



universität
wien

MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

Branchless Banking and Anti-Money Laundering: A Critical Analysis of the Digitisation of KYC within the European Union

verfasst von / submitted by

Samia Murgham, LL.B.

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of
Master of Laws (LL.M.)

Wien, 2016 / Vienna 2016

Studienkennzahl lt. Studienblatt /
Postgraduate programme code as it appears on
the student record sheet:

A 992 548

Universitätslehrgang lt. Studienblatt /
Postgraduate programme as it appears on
the student record sheet:

Europäisches und Internationales Wirtschaftsrecht /
European and International Business Law

Betreut von / Supervisor:

emer.o.Univ.-Prof. Dr. Peter Fischer

Table of Contents

List of Acronyms Used	4
Introduction	5
Money Laundering and Terrorist Financing	8
What is Money Laundering?	8
What is Terrorist Financing?	8
Know Your Customer (KYC)	9
The Difference between Identification and Verification of Customers.....	12
Anti-Money Laundering and Counter Terrorist Financing: The Current Legal Framework within the European Union.....	13
Directive 2015/849 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering or Terrorist Financing	19
Adoption of a Risk-Based Approach	20
Registry of Ultimate Beneficial Ownership.....	21
Conducting On-going Monitoring	22
Risks Associated with Politically Exposed Persons	23
New Customer Due Diligence Obligations.....	24
Reporting of Suspicious Transactions	25
Record Keeping	25
Digitization of KYC	26
Branchless banking.....	27
Non Face-to-Face Transactions	28
Enhanced Customer Due Diligence for Non F2F Situations.....	31
Due Diligence Outsourcing	34
Common Methods of ID Verification by Third parties within the EU	34
Conducting Online KYC Without the Use of Third Parties	37
Digital KYC Evidence of Practice in the EU: Dissimilarity across member states	39
Costs of Digital KYC	46
Fresh Challenges of Digital KYC: the Drive for Effectiveness and Efficiency.....	47
Other Legal Issues arising out of Digital KYC	49
Data Protection Law	49

Third Party Dependence	52
Impracticability of Access to Information.....	54
Conclusion.....	55
Bibliography.....	58
English Abstract	64
German Abstract.....	65

List of Acronyms Used

AML	Anti-Money Laundering
CDD	Customer Due Diligence
EU	European Union
F2F	Face to Face
KYC	Know Your Customer
FATF	Financial Action Task Force
CTF	Counter Terrorist Financing
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
PEP	Politically Exposed Person
CDPC	European Committee of the Council of Europe on Crime Problems
UBO	Ultimate Beneficial Owner
FIU	Financial Intelligence Units
NFC	Near Field Communication
RFID	Radio Frequency Identification

Introduction

In an era of unparalleled change, technological development has resulted in revolutionary advances in digital banking services. Innovation within the Banking and Financial sector has become increasingly apparent in this digital age since the introduction of online banking, and banks are embracing the opportunity to create added business value and to enhance customer engagement.

Banking has widely been a traditionalist industry, characterized by strict regulations, both nationally and internationally. Recently, however, the outpouring of new participants riding the digital wave of nouvelle banking technologies has radically lessened regulatory obstacles.

For reasons such as cost savings and efficiency, vast numbers of banks and other financial institutions are resorting to the creation of branchless banking, meaning that customers are able to open bank accounts, as well as obtain other financial products and services, such as loans and investment products, fully online without the need to be physically present upon account opening in a bank branch. The creation of these so called “neo-banks” or “digital only/ branchless banks” such as Dutch-owned Number26, and UK-owned Atom Bank, are one of few neo-banks that have been making international headlines.

As with the non-digital more traditional means of banking, background information about bank clients, or simply the verification of the identities of bank account holders, also known as Customer Due Diligence (CDD) or Know Your Customer (KYC), has been one of the most important regulatory requirements for banks to carry out in order to reduce financial fraud losses, prevent identity theft, identify potential areas of risk, prevent anti-money laundering and the financing of terrorist activities.

KYC involves financial institutions collecting and analyzing basic information on the identities of their customers, identifying whether names of potential account holders are on black lists, assessing the risk that each customer has with regard to their predisposition to partake in criminal activity such as money laundering, financial fraud, identity theft or the financing of terrorism, to name a few.

Another important part of KYC is the assessment of whether the customer or entity is a politically exposed person (PEP), that is, a person who currently holds or has held a powerful public position or title.

The meaning of PEP also extends to individuals who are related to (immediate family members) or affiliated with, currently or previously, to a prominent public figure (close business associates, senior executives of state enterprises etc.). PEPs are an important part in KYC as they usually pose increased risk with regards to their propensity for partaking in corruption and bribery by means of their powerful status and potential public influence.¹

The aim of having rules on KYC is to ward off the use of banks by criminals, whether with or without the bank's intent, for money laundering or other illegal dealings. Additionally, KYC regulations provide banks with means to enhance understanding of who their clients are and what their clients' financial transactions encompass. With KYC compliance, banks are able to cautiously manage risk.

In general, banks typically structure their KYC due diligence into the as follows:

- i. Monitoring client financial activity
- ii. Client policy structuring
- iii. Managing risks
- iv. Client identity verification

For the purpose of clarity, a "client" or "customer" of the bank within the meaning of this research paper will refer to:

- i. The beneficial owner of the bank account, within the meaning of the 4th Anti-Money Laundering Directive that will be subsequently mentioned.
- ii. Any legal person or legal entity that is a holder of any type of bank account with their relevant bank or partakes in any business activity with the bank or facilitated by the bank.

¹ There is currently no global definition of Politically Exposed Person and the meaning differs from one legal system to the next. A person who qualifies as a PEP in one jurisdiction might not qualify as a PEP in other jurisdiction. Within the European Union, the definition of PEP is stipulated in the 4th Anti-money laundering directive, which will be discussed later in this paper.

- iii. Any legal person or entity with the ability to subject the bank to any sort of risk, both monetary and non-monetary risk, or damage its reputability.
- iv. Financial beneficiaries of dealings carried out by qualified intermediaries such as traders, fund managers, accountants and lawyers.

One major issue that arises with banking digitization is that non-face-to-face interaction with customers fosters anonymity, leading to a greater risk of money laundering or terrorist financing. It is thus paramount that the laws governing customer due diligence or KYC (Know Your Customer) for financial institutions offering online services, adapt in order to mitigate this risk and become more stringent.

This paper will address the shift of face-to-face (F2F) to non-face-to-face customer due diligence processes (KYC) when bank customers initiate business relationships. Based on the fourth European Union Anti-Money Laundering Directive, a legal comparison of the differing approaches of EU Member States in relation to the transposition of this directive will be provided, in terms of customer due diligence for non-F2F dealings such as digital account opening and applying for additional online banking products and services.²

The central research questions to be investigated in this research paper are as follows:

- i. What are the problems involved with banking transactions for *in absentia* customers, and what solutions have Member States adopted?
- ii. What are the main procedural measures that have been taken by financial institutions to mitigate the risks of non-F2F transactions and what problems might arise from such application?
- iii. To what extent are these measures adequate to ensure the prevention of money laundering activities and terrorist financing and what improvements (if any) could be made?

² Directive 2015/849/EU of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing [2015] OJ 2 141/73.

Money Laundering and Terrorist Financing

What is Money Laundering?

Money laundering involves relocating the earnings from criminal activity into seemingly lawful wealth. The concept of money laundering, however, varies from one jurisdiction to another, and many seem to incorporate other financial crimes (involving the use of credit cards, virtual currencies and so on) under the umbrella term of “money laundering”. This may also consist of the financing of terrorist activities as well as the dodging international sanctions.³

What is Terrorist Financing?

Terrorist financing refers to process of funding of terrorist individuals, acts and organisations, whose main objective is to intimidate people or coerce governments to do certain things, by means of killing, endangering or harming people and property or by gravely disordering vital services or essential systems.⁴ Sources of funds to finance terrorism may include:

- i. Money generated from criminal activity (such as fraud, kidnapping, extortion, prostitution, drugs, gambling and smuggling)
- ii. Sponsoring from other countries supporting terrorism (especially in places of political unrest)
- iii. Funds obtained legitimately (businesses, charity organisations, donations).⁵

The main difference between money laundering and terrorist financing is the origin of the funds and its usage. Money laundering funds are gained out of illegal activity with the

³ Duhaime C, 'What Is Money Laundering? Duhaime's Anti-Money Laundering Law In Canada' (*Antimoneylaunderinglaw.com*, 2014) <<http://www.antimoneylaunderinglaw.com/aml-law-in-canada/what-is-money-laundering>> accessed 12 March 2016.

⁴ Bantekas I., 'The International Law Of Terrorist Financing' (2003) 97 *The American Journal of International Law*.

⁵ *ibid*.

intention of legal usage; whereas funds for terrorist financing are used for illegal purposes may not be sourced from illegal activity.

Know Your Customer (KYC)

Several methods used by criminals for money laundering or terrorist financing entail the exploitation of the financial system for the transmission of money. Financial institutions, and most specifically banks, are susceptible to misuse by criminals achieve such aims.

In order to safeguard the integrity and smooth running of the financial system, it is important that financial institutions are aware of who they are engaging in business with or on behalf of whom they are performing certain financial transactions for.⁶ Thus, it is crucial that financial institutions have sufficient control and capability, by means of having adequate measures set up, to facilitate their familiarisation with customers (KYC). A fundamental part of these controls is the implementation of appropriate customer due diligence methods within the bank, targeted at new as well as existing customers.

The term 'Know Your Customer' refers to the process of verifying the identity of bank customers (by making use of reliable and independent sources of information, such as authentic identification documents), monitoring the customer's transactions, as well as ensuring the latest information on the customer is filed in line with the bank's policy.⁷

KYC systems require banks to constantly have sufficient information on their customers, their spending habits, statement of income, what products and services s/he has requested or made use of, the location of the customer, as well as on the persons the customer transfers or receives funds from.

In general, KYC programs consist of three parts, namely:

- i. Identifying the customer
- ii. Carrying out customer due diligence

⁶ Mulligan D., 'Know Your Customer Regulations and the International Banking System: Towards a General Self-Regulatory Regime' (1998) 22 Fordham International Law Journal.

