inter alia* to available resources, sectorial knowledge or the lack of it and dependencies on the supervised entities.

It can be questioned if the national supervisors are adequate for effectively combating ML or if the EU should have a union-wide supervisory entity. The diverse supervisory policies on the national level and cross-border FinTech businesses cause challenges for supervisors to have a good overview on the actors on the field. Knowledge sharing and collaboration projects to increase the common knowledge are established, such as a Black Wallet-project, a collaboration between the FIUs of Finland and Sweden.[129] Both FIUs have acknowledged their lack of knowledge on the increasing amount of business models operating on the FinTech field in their jurisdictions and launched together an EU funded project, to recognize the ML/TF risks related to this.

[127] Van Den Broek, M. (2014). Designing supervision under the Preventive anti-Money laundering Policy in the European Union. *Utrecht Law Review.* 10 (5), 152-156.
[128] Ibid, 156.
[129] Keskusrikospoliisi: *Black Wallet*. Retrieved from https://www.poliisi.fi/keskusrikospoliisi/black_wallet, 4 March 2020.

In addition, basing the supervision on the local (private and public) supervisors increases the risk of interconnectedness between the supervisors and the supervised entities. The actors in the industry (especially in the countries with elements of internal model) with good relations to the supervisor may not be under strict enough supervision.

Also the resources in different MSs are diverse, resulting in less supervised jurisdictions having a risk of criminals finding their way to these jurisdictions. An EU-wide supervisor with less dependency in relation to the supervised entities, an ability to harmonize the architecture of the supervision and a possibility to provide equal resources for supervision is a considerable idea worthy of investigating. Currently the topic is discussed for example by the Task Force created under CEPS. The objective of the Task Force is to *inter alia* examine a better governance for the supervision of AML matters and if a new EU-wide AML authority is needed.[130] Further investigation is needed as to what would be the structure, powers and activities of this entity for it to be effective, respond to the gaps in the supervisory field, and to combat the ML in the most efficient way.

[130] Satuli, H., *Rahanpesuongelma jäytää Euroopan taloutta ja tilanne pahenee koko ajan – ”Heikoin lenkki on nyt tosi heikko”,* (2020). Retrieved from https://www.finanssiala.fi/uutismajakka/Sivut/Rahanpesuongelma-jaytaa-Euroopan-taloutta.aspx, 19 March 2020; CEPS- ECRI Task Force: *Anti-Money Laundering in the EU - Ensuring effective and efficient cross-border cooperation and mutual trust: Time to get serious*. (2020) Retrieved from https://www.ceps.eu/wp-content/uploads/2019/10/TF-PROSPECTUS-AML.pdf, 8 May 2020.

CONCLUSION

It is evident that the rapid emergence of FinTech creates new ML risks for the finance industry. When the whole aim of the FinTech is to disrupt the finance industry by designing better products and services, increase the financial inclusion and create whole new ways of thinking finance, it is expected that also new opportunities for criminals rise. When something is re-created and there are many players in the field participating the development, it is understandable that having an overall view on the unwanted side-effects of development is limited.

The study shows that a significant ML risk area associated with FinTech is related to the customer identification process. This is also where the current EU regulative framework provides differences compared to the traditional FIs, due to the RBA that obliges financial service providers to base their AML procedures on their own risk assessment of their business. The challenges in other CDD requirements such as transaction monitoring due to the amount of rapid cross-border transactions combined with the incomplete customer data due to a simple identification process create challenges to distinguish between usual and unusual behaviour of the customer and therefore to detect possible ML taking place in the company.

It can be concluded that the current EU regulative framework enables AML vulnerabilities related to the rapid emergence of the FinTech, but the vulnerabilities are not only due to the regulation. The lack of understanding of different parties at different levels, related to the technological innovations, development of new business models, and also how these developments reform the finance industry can be seen as the biggest challenges when combating ML in the FinTech field.

There is a lack of understanding on the FinTech's side as the product developers may not understand the ML risks of products they design, the employees acquiring the customers the risks of the customer-base, the senior management is unable to evaluate the ongoing development, and the emerging criminal trends. Loose standards, enabled by the RBA, can also be applied willingly in order to gain market share.

The supervisors also do not fully comprehend the businesses of the FinTechs, are unable to conduct effective supervision due to the cross-border nature of the FinTechs and there is a lack of cooperation with supervisory authorities in other countries. The fact that FinTechs reach to multiple jurisdictions does not make it easy for supervisors to monitor the FinTecs, but also it is challenging for FinTechs themselves to stay on top of what is required from them.

Last but not least, the banks need to improve their understanding of risks of having a FinTech as a customer. They may not fully comprehend the business the FinTech is conducting and therefore gets exposed to new risks such as a customer-base they would not be willing to take. In addition, as the FinTechs evolve all the time, they may develop new risky products after the partnering agreement with the bank is done. The thesis suggests the FinTechs should be under EDD by default, resulting in stringent continuous evaluation from the banks side.

This thesis suggests that an emphasis on detecting the AML vulnerabilities associated with FinTechs and to combat ML, should be given to develop collaborative and coordinating actions with different parties, and to create strong PPPs in order to increase understanding on the development that is taking place in the finance industry.

The study supports the increasing discussion between the FinTechs, FSAs and the regulators in order to create better understanding of the risks and requirements, for example in the form of introduced regulatory sandboxes. Also the cross-border collaboration of national FIUs to detect, define and evaluate the vulnerabilities in certain jurisdiction is recommended.

Improving the collaboration is also needed between the FinTech field and the traditional FIs. The thesis introduced the educational approach to AML applied for correspondent banking within the field of trade finance, and sees that a similar approach could be applied for FinTechs and their partner banks. It can be stated that the EU regulative framework enables competitive distortion to the extent that whilst the traditional banks and FinTechs provide similar services, the FinTechs may be able to apply less stringent AML procedures, enabling them for instance taking customers with looser standards due to their risk assessment based on the RBA. Therefore it could be asked why banks would spend their resources educating their competitors. However the educative approach would not be only a one way effort by banks providing their superior AML knowledge for FinTechs, but they will also gain from FinTechs innovative technology in their own CDD processes as well as products and services. The use of RegTech was not further discussed in this thesis, but the question of how FinTechs could contribute to combating ML by RegTech is up for debate.

In addition to the efforts in collaborative actions, the EU regulative framework has weaknesses that need improvement. EU AMLDs provide loopholes due to the variation on how the directives are implemented to the national legislations. The study suggests the EU AML regulative framework to move from directive-based to regulation-based, in order to minimize the variation between the MSs legislation, including for example the classification of the FinTech business

models and the variation in licensing between MSs that causes challenges for supervising as well as for FinTechs to stay on top of what is required from them in matters of AML. The study also sees the benefit of researching further the establishment of an EU-wide supervisory authority in order to *inter alia* harmonize the architecture of the supervision in the EU and minimize the dependencies between the local supervisors and supervised entities. The thesis did not discuss the possible structure and detailed activities of this authority.

It can still be concluded that the improvements in the EU regulative framework can be enabled only by the suggested increase in collaboration and continuous knowledge-sharing between parties in the FinTech era finance industry.

LIST OF REFERENCES

Scientific books

1. Arner, D. W., Buckley, R.P. (2011). *From Crisis to Crisis: The global financial system and regulatory failure.* Netherlands: Kluwer Law International. Referenced in Arner, D. W., Bargeris, J., Buckley, R.P. (2017). Fintech, regtech, and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business,* 37 (3).

2. Dare, P., Thornhill, S., Howarth, W.B. (2019). *ICA International Advanced Certificate in Anti Money Laundering – Course Manual*. (12th ed.) United Kingdom. International Compliance Association ICA.

3. Graig, P., De Burca, G. (2015). *EU Law: Text, Cases, and Materials.* (6th ed.) United Kingdom. Oxford Press.

4. Kasper, A. (2014) *The Fragmented Securitization of Cyber Threats*. In Kerikmäe, T. ed., *Regulating eTechnologies in the European Union – Normative Realities and Trends*. Germany. Springer.

5. Law, J. (Ed.). (2018). *Dictionary of Finance and Banking.* (9th ed.) United Kingdom. Oxford University Press.

6. Sironi, P.(2016) My Robo Advisor Was an iPod-Applying the Lessons from Other Sectors to FinTech Disruption. In Barberis, J., Chishti, S. (Eds.) *The Fintech Book: The financial technology handbook for investors, entrepreneurs and visionaries*. Wiley. Referenced in Wu, Y. (2017). Fintech innovation and anti-money laundering compliance, *National Taiwan University Law Review*, 12(2).

7. Unger, B., Ferwerda, J., Van Den Broek, M., Deleanu, I. (2014). *The Economic and Legal Effectiveness of the European Union's Anti Money Laundering Policy*. United Kingdom. Edgar Elgar Publishing Limited.

8. Van Duyne, P. C., (2003). *Money Laundering, Fears and Facts.* In Van Duyne, PC., von Lampe, K., Newell, J.L. (Ed.), *Criminal Finances and Organizing Crime in Europe*, Netherlands. Wolf Legal Publishers.