⁷ Byrne J, 'Know Your Customer: What Happened And What Happens Next?' (2000) 3 J of Money Laundering Control.

- iii. Having enhanced due diligence, should the need arise out of higher risk situations (discussed later)⁸

KYC facilitates the bank's comprehension of specific customer during the course of their business relationship, from the onboarding stage all the way up to the closing of an account. In certain instances, the customer intelligence gained by the bank may elicit more thorough investigations of the customer or the certain transaction that sparked such initiation.⁹

Anti-money laundering involves obliging financial institutions such as banks to develop appropriate systems through which they investigate their customers before entering into business relationships as well as to detect persons who may possibly harm the reputation of the bank.¹⁰

Conducting KYC is mandatory. It is a regulatory and legal requirement of all banks, which are expected to establish policies with regard to KYC standards and AML/CFT measures.

¹¹Requiring banks to conduct KYC is not something new; it has been a requirement for decades, and in the past, banks have been collecting customer data in accordance to international regulations and guidelines.¹²

In banking relationships with clients, KYC is performed at many stages:

- i. At first-time account-opening
- ii. When existing customers would like to open other types of accounts and KYC information is not up to date
- iii. In situations where the bank has used its discretion to justify collecting supplementary information on customers due to certain unusual behaviour.
- iv. When significant changes are made, for example, change of beneficial owners, account signatories etc.

⁸ Sullivan K, *Anti-Money Laundering In A Nutshell* (Springer 2015) 71.

⁹ *ibid* 71

¹⁰ 'International Guide To Money Laundering Law and Practice, 4th Edition' [2016] Commonwealth Law Bulletin <<http://www.tandfonline.com/doi/full/10.1080/03050718.2015.1019689>> accessed 12 March 2016.

¹¹ *ibid*.

¹² Mulligan D., *Know Your Customer Regulations and the International Banking System: Towards a General Self-Regulatory Regime* (Fordham Int'l Law Journal 1998) 22.

- v. When individuals or entities not holding an account at the bank, makes use of the bank's services to carry out single large transactions.¹³

Having efficient KYC standards in place within the financial industry are essential for the safeguarding of reliability in the financial system and, in particular, warding off money laundering and the financing of terrorism.¹⁴

To ensure such standards, the KYC policies in place within banks comprise of systems with adequate measures to:

- i. Identify and verify bank customers
- ii. Assess customer risk and
- iii. Monitor the accounts of customers as well as all corresponding transactions.¹⁵

With this in mind, the overall aim of performing KYC is so that financial institutions know who they are conducting business with and for which purpose.¹⁶

In situations where the required KYC information is not obtained by the bank, through voluntary customer refusal, the bank is permitted to deny potential customers the right to be account-holders at that bank, as well as end business relationships with existing customers for the same reasons.¹⁷

¹³ *ibid* 23.

¹⁴ Chong A and Lopez-De-Silanes F, 'Money Laundering And Its Regulation' (2015) 27 *Economics & Politics*.

¹⁵ BCBS, *Sound Management of Risks Related to Money Laundering and Financing of Terrorism* (BIS 2014) 10

¹⁶ Sullivan K, *Anti-Money Laundering In A Nutshell* (Springer 2015) 69.

¹⁷ *ibid* 69.

The Difference between Identification and Verification of Customers

The terms ‘identification’ and ‘verification’ are used interchangeably, however, it is important to note that these concepts differ greatly. In the internal policies of banks, these two terms are often mistaken and the confusion of such terms might lead to KYC being performed incorrectly.¹⁸

‘Identification’ and ‘verification’ are usually defined in the following manner:

- i. ‘Identification’ of the customer refers to the process by means of which data and information of the customer are gathered with the aim of ‘knowing your customer’, which enables an appropriate customer risk assessment to be generated. This is to prevent entering into business relationships with anonymous individuals and subsequently engaging in anonymous transactions.¹⁹
- ii. ‘Verification’ refers to the process by means of which the data provided, both by the customer and other means, are tested for accuracy, by making use of independent and trustworthy sources, for example genuine ID documents and supplementary inquiries.²⁰ The process of verification is more complex and requires extra input of the financial institution, which involves establishing whether or not identity information provided by the customer matches their actual identity.²¹

In principle, identifying and verifying customers is done prior to entering into the business relationship (before account opening, as well as before certain transactions are performed).²²

¹⁸ Meijling M, 'Whitepaper: Identification And Verification Of Natural Persons In Case Of Non-F2F Acceptance' (Kycnetblog.blogspot.co.at, 2014) < https://docs.google.com/document/d/1wyCt-JpRQQ8QEF_cPccqn0etAhjnLSpM6clF6AeQ3vA/edit > accessed 12 March 2016.

¹⁹ De Nederlandsche Bank, 'DNB Guidance On The Anti-Money Laundering And Counter-Terrorist Financing Act And The Sanctions Act Preventing The Misuse Of The Financial System For Money Laundering And Terrorist Financing Purposes And Controlling Integrity Risks' (DNB 2015) 17.

²⁰ *ibid.*

²¹ M. Meijling, *Identification and Verification of Natural Persons in case of non-F2F Acceptance* (KYCNet 2015).

²² De Nederlandsche Bank, *DNB Guidance On The Anti-Money Laundering And Counter-Terrorist Financing Act And The Sanctions Act Preventing The Misuse Of The Financial System For Money Laundering And Terrorist Financing Purposes And Controlling Integrity Risks* (DNB 2015) 20.

Anti-Money Laundering and Counter Terrorist Financing: The Current Legal Framework within the European Union

The term “anti-money laundering”, also referred to as AML, refers to the regulatory controls made use of by banks and other financial institutions in the identification, counteraction and reporting of activities involving money laundering. Anti-money laundering laws came into the international lime light with the creation of the Financial Action Task force, also known as the FATF, which is the main international body involved in the combatting of money laundering and terrorism financing.²³

The term “counter terrorist financing”, also referred to as CFT, refers to regulatory controls to strengthen the gathering of intelligence, the enforcement of the law, as well as the creation of financial restrictions aimed at preventing the transfer of funds for terrorist purposes.²⁴

The FATF’s international legal framework on anti-money laundering gained increasing importance in the early 2000s when the FATF initiated courses of action in order to publicly sift out countries whose regulations tackling anti-money laundering were lacking or faulty, or simply refused to cooperate internationally in the combatting of money laundering and terrorist financing.²⁵

This “naming and shaming” initiative resulted in a “FATF blacklist” that has proven to have tremendous impact, not only in raising global awareness on anti-money laundering and the prevention of terrorist financing, but also on encouraging countries to improve their local regulations on such issues.²⁶

When controlling the financial industry, most anti-money laundering regulations explicitly connect money laundering, which involves the origin or starting point from which the money

²³ Financial Action Task Force, 'About The FATF' (*Fatf-gafi.org*, 2012) <<http://www.fatf-gafi.org/trash/aboutfatf/whatisfatf/aboutthefatf.html>> accessed 12 March 2016.

²⁴ *ibid.*

²⁵ Financial Action Task Force. ‘About the Non-Cooperative Countries and Territories (NCCT) Initiative’ (*Fatf-gafi.org*, 2009) <<http://www.fatf-gafi.org/publications/fatfgeneral/documents/aboutthenon-cooperativecountriesandterritoriesncctinitiative.html>> accessed 12 March 2016.

²⁶ Muller W., Kalin C. and Goldsmith J., *Anti-Money Laundering* (John Wiley & Sons / Henley & Partners 2007) 78.

is criminally obtained, with the financing of terrorism, which primarily involves the money's end point or terminus.²⁷

A well-functional AML framework necessitates the criminalisation of money laundering within a jurisdiction. Secondly, it requires the appropriate regulatory watchdogs capable of effective law enforcement with the necessary devices for investigating, reporting suspicious activities, storing records and contributing information internationally when needed.

Laws counteracting money laundering and the financing of terrorist activities are structured to avert the financial system being utilised for criminal purposes. With regard to the AML legislative framework of the European Union (EU), the international standards created by FATF have played a great role in shaping what the Union has based its rules upon. The European Union has adapted the laws of the FATF and personalised them to meet the needs of the internal market as well as leave room for the national legislation of its member states to supplement union law.²⁸

The European Commission is currently part of the FATF and also has observer status with the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL).²⁹ MONEYVAL, which was established in 1997 as a subcommittee of the European Committee of the Council of Europe on Crime Problems (CDPC), is a regional body that operates under the mandate of the Council of Europe and reports to the FATF. Its main objective is to create effective mechanisms in the member states of the Council of Europe to fight money laundering and the financing of terrorism.³⁰ MONEYVAL additionally arranges events intended to share know-how in the combatting of money laundering and terrorist financing as well as provides trainings and seminars.

Aside from the global AML standards, there are various regulations existing at EU-level. Following the recommendations of the FATF, in June 2015, Directive 2015/849/EU on the prevention of the use of the financial system for the purposes of money laundering or terrorist

²⁷ Rodriguez R.M., *Is the European Union Doing Everything It Can to Force the Banks and the Financial Institutions to Comply With the Law?* (Lulu Press 2015) 5.

²⁸ *ibid.*

²⁹ Gilmore W.L.M., 'Terrorist Finance, Money Laundering and the Rise of Mutual Evaluation: A New Paradigm for Crime Control?' (2002) 4(2) *European Journal of Law Reform* 337–364.

³⁰ 'Council of Europe, 'About MONEYVAL' (*Coe.int*, 2016)
<https://www.coe.int/t/dghl/monitoring/moneyval/About/About_MONEYVAL_en.asp> accessed 12 March 2016.

financing, also known as the Fourth European Union Anti-Money Laundering Directive, came into force with the objective of safeguarding financial institutions from such dangers.³¹

This implementation of this directive by all EU member states is expected in 2017. Further EU-level standards are set out in Regulation 2015/847/EU on information accompanying transfers of funds. This regulation sets out provisions on information on payers and payees which is to be included with the transfer of money in any currency, aiming at counteracting, identifying and investigating money laundering and terrorist financing, in the event that one of the service providers participating in the transfer of funds is situated in the EU. It is aimed at creating greater transparency of money transfers and thus aiding the international criminal hunt-down.³²

The Fourth AML Directive has made EU AML regulations more aligned with those of the United States of America (USA), which has proven to be delightful information for banks and other financial institutions carrying out business in both jurisdictions.³³

The absence of synchronised AML regulations between the EU and the USA has convoluted AML compliance processes by multi-national financial institutions seeking to align their KYC mechanisms in all jurisdictions of operation. The Fourth AML Directive embraces further risk-based methods in comparison to the previous AML Directive.³⁴

Important to note is that specific parts of the Fourth AML Directive transcend EU requirements by inflicting fresh challenges on banks.³⁵ For example, the scope of the directive has broadened to include more public officials and member states of the EU are obliged to create new records of “ultimate beneficial owners” (UBOs), i.e. persons having ownership or control over a legal entity, and make this information available to third parties.

This new concept of beneficial ownership will be discussed more in detail later. The adoption of this directive further means that banks have new obligations to report suspicious

³¹ 4th AML Directive, Preamble.

³² CIMA, 'Anti-Money Laundering Regulations' (*Cimaglobal.com*, 2015) <<http://www.cimaglobal.com/Members/Members-handbook/Licencing-and-monitoring/Anti-money-laundering/Regulations/>> accessed 12 March 2016.

³³ PwC Financial Services Regulatory Practice, 'AML global alignment: Two steps forward, one step back' (*PwC.com* 2015) <<http://www.pwc.com/us/en/financial-services/regulatory-services/publications/aml-global-alignment.jhtml>> accessed 12 March 2016.

³⁴ 3rd AML Directive.

³⁵ PwC Financial Services Regulatory Practice, *AML global alignment: Two steps forward, one step back* (*PwC.com* 2015).

transactions, new customer due diligence or KYC requirements, as well as maintaining payment records.³⁶

The following tables show the regulators' initiatives, their corresponding KYC requirements and applicable regulations.

Initiative 1: Bank Customer Identification and Verification

KYC Requirement	Applicable Regulations
• Conduct customer due diligence/KYC according to risk categorisation • Politically exposed persons (PEPs) – enhanced KYC • Beneficial ownership determination and investigation • Taking into account various sanctions some customers are subject to	• Directive 2015/849/EU on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Fourth European Union Anti-Money Laundering Directive)³⁷ • Tax compliance acts such as the Foreign Account Tax Compliance Act of the United States (FATCA)³⁸ • FATF Recommendations³⁹ • International Sanctions legislation applicable to certain countries or persons⁴⁰

Source: JWG analysis of regulatory requirements for KYC information, February 2015⁴¹

³⁶ Rodriguez R.M., *Is the European Union Doing Everything It Can to Force the Banks and the Financial Institutions to Comply With the Law?* (Lulu Press 2015).

³⁷ 4th AML Directive.

³⁸ Foreign Account Tax Compliance Act of 2009 (US).

³⁹ Financial Action Task Force, 'International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation - FATF Recommendations' (FATF updated 2015).

⁴⁰ 'European Union - EEAS (European External Action Service) | Consolidated List Of Persons, Groups And Entities Subject To EU Financial Sanctions' (*Eeas.europa.eu*, 2016) <http://eeas.europa.eu/cfsp/sanctions/consol-list/index_en.htm> accessed 16 March 2016.

⁴¹ Regtechfs, 'The 2015 Challenge: Hurdling The KYC Bar' (*Regtechfs.com*, 2015) <<http://regtechfs.com/the-2015-challenge-hurdling-the-kyc-bar/>> accessed 12 March 2016.

Initiative 2: Categorisation

KYC Requirement	Applicable Regulations
• Tests of suitability and appropriateness • Bank customer classification • Risk assessments with regard to creditworthiness	• The Directive on markets in financial instruments (MiFID II) repealing Directive 2004/39/EC⁴² • Regulation on markets in financial instruments (MiFIR)⁴³ • Regulation No 648/2012/EU on OTC derivatives, central counterparties and trade repositories (EMIR)⁴⁴ • FATCA • Basel III – Agreement of the Basel Committee on Banking supervision (BCBS) to “strengthen global capital and liquidity rules with the goal of promoting a more resilient banking sector”⁴⁵

⁴² Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments [2014] OJ L173/349.

⁴³ Regulation No 600/2014/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments [2014] OJ L173/84.

⁴⁴ Regulation 648/2012/EU on OTC derivatives, central counterparties and trade repositories [2012] OJ L201/1.

⁴⁵ Basel Committee on Banking Supervision, 'Basel III: A Global Regulatory Framework For More Resilient Banks And Banking Systems' (www.bis.org, 2011) <<http://www.bis.org/publ/bcbs189.pdf>> accessed 16 March 2016.

Initiative 3: Monitoring

KYC Requirement	Applicable Regulations
• Monitoring of Sanctions some customers are subject to • Monitoring fraudulent activity • Monitoring misuse of the financial industry through criminal transactions • Monitoring suspicious activity	• International Sanctions legislation applicable to certain countries or persons • Anti-corruption legislation⁴⁶ • Regulation No 596/2014 on market abuse⁴⁷ • Directive 2014/57/EU on criminal sanctions for market abuse⁴⁸ • Fourth European Union Anti-Money Laundering Directive

Initiative 4: Reporting

KYC Requirement	Applicable Regulations
• Reporting on: – Transactions/trade/finance – Risk – Suspicious Activity – Sanctions – Tax – Beneficial ownership/control	• EMIR • MiFID II • Fourth European Union Anti-Money Laundering Directive • International Sanctions legislation • FATCA • Basel III

⁴⁶ Anti-corruption legislation, for example Convention drawn up on the basis of Article K.3 (2) (c) of the Treaty on European Union on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union [1997] OJ C195/1.

⁴⁷ Regulation No 596/2014/EU of the European Parliament and of the Council of 16 April 2014 on market abuse [2014] OJ L 173/1.

⁴⁸ Directive 2014/57/EU on criminal sanctions for market abuse [2014] OJ L 173/179.

Directive 2015/849 on the Prevention of the Use of the Financial System for the Purpose of Money Laundering or Terrorist Financing

The AML Directive 2015/849, in Article 1(2), states that ‘Member States shall ensure that money laundering and terrorist financing are prohibited.’⁴⁹

It replaces the old Directive 2005/60/EC (Third AML Directive) and adopts a risk-based legal framework that is targeted at preventing new threats and gaining uniformity across all the EU member states with regard to AML and CFT regulation.⁵⁰

In terms of what money laundering and terrorist financing comprises of, the Directive lists four types of conduct, if committed intentionally, as illegal acts that can be classified as such. They are as follows:

- ‘a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;
- (b) The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
- (c) The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;
- (d) Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).’⁵¹

The Fourth AML Directive is also concerned with Counter Terrorist Financing and the imposition of more client identification and verification obligations. It is additionally aimed at enhancing economic stability of the EU internal market by safeguarding its reliability and the

⁴⁹ 4th AML Directive, Article 1(2).

⁵⁰ 4th AML Directive, Preamble.

⁵¹ 4th AML Directive, Article 1(3).

effective operations of EU financial institutions, along with the lessening of regulatory challenges that institutions operating cross-border might face.⁵²

The scope in this directive has been broadened as compared to the third AML Directive. It applies mainly to the financial industry including banks, and also includes all goods traders that earn or gain cash payments that exceed 10, 000 Euros, an amount lower than what was required in the Third AML Directive.⁵³ This is irrespective of whether payments are made in multiple transactions or carried out in one whole transaction.⁵⁴

A brief overview on some of the primary modifications presented in this new directive is set out below:

Adoption of a Risk-Based Approach

The Fourth AML Directive requires EU member states to focus on risk assessments and equivalent risk-based approaches.⁵⁵

Recital 22 of the Directive states that ‘the risk of money laundering and terrorist financing is not the same in every case’ and that ‘accordingly, a holistic, risk-based approach should be used’, It further mentions that such an approach is ‘not an unduly permissive option for Member States and obliged entities. It involves the use of evidence-based decision-making in order to target the risks of money laundering and terrorist financing facing the Union and those operating within it more effectively.’⁵⁶

National Authorities are obliged to provide proof that appropriate action has been taken by the member state in order to identify, evaluate and lessen the risks associated with money laundering and terrorist financing by means of a “National Risk Assessment”.⁵⁷ Furthermore, obliged entities will be required to prove that they have taken measures to mitigate the same

⁵² Canestri D, 'Fourth EU AML Directive: What Is Missing? Section 319 Patriot Act And The New EU AML Directive' (2015) 23 European Journal of Crime, Criminal Law and Criminal Justice 214-240.

⁵³ 4th AML Directive, Article 2(1)(3)(b).

⁵⁴ *ibid.* Article 11 (b)(i).

⁵⁵ *ibid.* Article 4.

⁵⁶ *ibid.* Recital 22.

⁵⁷ *Ibid.* Recital 24.

risks, together with assessing the risks stemming from clients, products, certain locations and means in more perspicuous ways than required previously.⁵⁸

The reasons for having risk-based approach is due to the risks associated with money laundering and terrorist financing differing from one case to the other. It has become paramount that competent authorities and institutions within EU member states are efficient in identifying, assessing and understanding the risks of money laundering and terrorist financing and are subsequently able to respond to these risks by use of anti-money laundering and counter terrorist financing methods in their appropriate proportions.⁵⁹

Registry of Ultimate Beneficial Ownership

The Directive presents new measures to ensure additional transparency by the creation of national registers that are centralised and contain information on “beneficial ownership”. Article 3 of the Directive defines the beneficial owner as:

“Any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted”.⁶⁰

In the case of corporate entities the directive defines the beneficial owner as:

“The natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Union law or subject to equivalent international standards which ensure adequate transparency of ownership information.”

The Directive stipulates clear obligations for legal persons, as well as companies to obtain, hold and provide accurate, up-to-date and adequate information on beneficial ownership to

⁵⁸ Canestri D, *Fourth EU AML Directive: What Is Missing? Section 319 Patriot Act And The New EU AML Directive* (European Journal of Crime, Criminal Law and Criminal Justice 2015) 230.

⁵⁹ Verhage A, *The Routledge Handbook Of White-Collar And Corporate Crime In Europe* (Routledge 2015) 481.