Scientific articles

9. Alldridge, P. (2008). Money laundering and globalization. *Journal of Law and Society*, 35 (4), 437-463.

10. Arner, D. W., Bargeris, J., Buckley, R.P. (2016). The evolution of FinTech: A New Post-Crisis Paradigm?, 47 *Georgetown Journal of International Affairs,* 1271, 1272-1219. Referenced in Arner, D. W., Bargeris, J., Buckley, R.P. (2017). Fintech, regtech, and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business,* 37 (3), 371-414.

11. Arner, D. W., Bargeris, J., Buckley, R.P. (2017). Fintech, regtech, and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business,* 37 (3), 371-414.

12. Axelrod, R. (1986). An Evolutionary Approach to Norms. *The American Political Science Review.* 8 (4), 1095-1111.

13. Cooter, R.D. (1996). Decentralized Law for a complex economy: The Structural approach to adjudicating the New Law Merchant. *University of Pennsylvania Law Review.* 144 (5), 1643-1696.

14. Douglas, J. L., (2016) New Wine into Old Bottles: Fintech Meets the Bank Regulatory World. *North Carolina Banking Institute,* 17-66.

15. Ferweida, J. (2009). The Economics of Crime and Money Laundering: Does Anti-Money Laundering Policy Reduce Crime? *Review of Law and Economics,* 5 (2), 903-928.

16. Gangull, I., Actelik, O., Kohling, L., Mauhs, FM. (2009). The Third AML-directive: Europe's response to the threat of money laundering and terrorist financing: Part ii. *Banking Law Journal,* 126 (8), 728-759.

17. Ionescu, L. (2012). Money laundering directives and corruption in the European union. *Contemporary Readings in Law and Social Justice.* 4 (2), 562-566.

18. Kobor, E. S. (2013). The role of anti-money laundering law in mobile money systems in developing countries. *Washington Journal of Law, Technology & Arts.* 8 (3), 306-316.

19. Levi, M., Reuter, P. (2006). Money Laundering. *Crime & Justice,* 34, 289-375.

20. Magnusson, W. (2018). Regulating FinTech. *Vanderbilt Law Review.* 7 (4), 1167-1226.

21. Meklin, H. (2018), AML risks and challenges at the time of crypto currencies. *L'Europe Unie / United Europe*, 59-67.

22. Pellegrina, L., Masciandaro, D. (2009). The risk-based approach in the new European anti-money laundering legislation: law and economics view, *Review of Law and Economics,* 5 (2), 931-952.

23. Tsang, C. (2019). From industry sandbox to supervisory control box: rethinking the role of Regulators in the Era of FinTech. *University of Illinois Journal of Law, Technology & Policy,* 2019 (2), 355-404.

24. Van Den Broek, M. (2014). Designing supervision under the Preventive anti-Money laundering Policy in the European Union. *Utrecht Law Review*. 10 (5), 151-167.

25. Wu, Y-T. (2017). FinTech Innovation and Anti-Money Laundering Compliance. *National Taiwan University Law Review*, 12 (2), 201-258.

EU and international legislation

26. Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering

27. European Parliament and of the Council of 4 December 2001 Directive 2001/97/EC amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering
28. European Parliament and of the Council of 26 October 2005 Directive 2005/60/EC of the on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

29. European Parliament and of the Council of 20 May 2015 Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

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

Other countries' legislation

31. Laki Finanssivalvonnasta 19.12.2008/8780

32. Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444

33. Maksulaitoslaki 30.4.2010/297

Other sources

34. *Authorisation of Banks.* Bank of Lithuania. https://www.lb.lt/en/authorisation-of-banks#ex-1-2, 9 May 2020.

35. *Basel Committee on Banking Supervision: Sound Practices, Implications of fintech developments for banks and bank supervisors* (2018). Bank for International Settlements, 4. Retrieved from, https://www.bis.org/bcbs/publ/d431.pdf, 14 March 2020.

36. Bilkstys, G.E., Kanapienis, L., Pinot, A., Schnieder, M. (2020, 5 March) *The Risks and Opportunities of Technology*. ACAMS Anti-Financial Crime Symposium – Baltics, Riga, Latvia.

37. Cabell, J. *Fintechs vs. Traditional Banks: Who Has the Bigger Advantage?* Retrieved from https://thefinancialbrand.com/84106/fintech-bank-credit-union-competition-advantages/, 15 March 2020.