⁶⁰ *ibid.* 481.

obliged entities that partake in customer due diligence processes as well as to provide such information to a centralised register or database.⁶¹

The necessity of having information on beneficial ownership is paramount in the tracking down of criminals who may conceal their identities behind commercial establishments. To prevent misuse of the financial institutions by criminals, member states are obliged to make information on the ultimate beneficial ownership to Financial Intelligence Units (FIUs).⁶²

Persons able to show “legitimate interest” with regard to money laundering and terrorism financing and other related crimes for example those involving fraud, tax evasion and corruption are able to proportionally access information on beneficial ownership, and in compliance with other Union laws such as data protection regulations.⁶³

Conducting On-going Monitoring

The Directive requires continuous scrutiny of customers, specifically in the outlining of aspects to take into account when conducting risk assessments of clients, as well as the constant monitoring of transactions taking place, including investigating the source of funds and making sure that the documents and other related information are up to date. Such monitoring should be carried out on the basis of risk, and from a practical perspective, the Directive requires that financial institutions such as banks should be able to provide evidence with regard to justifying the level of risk of each customer.⁶⁴

Obliged entities should assess all the information attained as part of their on-going monitoring of customers and other business entities in order to determine whether it influences the associated risk assessments.⁶⁵

⁶¹ 4th AML Directive, Article 30(3).

⁶² *ibid.* Article 30(2).

⁶³ *ibid.* Article 30(5).

⁶⁴ De Vido, S., ‘Anti-Money Laundering Measures versus European Union Fundamental Freedoms and Human Rights in the Recent Jurisprudence of the European Court of Human Rights and the European Court of Justice’ (2015) 16 German Law Journal 1271-1292.

⁶⁵ Joint Committee of the European Supervisory Authorities, ‘Joint Guidelines under Article 17 and 18 (4) of Directive 2015/849/EU on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions’ (2015) 061 Joint Consultation Paper.

Risks Associated with Politically Exposed Persons

Foreign politically exposed persons (PEPs) have been regarded as having high risk profiles due to the powerful public influence that they may have as well as their increased tendency to engage in corruption. Article 3(9) of the Directive defines “politically exposed person” as:

“A natural person who is or who has been entrusted with prominent public functions and includes the following:

- (a) Heads of State, heads of government, ministers and deputy or assistant ministers;
- (b) Members of parliament or of similar legislative bodies;
- (c) Members of the governing bodies of political parties;
- (d) Members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
- (e) Members of courts of auditors or of the boards of central banks;
- (f) Ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
- (g) Members of the administrative, management or supervisory bodies of State-owned enterprises;
- (h) Directors, deputy directors and members of the board or equivalent function of an international organisation.”⁶⁶

Unlike the Third AML Directive, the new Directive broadens the scope of PEPs to include also local PEPs, as seen above.⁶⁷

In terms of financial institutions’ relationships with PEPs, the Directive requires additional measures to be taken with regard to customer due diligence and that institutions have appropriate risk management systems in place in order to identify which beneficial owners are

⁶⁶ 4th AML Directive, Article 3(9).

⁶⁷ Ioannides E, *Fundamental Principles Of EU Law Against Money Laundering* (Ashgate Publishing Limited 2014).

PEPs, and appropriately mitigate the additional risk that PEPs might render by use of enhanced and on-going monitoring of such relationships.⁶⁸

Senior management approval is also needed to initiate business relationships with PEPs as well as to continue doing so.⁶⁹ Further measures are essential to ascertain the source and destination of funds of PEP transactions. The directive stipulates enhanced due diligence as a prerequisite for PEPs and that obliged entities are required to assess the new risk of beneficial owners that cease to be PEPs. This is to be applied for the duration of 18 months, which is a requirement of an extra six months in comparison to the previous AML directive.⁷⁰

As much as it seems quite stigmatizing, the preamble of the Directive makes it clear that the aim of having enhanced due diligence is a preventative measure and “should not be interpreted as stigmatising politically exposed persons as being involved in criminal activity”. It goes against the spirit of the Directive as well as the recommendations provided by the FATF for financial institutions to refuse to have business relations with PEPs for the sole reason of them being politically exposed.⁷¹

The nouvelle risk-based approaches, as well as the alterations made to PEP rules in the fourth AML Directive, validate the position that PEPs are vital in anti-money laundering.

New Customer Due Diligence Obligations

Customer Due diligence, also known as KYC, comprises of the identification of the customer and the verification of their identity based on documentation, information or data obtained from an independent and reliable source. It involves taking measures that are reasonable in order to ascertain beneficial ownership, which included investigating legal arrangements, business structures and customer’s control structure. KYC encompasses the scrutiny of customer transactions and their on-going monitoring based on risk-assessments as well as investigating the source of the funds and whether the documents relating to the customer are up to date.⁷²

⁶⁸ 4th AML Directive, Article 20.

⁶⁹ *ibid* Article 20 (b)(i).

⁷⁰ *ibid* Article 22.

⁷¹ *ibid*. Recital 33.

⁷² *ibid*. Article 13.

At present, obliged entities are compelled to carry out enhanced procedures when dealing with high-risk customers.⁷³ Simultaneously, where the customers are classified as low-risk, more simplified processes can be carried out.⁷⁴ The Directive requires obliged entities to be able to justify reasons for applying simplified due diligence and why they consider a customer that low of a risk, as well as set out minimum factors to take into consideration before conducting simplified due diligence to a customer.⁷⁵

The risk-assessment done by financial institutions should help it in identifying where its anti-money laundering and counter terrorist financing efforts should be centred. This applies to customer on-boarding as well as for the entire duration of the business relationship.⁷⁶

Conducting riskier KYC by virtual means, with the creation of branchless banks specifically, will be focus of this paper and discussed more thoroughly in the next section.

Reporting of Suspicious Transactions

The new AML regime involves obligations to report transactions that are suspicious, or any underlying criminal activity that is relevant to money laundering and terrorist financing, to the FIU.⁷⁷ The FIU should act as the central national unit responsible for the reception, analysis and the dissemination of results of its investigations to the appropriate authorities. The directive further stipulates that the meaning of “suspicious transactions” should also extend to transactions that have merely been attempted, irrespective of the amount involved.⁷⁸

Record Keeping

The new Directive describes a maximum retention period for documentation on customer due diligence after the ending of the business relationship of 5 years. Based on the national law of member states, this period may be prolonged up to 10 years, where the necessity and

⁷³ 4th AML Directive, Article 18.

⁷⁴ 4th AML Directive, Article 15(1).

⁷⁵ 4th AML Directive, Article 15(2).

⁷⁶ Joint Committee of the European Supervisory Authorities, The Risk Factor Guidelines (2015) Joint Consultation Paper 22.

⁷⁷ 4th AML Directive, Article 9(2).

⁷⁸ *ibid.* Article 33.

proportionality of keeping the records for a longer amount of time has been ascertained to facilitate the prevention, detection, investigation or prosecution of alleged money laundering or financing of terrorism.⁷⁹

New developments in EU AML and CFT law, as set out in the directive are important to take note of as they will form the new foundation of compliance mechanisms that banks will need to have after amendment of company systems, policies, procedures and controls in order to conduct branchless banking.

Digitization of KYC

The financial services industry is going through drastic changes in terms of digitization of business, and banks are keen to take up this cost-saving opportunity. With the introduction of online banking, there has been a rapid growth in use of online products and services, state of the art mobile applications, all changing customer experience and bringing significant growth potential in the financial sector, most especially in retail banking.

Identifying customers online creates a multitude of problems. There is no F2F identification in order to match customers with their photo ID and verify them. When customers open accounts remotely by virtual means, it is safer to require more identification procedures, and not just a one-step process such as requiring a copy of an ID document. For in absentia customers this would not suffice.⁸⁰

In general, purely based on practice, some of the main methods that have been used by banks within the EU when conducting online KYC are as follows:

- i. Asking for many ID documents at once
- ii. Asking for both primary and secondary documents in order to verify IDs of customers
- iii. Using verification texts or calls to telephone numbers provided in order to test if the information is valid

⁷⁹ 4th AML Directive, Article 40.

⁸⁰ Ioannides E, *Fundamental Principles Of EU Law Against Money Laundering* (Ashgate Publishing Limited 2014).

- iv. Double-checking information in public directories to prevent the use of fake IDs
- v. Verifying data obtained with customer credit reports
- vi. Requiring notarised documentation

Although banks have always been conducting customer due diligence before the introduction of the Fourth AML Directive, the introduction of branchless banking renders the whole process more complex, and more traditional banking methods utilised for the identification and verification of customers have begun to be substituted by more modern methods.

Branchless banking

Branchless banking is the provision of financial services and products outside the conventional means of bank branches. The reliance on information technology, such as mobiles, card-reading point of sales (POS), internet banking, and ATMs to carry out transactions plays a significant role in digital banking, with this new phenomena greatly reducing costs and ensuring better convenience to customers.⁸¹ Digital banking provides customers with a wider range of channels through which banking services can be accessed and further makes account opening easier and faster.⁸²

An essential part of the Fourth AML Directive is the obligation for financial institutions to “know their customer”. This is specifically shown in the obligations set out by this Directive to identify customers. Provisions that particularly correspond to non-face to face transactions are explicitly detailed, and apply to various situations, namely:

- i. Customers physically *in absentia* at the initiation of the business relationship
- ii. Instances where the bank customer is acting as an economic beneficiary, that is, on behalf of a physically *in absentia* third party.

⁸¹ CGAP 'Branchless Banking Diagnostic Template' (<https://www.cgap.org/>, 2010) 1 <<https://www.cgap.org/sites/default/files/CGAP-Branchless-Banking-Diagnostic-Template-Feb-2010.pdf>> accessed 14 March 2016.

⁸² PwC, 'Rebooting The Branch: Branch Strategy In A Multi-Channel, Global Environment' (<http://www.pwc.com/>, 2012) <<http://www.pwc.com/us/en/financial-services/publications/viewpoints/reinventing-branch-banking-network.html>> accessed 14 March 2016.

- iii. An instance where the customer is *in absentia*, however, is not a new customer to the bank, having already engaged in previous business relationships and having previously been identified by the banks KYC system.⁸³

Non Face-to-Face Transactions

Nowadays, banks are increasingly required to open bank accounts for customers who do not physically present themselves in person at a bank branch. This situation is increasing with the growth of banking digitization and the EU legal framework on AML and CFT need to ensure that financial and credit institutions within the EU conduct equally effective customer due diligence to *in absentia* clients as they do with physically present clients.