38. CEPS- ECRI Task Force: *Anti-Money Laundering in the EU - Ensuring effective and efficient cross-border cooperation and mutual trust: Time to get serious*. (2020)

Retrieved from https://www.ceps.eu/wp-content/uploads/2019/10/TF-PROSPECTUS-AML.pdf, 8 May 2020.

39. Chief AML & Sanctions Processing Specialist at Nordea, Sillanpää, P. (17 April 2020). *Training on Payment Service Providers.*

40. Chief AML & Sanctions Processing Specialist at Nordea, Vuorinen, M. Author's interview. Transcript. 23 March 2020.
41. Dare, P. (2020, 17 March). *ICA International Advanced Certificate in Anti Money Laundering Workshop 2*. Virtual workshop.

42. *Deposit Guarantee Scheme* – European legislation protects banks deposits in case of bank failure. European Comission. Retrieved from https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/managing-risks-banks-and-financial-institutions/deposit-guarantee-schemes_en, 21 March 2020.

43. *Discussion Paper on the EBA's approach to financial technology (FinTech).* EBA, 10-11. Retrieved from https://eba.europa.eu/sites/default/documents/files/documents/10180/1919160/7a1b9cda-10ad-4315-91ce-d798230ebd84/EBA%20Discussion%20Paper%20on%20Fintech%20(EBA-DP-2017-02).pdf, 23 March 2020.

44. EU: *Pankkitili toisessa EU-maassa*. Retrieved from https://europa.eu/youreurope/citizens/consumers/financial-products-and-services/bank-accounts-eu/index_fi.htm, 29 April 2020.

45. EBA: *Passporting and supervision of branches.* Retrieved from https://eba.europa.eu/regulation-and-policy/passporting-and-supervision-branches, 18 April 2020.

46. FCA: *Regulatory sandbox.* (2015). Retrieved from https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf, 2 May 2020.

47. FATF: *Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services.* (2013), 11-13. Retrieved from https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf, 23 March 2020.

48. FATF: *What we do.* Retrieved from http://www.fatf-gafi.org/about/whatwedo/, 2 Jan 2020.

49. FATF: *Risk-Based Approach - 18 publications*. Retrieved from http://www.fatf-gafi.org/documents/riskbasedapproach/?hf=10&b=0&s=desc(fatf_releasedate), 12 March 2020.

50. Financial Crimes Risk Specialist at Transferwise, Schnieder, M. Author's interview. 23 March 2020.

51. FIN-FSA, Financial Supervisory Authority: *Authorisations, registrations and notifications in the financial markets*. https://www.finanssivalvonta.fi/en/banks/authorisations-registrations-and-notifications/, 19 March 2020.

52. Finantsinspektsioon: *Applying for an operating license in payment services*, Retrieved from https://www.fi.ee/en/payment-and-e-money-services/applying-operating-licence-payment-services, 20 March 2020.
53. *Fully digitised opening of a bank account is available from anywhere in the world now*. Luminor. Retrieved from https://www.luminor.lv/en/news/fully-digitised-opening-bank-account-available-anywhere-world-now, 2 May 2020.

54. Government Office for Science: FinTech Futures - *The UK as a World Leader in Financial Technologies - A report by the UK Government Chief Scientific Adviser* (2015). Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf, 21 March 2020.

55. Hanley-Giersch, J., Status of the European AML Framework. (2019) *AcamsToday*. Retrieved from https://www.acamstoday.org/status-of-the-european-aml-framework/, 21 March 2020.

56. ICA - International Compliance Association: *What is Customer Due Diligence (CDD)?* Retrieved from https://www.int-comp.org/careers/your-career-in-aml/what-is-customer-due-diligence-cdd/, 18 March 2020.

57. ICA – International Compliance Association: *What is Money Laundering?*. Retrieved from https://www.int-comp.org/careers/your-career-in-aml/what-is-money-laundering/ , 21 March 2020.

58. Keskusrikospoliisi: *Black Wallet*. Retrieved from https://www.poliisi.fi/keskusrikospoliisi/black_wallet, 4 March 2020.

59. *Lithuanian finance institution – licensing solutions for FinTech companies providing services in single European market*, Ecovis, https://ecovis.lt/lithuanian-finance-institution-the-licensing-solution-for-foreign-companies-providing-services-in-single-european-market/, 9 May 2020.

60. London FinTech FinCrime Exchange Survey. Retrieved from https://www.fintrail.co.uk/ffe, 17 March 2020.

61. Money Laundering Reporting Officer of SONECT. Pinot, A. Author's interview in LinkedIn. Transcript. 25 March 2020.

62. McKinsey & Company: *Global Banking Annual Review* (2015). Retrieved from https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review-2019-the-last-pit-stop-time-for-bold-late-cycle-moves, 14 March 2020.

63. Monese. https://monese.com/about, 29 April 2020.

64. *Money-Laundering and Globalization.* United Nations Office on Drugs and Crime. Retrieved from https://www.unodc.org/unodc/en/money-laundering/globalization.html, 21 March 2020.

65. *Money laundering and terrorist financin*g. (2015/2020). Financial Conduct Authority (FCA) UK. https://www.fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing, 12 March 2020.

66. Monzo. Retrieved from https://monzo.com,15 March 2020.

67. Murat, Y. (2020, 5 March) *Correspondent Banking Relationships and De-Risking.* ACAMS Anti-Financial Crime Symposium – Baltics, Riga, Latvia.

68. N26. Retrieved from https://n26.com/en-eu, 15 March 2020.

69. Pinot, A., Fintech: Friend or foe to anti-financial crime? *AcamsToday*. (2019) Retrieved from https://www.acamstoday.org/fintech-friend-or-foe-to-anti-financial-crime/, 18 March 2020.

70. Replace Your Documents. Retrieved from https://www.replaceyourdoc.com, 17 March 2020.

71. Revolut. Retrieved from https://www.revolut.com, 15 March 2020.

72. Revolut: *How we're different from a bank (and what that means for your business)* https://blog.revolut.com/business-what-makes-us-different-from-a-bank-and-what-that-means-for-your-business/ , 15 March 2020.

73. Runde, D. (2015) M-Pesa And The Rise Of The Global Mobile Money Market. *Forbes*. Retrieved from https://www.forbes.com/sites/danielrunde/2015/08/12/m-pesa-and-the-rise-of-the-global-mobile-money-market/, 21 March 2020.

74. Satuli, H., *Rahanpesuongelma jäytää Euroopan taloutta ja tilanne pahenee koko ajan – ”Heikoin lenkki on nyt tosi heikko”,* (2020). Retrieved from https://www.finanssiala.fi/uutismajakka/Sivut/Rahanpesuongelma-jaytaa-Euroopan-taloutta.aspx, 19 March 2020.

75. Standard Chartered Bank: *De-risking through education: a powerful tool for raising industry standards*. Retreived from https://www.sc.com/en/explore-our-world/correspondent-banking/, 4 May 2020.

76. *The Amounts and Effects of Money Laundering*. A Report for the Ministry of Finance. (2006), 84-95, 160. Retrieved from www.ftm.nl/wp-content/uploads/2014/02/witwassen-in-nederland-onderzoek-naar-criminele-geldstromen.pdf, 2 Jan 2020.

77. The Long, Dark Shadow of Herstatt. *The Economist*. (2001). Retrieved from http://www.economist.com/node/574236, 10 March 2020.

78. Transferwise. Retrieved from https://transferwise.com,15 March, 2020.

79. Transferwise for Business (New). Retrieved from https://transferwise.com/gb/business/, 16 March 2020.

80. Transferwise. Wikipedia. Retrieved from https://en.wikipedia.org/wiki/TransferWise, 15 March 2020.

81. Turp, G.: Emerging Europe: *Sandbox success cements Lithuania's reputation as fintech hub.* Retrieved from https://emerging-europe.com/new-industry/sandbox-success-cements-lithuanias-reputation-as-fintech-hub/, 4 May 2020.

82. Wright, M. *An insight into virtual banking*. A recording from the International Compliance Association's 2nd APAC conference. Retrieved from https://www.int-comp.org/cpditem/?product=Aninsightintovirtualbanking, 18 March 2020.

83. Znotina, I., (2020, 5 March) *Regulatory Roundtable on Financial Crime Prevention.* ACAMS Anti-Financial Crime Symposium – Baltics, Riga, Latvia.

Appendix 1. Non-exclusive licence

Non-exclusive licence for reproduction and for granting public access to the graduation thesis[1]

I, Heli Meklin

1.Give Tallinn University of Technology a permission (non-exclusive licence) to use free of charge my creation

THE EMERGENCE OF FINTECH – THE AML VULNERABILITIES IN THE EU REGULATORY FRAMEWORK

supervised by Jenna Uusitalo

1.1. to reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of TalTech library until the copyright expires;

1.2. to make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of TalTech library until the copyright expires.

2. I am aware that the author also retains the rights provided in Section 1.

3. I confirm that by granting the non-exclusive licence no infringement is committed to the third persons' intellectual property rights or to the rights arising from the personal data protection act and other legislation.

---

[1] *The non-exclusive licence is not valid during the access restriction period with the exception of the right of the university to reproduce the graduation thesis only for the purposes of preservation.*