The Fourth AML Directive, in Annex III, lists non-face-to-face business relationships as potentially higher-risk factors, and this is due to the fact that Non-F2F situations foster anonymity and the risk of false identity, which is an increasing threat within the European Union.⁸⁴

The Directive requires that in the assessment of the risks of money laundering and terrorist financing, the member states of the EU as well as their obliged entities shall take into consideration “at least” the factors of these potentially higher risk situations.⁸⁵ It specifies the obligations that member states have to make sure that financial institutions take particular and appropriate measures to offset the increased risk of money laundering and terrorist financing which results from customers being physically absent, in order to be identified, during the creation of the business relationship, such as the opening of a bank account.

Specifically, non-F2F dealings test the ability of the KYC rules currently in place to guarantee the proper identification of bank customers and economic beneficiaries acting on behalf of third parties.⁸⁶

⁸³ 4th AML Directive, Article 18(3).

⁸⁴ *ibid.* Annex III.

⁸⁵ *ibid.* Article 18(3).

⁸⁶ European Commission, 'The Application Of Directive 91/308/EEC On The Prevention Of The Use Of The Financial System For The Purpose Of Money Laundering In Relation To The Identification Of Clients In Non-Face To Face Transactions And Possible Implications For Electronic Commerce' (2006) SEC 1792 Commission Staff Working Document, page 6.

Based on recommendation 15 of the FATF, financial institutions are required to pay special attention to any threats of money laundering that may arise as a result of new or developing technologies which may favour anonymity. Furthermore, they should take appropriate measures, if necessary, to mitigate the risks of using such technology for money laundering schemes. Above all, policies and procedures need to be in place by banks, to tackle any particular risks connected to non-F2F transactions or business relations.⁸⁷ Reasonable measures should be implemented in order to identify and verify the beneficial owner, which involves understanding the ownership and control structure of bank customers is critical.⁸⁸

Additionally, attributable to easy accessibility and speed, the increased risks associated with non-F2F transactions that take place in electronic commerce operations, should be taken into consideration.⁸⁹ The highest risk factor lies in the identification process, as electronic transactions are usually carried out non-F2F. Thus, properly identifying customers enables banks to tackle concerns associated with electronic commerce.⁹⁰

It should also be noted that, even though the transactions in themselves, taking place digitally by means of the internet, might not render additional risk in comparison to other non-F2F situations, the risks may be intensified by certain factors. Examples of these factors include:

- i. Speed of digital transactions
- ii. Easy accessibility to the service, irrespective of geographical setting or time
- iii. Easy creation of fake applications
- iv. The absence of physical documentation.⁹¹

Furthermore, electronic commerce transactions generate additional challenges in comprehending their nature and purpose, as well as in the verification of the identity of the customer, in addition to identifying parties involved in wire transfers.⁹²

The Directive points out mandatory measures on customer due diligence and Article 14 indicates that member states shall require that, in the event that obliged entities are unable to

⁸⁷ FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation –FATF Recommendations*, (FATF updated 2015) Recommendation 15.

⁸⁸ de Koker L, 'Money Laundering Control And Suppression Of Financing Of Terrorism' (2006) 13 *Journal of Financial Crime*, page 26.

⁸⁹ European Commission, *Staff Working Document (SEC 1792 2006)*, page 5.

⁹⁰ *ibid.* page 5.

⁹¹ *ibid.* page 18.

⁹² *ibid.*

comply with the customer due diligence requirements that are set out in Article 13, it shall not proceed with a transaction through a bank account, establish a business relationship or perform a transaction with potential customers and shall terminate the business relationship and consider reporting a suspicious transaction to the FIU in compliance with Article 33.⁹³

The new AML directive does not distinguish between the different non-F2F circumstances. Specifically, appropriate measures to identify the customer should be taken irrespective of whether the *in absentia* customer is performing a transaction or initiating a business relation with the bank. It is the role of each EU member state to develop suitable measures on a case-to-case basis, on condition that such measures are sufficient to balance out the increased risk of money laundering and terrorist financing that could stem from non-F2F dealings.⁹⁴

It is important to note that obliged entities should place equal importance on integrating such measures into their internal KYC compliance systems, in line with the customer due diligence requirements laid down in Chapter II of the Directive.⁹⁵

Although the same documentation could be submitted in both F2F and non-F2F, relationships, there are additional challenges in the identity verification of non-F2F customers. This problem is exacerbated in cases whereby mobile phone and electronic banking is used.

The risks in themselves are variable in nature, whether isolated or in combination with other others, and may increase or decrease the overall potential risk to the financial system. This in turn affects the appropriate degree of preventative action that needs to be carried out as a countermeasure, for example KYC measures.⁹⁶ Thus, there are situations in which enhanced KYC should be conducted and others in which simplified KYC would be fitting.

⁹³ 4th AML Directive, Article 14.

Article 33 (1) provides: “Member States shall require obliged entities, and, where applicable, their directors and employees, to cooperate fully by promptly:

(a) Informing the FIU, including by filing a report, on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, and by promptly responding to requests by the FIU for additional information in such cases; and

(b) Providing the FIU, directly or indirectly, at its request, with all necessary information, in accordance with the procedures established by the applicable law.

All suspicious transactions, including attempted transactions, shall be reported.”

⁹⁴ 4th AML Directive, Article 18

⁹⁵ Böszörményi J. and Schweighofer E., 'A Review Of Tools To Comply With The Fourth EU Anti-Money Laundering Directive' (2015) 29 International Review of Law, Computers & Technology.

⁹⁶ Kingah S. and Zwartjes M., 'Regulating Money Laundering For Terrorism Financing: EU–US Transnational Policy Networks And The Financial Action Task Force' (2015) 21 Contemporary Politics.

Enhanced Customer Due Diligence for Non F2F Situations

High-risk Customers and their transactions, that pose greater likelihood of engaging in money laundering or terrorist financing, should be scrutinized more extensively by the bank, and should be closely monitored throughout the entire duration of the business relationship.

Consequently, KYC policies and procedures should be intensified. The Directive's requirement of carrying out enhanced due diligence for non-F2F transactions is vital in the investigation of transactions likely to take place, as well as in the implementation of monitoring systems to detect suspicious operations.⁹⁷

Enhanced customer due diligence is laid down in Article 18 of the Directive, and shall be carried out by obliged entities using a risk-based approach. Article 18(1) states that 'in cases of higher risk that are identified by Member States or obliged entities, Member States shall require obliged entities to apply enhanced customer due diligence measures to manage and mitigate those risks appropriately.'

It should encompass the examination of the "background and purpose of all complex and unusual transactions, which have no apparent economic or lawful purpose" as far as it is reasonably possible.⁹⁸ The Directive also requires that the degree and nature of on-going monitoring be elevated in order to establish whether or not the transactions seem suspicious.⁹⁹

Transactions that give rise to any sort of suspicion must include, at minimum:

- i. Taking steps to understand the source and destination of the funds
- ii. Conducting more in-depth investigations into the customer's business to determine the customer's tendency to perform specific transactions
- iii. More frequent and detailed monitoring of customer transactions and business relationship.¹⁰⁰

When dealing with such high-risk customers, banks should assess which enhanced KYC measures to best suit a certain risky situation and to what extent supplementary information should be sought. Enhanced measures that banks shall apply may include:

⁹⁷ Joint Committee of the European Supervisory Authorities, *The Risk Factor Guidelines* (2015) Joint Consultation Paper 22.

⁹⁸ 4th AML Directive, Article 18(2).

⁹⁹ *ibid.*

¹⁰⁰ Joint Committee of the European Supervisory Authorities, *The Risk Factor Guidelines* (2015) Joint Consultation Paper 26.

- i. Obtaining greater amounts of KYC information
 - a. Concerning the identification of the beneficial owner and control structure to ease understanding on the amount of risk involved in the relationship. Examples of this may include:
 - i. Obtaining information on family members and close business partners of the customer,
 - ii. Obtaining information on the past and present business activities of the customer,
 - iii. Obtaining information from media sources.
 - b. Ascertaining the legitimacy of the nature and purpose of the business relationship with the customer to establish the level of risk posed by the customer, including:
 - i. Keeping track of the number, monetary amounts and rate of occurrence of transactions performed through bank accounts in order to identify any sudden deviations that seem suspicious
 - ii. Obtaining information explaining why the customer chose and insisted on a specific banking product over another that better suited their needs.
 - iii. Obtaining information on the end point to which the funds are bound,
 - iv. The nature of the business of the customer to facilitate understanding of his potential business relationship with the bank.
- ii. Obtaining better quality information for customer ID verification by:
 - a. Requiring the first payment to be conducted through another bank account that the customer has in his name with another European bank that is bound by similar KYC obligations,

- b. Ascertaining that the sources of the money involved in the customer's transactions have not been generated by criminal means and that they are in line with the bank's familiarity with the customer.
- iii. Conducting KYC checks more often to establish whether the risk profile of the customer has changed. This can be done by:
 - a. Obtaining senior management approval to initiate or continue business relationships with customers,
 - b. Reviewing business relationships more frequently to identify, assess and respond risk profiles of customers
 - c. Discovering the purpose of certain customer transactions.¹⁰¹

The Directive further stipulates that if banks fail to fulfil their KYC obligations, in situations where they question the legitimacy of purpose and nature of the business relationship or where they have reason to believe that they are unable to cope with the risk, then they should not enter into a business relationship with the corresponding customer. In the case where the customer is an already existing customer, then the banks should either suspend or terminate the relationship.¹⁰²

Additionally, it should be noted that just because the Directive requires a risk-based approach to be made use of with AML and CFT, it does not signify that banks should avoid business relations with high-risk customers altogether as this goes against the spirit of the Directive.¹⁰³

¹⁰¹ Joint Committee of the European Supervisory Authorities, *The Risk Factor Guidelines* (2015) Joint Consultation Paper, page 27 and 28.

¹⁰² 4th AML Directive, Article 14(4).

¹⁰³ Chance C, 'EU Regulatory Developments' (2015) 9 Law and Financial Markets Review, page 293-297.

Due Diligence Outsourcing

The Directive upholds the prospect of having obliged entities rely on third parties for carrying out their KYC obligations.¹⁰⁴ In situations where KYC is outsourced the Directive requires that obliged entities accept liability for subsequent monitoring on an on-going basis and that all obligations set out in the directive with regards to customer due diligence be fulfilled to the same degree.¹⁰⁵

Furthermore, the Directive, in Article 29, echoes that the use of an outsourcing service provider or agent does not render the situation any different or classify as performance by third parties, and is to be regarded as part of the obliged entity.¹⁰⁶

Understanding this discrepancy is essential in delineating the associated responsibilities. In situations where KYC and on-going monitoring is outsourced, it regarded as if it were performed by the obliged entity, i.e., the bank, and hence it is compliant with EU law.¹⁰⁷

Previously, banks have been reluctant to the outsourcing of KYC to other enterprises; however, with the introduction of the Fourth AML banks have wider capacities to consider such options.¹⁰⁸

Common Methods of ID Verification by Third parties within the EU

With the digitization of banking, outsourcing KYC to other agencies enables the banks to forego the use of branches and to be able to conduct their activities fully or partially online. This is both with regard to the initiation of business relationships, such as first-time account opening, as well as offering additional banking products and services to already existing customers of the bank.¹⁰⁹

¹⁰⁴ 4th AML Directive, Article 29.

¹⁰⁵ Paragraph 36 alongside Article 29 of the 4th AML Directive helps to illustrate the aim of the directive in this regard.

¹⁰⁶ 4th AML Directive, Article 29.

¹⁰⁷ Joint Committee of the European Supervisory Authorities, *The Risk Factor Guidelines* (2015) Joint Consultation Paper 12.

¹⁰⁸ Froomkin A, 'From Anonymity To Identification' (2016) 1 J. Reg. & Self-Reg.

¹⁰⁹ Vaithilingam S, Nair M and Thiyagarajan T, 'Managing Money Laundering In A Digital Economy' (2015) 16 Journal of Asia-Pacific Business.

The most common measures in place in member states today with regard to verifying non-F2F KYC by utilising qualified third parties include the following:

- i. Making use of qualified notaries, who identify customers appearing before them with proof such as passports, birth certificates, drivers' licenses, or other appropriate legal documentation issued by the government. The authenticity of these documents is checked and copies are made with a statement from the notary that it is a certified and true copy of the original version. Costs in this situation are covered by the customer and not the bank and can be quite inconvenient.¹¹⁰
- ii. Using diplomatic missions such as embassies and consulates to identify and verify customers on the bank's behalf.¹¹¹
- iii. Using credit institutions, where the customer has previously been identified and verified.¹¹²
- iv. Conducting KYC through insurance companies.
- v. Verifying customer identities using reliable courier services or post offices. This involves visits to residential addresses of customers in order to verify their identities, using devices that are able to test the authenticity of the ID documents, and get them to sign contracts on behalf of the bank. This method allows the bank customer to stay at home and have the courier service costs covered by the bank. Once ascertaining the originality of the ID documents of the customer, the courier submits proof of ID verification to the bank, allowing it to initiate or continue a business relationship with the client.¹¹³

¹¹⁰ European Commission, *Staff Working Document* (SEC 1792 2006), page 6.

¹¹¹ *ibid.* page 6.

¹¹² Isaacs M and Wilding R, 'Banks And Money Laundering– Certainty At Last?' (2015) 1 *Law and Financial Markets Review*, page 427-433.

¹¹³ M. Meijling, *Identification and Verification of Natural Persons in case of non-F2F Acceptance* (KYCNet 2015) 3.

- vi. Using other adequately reliable third parties on under the basis of a contract that permits them to perform customer due diligence in accordance with the Fourth AML Directive.¹¹⁴

It is important that the qualified third party ensures that their staff members have been properly trained in conducting KYC and in anti-money laundering and counter-terrorist financing according to the requirements of the fourth AML Directive as well as the global FATF requirements. Staff members should be reliable and knowledgeable about potentially high-risk customers as well as informed about the enhanced measures to be taken in correspondence to such groups of people.¹¹⁵

Nonetheless, according to the Directive, the bank has the ultimate responsibility with regard to conducting KYC in a correct manner. In the event of failure to comply with these obligations, liability cannot be transferred to the third party.¹¹⁶

It could be argued that the above examples do not qualify as ‘genuine’ non-F2F KYC as they involve the physical presence of the bank customers with the reliable third party.¹¹⁷

To circumvent having to constantly inquire about whether a third party has conducted various stages of the KYC process, another innovative advancement in digital banking is block-chain technology, which helps banks to provide evidence that all the appropriate KYC obligations have been conducted by the qualified third party.

This is a digital version of ‘notarised identity proof’, which evidences all the transactions that take place on the network. The so-called ‘block’ records all the latest transactions and once performed, they are added into the block-chain as a permanent database.¹¹⁸

¹¹⁴ European Commission, *Staff Working Document* (SEC 1792 2006), page 6.

¹¹⁵ Joint Committee of the European Supervisory Authorities, *The Risk Factor Guidelines* (2015) Joint Consultation Paper 22.

¹¹⁶ 4th AML Directive, Article 29.

¹¹⁷ Bilali G, 'Know Your Customer - Or Not' (2012) 43 University of Toledo Law Review.

¹¹⁸ Prableen Bajpai C, 'Blockchain Definition | Investopedia' (*Investopedia*, 2014) <<http://www.investopedia.com/terms/b/blockchain.asp#ixzz40c41h4fy>> accessed 14 March 2016.

Conducting Online KYC Without the Use of Third Parties

There are other methods of conducting KYC that does not require the outsourcing of KYC to third parties by the bank, for example, having fully digital methods of identifying and verifying customer identities.¹¹⁹

The drastic technological advances since the introduction of online banking have gained wide acceptance. In a modern-day society where almost every person owns a smartphone and has access to the internet, such a phenomena of virtual KYC has been made possible and is currently in use in a number of EU member states already.¹²⁰

Examples of current practices include:

- i. Requiring electronic signatures to identify customers. Utilisation of this method is increasing in many countries and provides an alternative means of customer verification as compared to the traditional method of collecting hard copy documents. The use of electronic signatures is more frequent in Belgium, the United Kingdom and Spain, who have successfully managed to do so within the boundaries of the risk-based legal framework required by the Directive.¹²¹
- ii. Video KYC, whereby customers are identified via means of webcam technology, and facial as well as age recognition software is used. The customer's ID is verified in real time virtually, by use of smartphone camera's or computer webcams. This involves customers holding up their identification document such as a passport to the webcam of their device, whereby the software instantly scans the name, date of birth and ID number of the customer as well as facially match the face of the customer with his photo ID, thus authenticating it using biometric scanning.¹²²

¹¹⁹ Froomkin A, *From Anonymity To Identification* (J. Reg. & Self-Reg. 2016) 1.

¹²⁰ Vaithilingam S, Nair M and Thiyagarajan T, *Managing Money Laundering In A Digital Economy* (Journal of Asia-Pacific Business 2015)16.

¹²¹ European Commission, *Staff Working Document* (SEC 1792 2006), page 10.

¹²² Barber N, 'Privacy: Can You Know Your Customer But Not Break The Rules' (2002) 10 Bank Accounting and Finance Journal.

Bilali G, Know Your Customer - Or Not (U Toledo L. Rev. 2012) 43.

- iii. Customers carrying out their own identification by making use of smartphones which are equipped with Near Field Communication (NFC) chips which are able to read radio frequency identification (RFID) chips and subsequently identify and track tags associated with certain objects. The majority of modern passports also contain RFID chips, which enables smartphones and other electronic devices equipped with NFC chips to read information stored on the passport chip.¹²³
- iv. Using electronic identity cards, which are physical ID cards that provide an online identification solution with pin-code verification, and in some circumstances also enabling customers to digitally sign electronic documents, in line with the European Directive on Electronic Signatures.¹²⁴
- v. Identifying the Customer by requiring them to perform their first monetary transaction through an already existing account in the name of the customer at another financial institution situated within the EU who is subject to the same KYC obligations.¹²⁵

Although the above methods seem highly simplified, they still have to be in accordance with the bank's obligations involving enhanced due diligence that the Directive requires for high-risk situations such as non-F2F KYC.¹²⁶

¹²³ Isaacs M and Wilding R., *Banks And Money Laundering– Certainty At Last?* (Law and Financial Markets Review 2015).

¹²⁴ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [1999] OJ L 13/12.

This directive is soon to be replaced in July 2016 by the "Regulation 910/2014/EU on electronic identification and trust services for electronic transactions in the internal market" ("e-IDAS" Regulation).

¹²⁵ 4th AML Directive, Article 19.

¹²⁶ Vaithilingam S, et al, *Managing Money Laundering In A Digital Economy* (Journal of Asia-Pacific Business 2015)16.

Digital KYC Evidence of Practice in the EU: Dissimilarity across member states

Most EU member states have already implemented laws addressing non-F2F KYC.¹²⁷ The particular methods of KYC to be performed domestically in non-F2F situations are found in the national laws, by-laws or among a combination of regulations, by means of which broad safeguards are recognised and secondary laws such as regulatory guidelines stipulate more precise or supplementary measures.¹²⁸

Where member states have not yet enacted laws that tackle non-F2F KYC, it could signify that such means of conducting KYC has not yet been legalised under national law, and therefore is not permissible, requiring that customer due diligence be performed in the physical presence of the customer.

Currently EU member states have put into effect three general methodologies with regard to non-F2F KYC:

- i. Non-F2F KYC is not allowed
- ii. Non-F2F KYC is allowed under certain conditions specified in national legislation, together with possible exemptions from the rule for exceedingly risky situations where the customer should be personally identified.
- iii. A risk-based approach is used, by means of which explicit rules are not provided and non-F2F KYC needs to be conducted by the obliged entity in relation to the risk posed by the customer.

First Approach: Non-F2F KYC is not allowed

A number of member states still do not permit the non-F2F identification of bank customers, for example, the Slovak Republic, Hungary and Romania. Such non-authorisation may also be consequential of having an absence of laws addressing this new method of conducting customer due diligence on bank customers *in absentia*.¹²⁹

¹²⁷ European Commission, *Staff Working Document* (SEC 1792 2006), page 6.

¹²⁸ *ibid.* paragraph 9.

¹²⁹ *ibid.* paragraph 11.

In these member states, with the exception of Romania, a reliable third party to conduct part of the KYC on behalf of banks is permitted as an alternative solution, whereby customers are still physically identified in the presence of courier personnel, notaries, other financial institutions, post services, diplomatic missions or insurance companies.¹³⁰

The use of reliable third parties could be said to not constitute ‘genuine’ non-F2F KYC as the bank customer is still physically identified in the presence of the third party. However, it is still important that the qualified third party ensures that their staff members have been properly trained in conducting KYC and in anti-money laundering and counter-terrorist financing according to the requirements of the fourth AML Directive and should be reliable and knowledgeable about potentially high-risk customers as well as informed about the enhanced measures to be taken in correspondence to such groups of people.¹³¹

In Romania, new customers are not permitted to open bank accounts online and be subject to digital KYC. The reason for this lies in the Romanian Ordinance No. 85/2004 (which implements EU Directive 2002/65/EC on the conclusion of distance contracts for financial services, the OUG 99/2006 Banking Act as well as in local laws on consumer protection, which all provide that any banking services and products sold by banks to customers are to be provided “only based on a written contract”, which is to be interpreted as existing as a hardcopy.¹³²

Existing bank customers in Romania, that already have a relationship with the bank, are permitted to operate in absentia on condition that enhanced due diligence is carried out. With regard to obtaining loan products in Romania, doing so online is not possible, as national law requires the customer’s physical presence at the bank in order to conclude the contract, especially for mortgage contracts.¹³³

In short, in line with Romanian national legal requirements, only existing clients of the bank can open an additional current account without visiting a bank branch, and non-F2F KYC is only permitted for existing customers of a bank, since KYC has theoretically already been conducted at the onboarding stage. First time customers are required to physically present

¹³⁰ PwC, 'Anti-Money Laundering: Know Your Customer Quick Reference Guide And Global AML Resource Map' (PwC, 2016) <<http://www.pwc.com/gx/en/industries/financial-services/publications/anti-money-laundering-know-your-customer-quick-reference-guide.html>> accessed 16 March 2016.

¹³¹ European Commission, *Staff Working Document* (SEC 1792 2006).

¹³² No.85/2004, on consumer protection on the conclusion and implementation of distance contracts for financial services 2004 (Romania).

¹³³ Gardikiotis C and Anitei N, *Money Laundering. National And European Regulations* (Jurnalul De Studii Juridice.2015).

themselves to the bank in order to conclude contracts, and digital KYC, in this case, is not permitted. Romanian law does not allow the use of third parties to circumvent this problem as third party use only applies to simplified due diligence processes which are, of course, not applicable with non-F2F situations i.e. high-risk situations.¹³⁴

In Hungary, Section 13 of Act LXXXV of 2009 on the Pursuit of the Business of Payment Service prescribes that the agreement for opening a deposit account shall be in writing, which is interpreted as F2F conclusion of contracts.¹³⁵ However, in accordance with Section 18 of the Act CXXXVI of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing (AML Act), the mandatory client identification and due diligence process can be accepted if it has been carried out by another bank located within the EU.¹³⁶

Second Approach: Non-F2F KYC is allowed under certain conditions specified in national legislation, together with possible exemptions from the rule for exceedingly risky situations where the customer should be personally identified.

Various member states permit non-F2F KYC, and this is usually as derogation from the general rule of conducting KYC on an F2F basis and, given that in certain cases, particular conditions are met. Examples of member states using this approach are Latvia and Spain, whereby it is required under national law to physically identify bank customers at the beginning of the business relationship at account opening, and requiring a copy of the customers ID documentation after a certain amount of time after the start of the business relationship.¹³⁷

Nonetheless, conducting KYC on a non-F2F basis may not be permitted by these member states in situations they deem particularly risky. Examples of such situations in which non-F2F KYC is prohibited are:

- i. When another company is appointed to act on behalf of third parties in non-F2F cases in relation to certain types of transactions. In

¹³⁴ Gardikiotis C and Anitei N, *Money Laundering. National And European Regulations* (Jurnalul De Studii Juridice.2015).

¹³⁵ Act LXXXV on the Pursuit of the Business of Payment Services 2009 (Hungary) Section 13.

¹³⁶ Act CXXXVI on the Prevention and Combating of Money Laundering and Terrorist Financing 2007 (Hungary) Section 18.

¹³⁷ European Commission, *Staff Working Document* (SEC 1792 2006), page 7, paragraph 12.

Belgium, it is not permitted to have KYC conducted by a third party business introducer on a non-F2F basis. In this case, the bank making use of the third party business introducer retains ultimate accountability for failure to perform adequate KYC.

- ii. At the initiation of the business relationship between banks and new customers, such as at account opening. Non-F2F ID verification for already-existing bank customers would be permitted, as KYC has previously been conducted adequately. In this scenario, the bank would only have to ascertain whether new data obtained from the customer matched with data previously obtained from the customer at the start of the business relationship.
- iii. Where customers are ineligible. Particular restrictions could apply to customers who, for example, have their main residence outside the EU, in a country that is non-compliant (unless certain precautions have been taken, such as obtaining confirmation in writing from another bank situated within the EU, who has already performed appropriate KYC based on the requirements of the Directive, with which the customer already has a permanent business relationship).

In Slovenia, it is permitted to conduct KYC on a non-F2F basis of both Slovenian nationals who are non-residents and non-resident foreigners, on condition that those countries in which they reside are on the list of compliant countries paying regard to anti-money laundering and counter terrorism financing, as required by the FATF. The Slovenian Ministry of Finance is responsible for drafting this list.

- iv. Where the money involved in transactions is in the form of cash. In the Netherlands, banks are permitted to perform KYC of in absentia customers if the transaction does not involve cash. The initial payment is undertaken through an account in the name of the customer at another bank registered within the EU.

- v. Where there are transactions in bearer securities. Such securities differ from the more common types in the sense that there are no records of the owner or the transactions with regard to ownership.¹³⁸

It is important to note that even in cases where non-F2F KYC is allowed under usual circumstances, physically identifying a customer may possibly be necessary to balance the outcome of non-F2F KYC when certain risks arise. This includes, for example, inconsistencies in the data obtained, the existence of unusually high risks, or suspicion of avoiding direct ID checks.¹³⁹

In the Czech Republic, national law permits the opening of a digital account or deposit account fully online by new as well as existing customers, with no need to physically present oneself at a bank branch.¹⁴⁰ Czech law allows KYC to take place on a non-F2F basis, under a remote financial services agreement, provided that it fulfils all Czech anti-money laundering legal requirements, which are:

- i. All data required for customer identification have been obtained by the bank
- ii. Photocopies of customer ID documents have been made
- iii. Information with regard to the purpose as well as the nature of the business relationship has been attained
- iv. Money has been transferred from an existing account that the potential customer has with another bank situated within the EU (who have already conducted KYC of the client) to the new account.¹⁴¹

The same KYC requirements apply to existing customers of the bank.¹⁴²

With regard to obtaining loan products such as overdrafts, credit cards and consumer loans, the same KYC requirements applicable to current account opening apply. Czech law also does not distinguish between conducting business by virtual means with private individuals and conducting online business with small to medium enterprises (SME).

¹³⁸ European Commission, *Staff Working Document* (SEC 1792 2006), page 7.

¹³⁹ *ibid.* page 7.

¹⁴⁰ Law No. 89/2012 Coll. Civil Code 2012 (Czech Republic).

¹⁴¹ Act No. 253/2008 on selected measures against legitimisation of proceeds of crime and financing of terrorism 2008 (Czech Republic).

¹⁴² *ibid.*

In short, non-F2F identification is permitted in the Czech Republic, provided that specific national criteria concerning AML are fulfilled. The use of ‘reliable third parties’ to personally identify the bank customers, such as notaries or couriers trained in and informed about AML issues, may be used. In the case where banks do not wish to make use of notaries or couriers, Czech law provides for the use of other sufficiently reliable third parties under a contractual relationship.

National KYC laws in the Czech Republic also permit the scanning of ID documents to banks in combination with a small monetary transfer to the new bank account as part of the non-F2F KYC process.¹⁴³

In the Slovakia with regard to new customers, the opening of digital current accounts remotely is not allowed under the national law system. With regard to the verification of the identity of new customers, Act 297/2008 on the Prevention of Legalisation of Proceeds of Criminal Activity and Terrorist Financing provides that verification of the identity of natural person should be understood as verifying the ‘appearance of the person by comparing it to the appearance on his identification document in his physical presence’.¹⁴⁴

Existing customers’ physical presence in order to open online accounts, however, is not required. In Slovakia there is no difference in conducting online business with private individuals or SME, provided that consent of the client (or its legal representative) required under national law, is obtained and the original documentation is at the disposition of the bank. Obtaining loan products online, such as overdrafts, credit cards, and consumer loans, are not permissible under Slovak law.¹⁴⁵

As circumvention to restricting the opening of bank accounts and purchasing additional banking services and products remotely, Section 13 of this Act could still make branchless banking possible, as the law permits obtaining data and documentation necessary to conduct KYC from a credit or financial institution which operates in the territory of the EU. This approach however may be costly and time consuming.¹⁴⁶

¹⁴³ PwC, Anti-Money Laundering: *Know Your Customer Quick Reference Guide And Global AML Resource Map* (PwC, 2016).

¹⁴⁴ Act 297/2008 on the Prevention of Legalisation of Proceeds of Criminal Activity and Terrorist Financing 2008 (Slovak Republic).

¹⁴⁵ *ibid.*

¹⁴⁶ PwC, Anti-Money Laundering: *Know Your Customer Quick Reference Guide And Global AML Resource Map* (PwC, 2016).

Another alternative option of conducting branchless KYC is by engaging a reliable third party, as provided by Act 277/2008, to identify the customer on behalf of the customer. This third party, like in the case of the Czech Republic, may be a courier or notary.¹⁴⁷

A new development with regards to KYC in Slovakia has been the introduction of electronic identification systems (eID KYC) as an alternative to the acquisition of identity data through collecting traditional paper documentation. All residents of Slovakia will soon get an eID alongside a machine to read the eCard. This is a relatively new development and will take time to be fully implemented.¹⁴⁸

Third Approach: A risk-based approach is used, by means of which explicit rules are not provided and non-F2F KYC needs to be conducted by the obliged entity in relation to the risk posed by the customer.

With this approach, national laws in a number of member states do not clearly define precise situations eligible for non-F2F identification and neither do they provide specific exemptions. Instead, financial institutions adopt a risk-based approach, and take suitable measures according to the risks at hand. This is the case in the United Kingdom, where a completely risk-based approach has been applied.

In the UK, non-F2F cases require further information to be collected by banks such as information from credit bureau checks, utility bills containing the customer's physical address and other bank statements. Depending on the amount of risk posed by a customer, banks may investigate a customer's location, behaviour, products and services being used by the customer, or the nature of the intended business relationship, in order to assess the risk profile of the customer.¹⁴⁹

This approach involves taking into consideration the higher possibility of money laundering with non-F2F dealings. Member states adopting such an approach, currently in line with the Fourth AML Directive will not need to drastically amend their national laws by the 2017 implementation deadline.

¹⁴⁷ Act No. 277/2008 Coll. establishing classification symbols for categorizing and ranking accommodation establishments 2008 (Slovakia).

¹⁴⁸ SDW, 'Slovakia To Allow eID Holders To Update Civil Registry | Security Document News' (*Securitydocumentworld.com*, 2016) <<http://www.securitydocumentworld.com/article-details/i/12145/>> accessed 16 March 2016.

¹⁴⁹ European Commission, *Staff Working Document* (SEC 1792 2006), page 8.

Costs of Digital KYC

While branchless banking is indeed cost effective for banks with regards to the long-term gains of digitization, identifying customers on a non-F2F basis usually results in extra costs not only for the customer, but also for the system as well as for the institutions on the short term.¹⁵⁰

These costs originate as early as from the initial stages of the bank entering into the business relationship with the potential client.¹⁵¹

Undeniably so, and subject to the kinds of transactions performed, remotely conducted banking operations may offer banks a change to save significant amounts of money later on.¹⁵²

- Extra costs for the customer may be a result of having to pay for documentary evidence, for instance, having their ID documents checked and certified by notaries.¹⁵³
- Additional costs for the financial institution may originate from having to pay for costly new software systems as part of their compliance processes.¹⁵⁴
- Costs for the system relate to issues of duplication. Since it is compulsory for each institution involved in the ‘chain’ of providing financial services to conduct comparable KYC, there is a high probability of duplication with regards to KYC of the same customer. As a result of such replication, in addition to further aspects that render the attainment of customer information more difficult, such as obtaining information on customers operating under corporations or other legal

¹⁵⁰ Schroeder A, Hodge R and Morse E, 'Electronic Payments: Winnowing The Network And Avoiding The Shadows' (*Papers.ssrn.com*, 2015) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567806> accessed 14 March 2016.

¹⁵¹ European Commission, *Staff Working Document* (SEC 1792 2006), page 12.

¹⁵² *ibid.* paragraph 24.

¹⁵³ Gill M, 'Preventing Money Laundering Or Obstructing Business?: Financial Companies' Perspectives On 'Know Your Customer' Procedures' (2004) 44 *British Journal of Criminology*.

¹⁵⁴ Joyce B, 'E- Diligence: Money Laundering Risks In The Electronic Arena' (2001) 5 *J of Money Laundering Control*.

entities, stakeholders usually consider costs and other business-related burdens too high in relation to the possible gains.¹⁵⁵

Fresh Challenges of Digital KYC: the Drive for Effectiveness and Efficiency

The requirement of having supplementary KYC for non-F2F situations could possibly be off-putting to obliged entities, assuming its arduousness. In a few instances, measures to be taken for non-F2F customers could be discouraging on a bank's choice of selling certain products or services, and this could also be true for the onboarding of certain customers.¹⁵⁶

Conversely, banks should not overlook the fundamental aim of anti-money laundering regulations in place today, which is to be well acquainted with customers and to use such knowledge of their customers accordingly.¹⁵⁷

It could be questioned, from this viewpoint, whether existing KYC procedures used in the verification of customer identities could be bettered.

In addition, the adequacy of the system to efficiently accomplish its AML aims, in this respect, is also connected to the price paid to maintain such KYC standards. Details of such costs are referenced in the previous section of this paper.

From a stakeholder standpoint, the money spent on conducting digital KYC on a non-F2F basis, outweighs the tangible benefits. However, the new AML Directive provides burden and cost amelioration through requiring the employment of a risk-based approach. Such risk-based approaches would provide enhanced flexibility to financial institutions with regard to resource allocation. This practical tool is essential in the creation of a strong foundation on which decisions based on evidence and risk is achievable.¹⁵⁸ This ultimately enhances the system of KYC in terms of effectiveness.

¹⁵⁵ European Commission, *Staff Working Document* (SEC 1792 2006), page 12, subparagraph 2.

¹⁵⁶ European Commission, *Staff Working Document* (SEC 1792 2006), page 13.

¹⁵⁷ *ibid.* paragraph 26.

¹⁵⁸ ACAMS Today, 'Europe's Upcoming Fourth AML/CFT Directive' ([www.acams.org](http://files.acams.org/pdfs/2015/Europes_Upcoming_Fourth_AML_CFT_Directive.pdf), 2015) <http://files.acams.org/pdfs/2015/Europes_Upcoming_Fourth_AML_CFT_Directive.pdf> accessed 14 March 2016.

With regard to the future of anti-money laundering, the challenges that exist are twofold, namely, third-party reliance and adopting a risk-based approach.¹⁵⁹

¹⁵⁹ European Commission, *Staff Working Document* (SEC 1792 2006), page 14.

Other Legal Issues arising out of Digital KYC

The use of digital KYC, in other words non-F2F customer due diligence, usually rings alarm bells with the creation of three major legal concerns, namely, protecting the data of customers, being dependent on third parties, and the difficulty and impracticability of obtaining information.¹⁶⁰

Data Protection Law

Data protection of individuals is addressed in a variety of EU legal instruments.

Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provides that ‘everyone has the right to the protection of personal data concerning him or her’.¹⁶¹

Article 8(1) of the Charter of Fundamental Rights of the European Union (hereinafter the Charter) states that ‘Everyone has the right to the protection of personal data concerning him or her’ and that in accordance with Article 8(2), ‘such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law’.¹⁶²

Article 52(1) of the Charter provides that ‘any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms’.¹⁶³ Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others’.¹⁶⁴

¹⁶⁰ European Commission, *Staff Working Document* (SEC 1792 2006), page 11, paragraph 20.

¹⁶¹ Consolidated Version of the Treaty on the Functioning of the European Union (2010) OJ C 83/47, Article 16(1).

¹⁶² Charter of Fundamental Rights of the European Union [2012] OJ C 326/391, Article 8(1).

¹⁶³ *ibid.* Article 52(1).

¹⁶⁴ *ibid.*

The implementation of the fourth AML Directive involves the pooling, analysing, assessing, storing and the sharing of data.¹⁶⁵ While fully protecting fundamental rights enshrined in the Charter of Fundamental Rights of the European Union.¹⁶⁶

Article 2(a) of the Data Protection Directive defines ‘personal data’ as ‘any information relating to an identified or identifiable natural person (“data subject”)’ and ‘an identifiable person’ as ‘one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity’.¹⁶⁷

The handling of such data is allowed only for the purposes laid down in the Directive, which are:

- i. Conducting KYC
- ii. On-going monitoring
- iii. Investigating suspicious activity
- iv. Reporting suspicious transactions
- v. Identifying the beneficial owner or controller of corporate entities.
- vi. Identifying PEPs
- vii. Sharing information by competent authorities and other obliged entities¹⁶⁸

The collection and subsequent processing of personal data should be limited to ‘what is necessary’ with regards to the above purposes.¹⁶⁹ This means that personal data should not be ‘further processed’ in a manner that is not aligned with these purposes, such as processing for commercial purposes.¹⁷⁰ The Directive strictly prohibits this.¹⁷¹

¹⁶⁵ Ioannides E, *Fundamental Principles Of EU Law Against Money Laundering* (Ashgate Publishing Limited 2014).

¹⁶⁶ Böszörményi J. and Schweighofer E., *A Review Of Tools To Comply With The Fourth EU Anti-Money Laundering Directive* (International Review of Law 2015) 29.

¹⁶⁷ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31, Article 2.

¹⁶⁸ Böszörményi J and Schweighofer E., *A Review Of Tools To Comply With The Fourth EU Anti-Money Laundering Directive* (International Review of Law 2015).

¹⁶⁹ Siclari D, 'The Forthcoming EU 4th Anti Money Laundering Directive and the Supervision of Payment Institutions' (2014) 4 Bankpedia Review.

¹⁷⁰ *ibid.*

¹⁷¹ Chong A and Lopez-De-Silanes F, 'Money Laundering And Its Regulation' (2015) 27 Economics & Politics.

According to Article 3(1), the Personal Data Directive applies to ‘the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system’.¹⁷²

In general, identifying customers *in absentia* involve acquiring and managing information on customer identity in various phases of the KYC process.¹⁷³ This process also involves obtaining information from multiple sources – firstly, the customer, followed by information from other institutions, persons or media, as well as external databases.¹⁷⁴

KYC, the sharing of data and privacy requirements vary from one country to the next, however the Directive stipulates minimum requirements to be met with regards to privacy and data protection throughout member states.¹⁷⁵

The necessity to act in accordance with data protection obligations is often a hindrance to the collection and processing of data involving customer identities.¹⁷⁶ The Directive obliges member states to provide means and methods to protect the privacy of customers, professional secrecy as well as confidentiality, and take appropriate steps to identify, assess and mitigate data protection concerns.¹⁷⁷

National risk assessments form a fundamental part of the information collected in the KYC process. However, such assessments should involve anonymised data only.¹⁷⁸ FIUs are required to make use of technologies for data matching with that of other FIUs in an anonymous manner while ensuring full protection of personal data with the only aim of detecting subjects of interest in other member states and identifying their corresponding funds and proceeds.¹⁷⁹

¹⁷² Chong A and Lopez-De-Silanes F, *Money Laundering And Its Regulation* (Economics & Politics 2015) 27.

¹⁷³ *ibid*, paragraph 21.

¹⁷⁴ Barber N, *Privacy: Can You Know Your Customer But Not Break The Rules* (Bank Accounting and Finance Journal 2002)10.

¹⁷⁵ Siclari D, *The Forthcoming EU 4th Anti Money Laundering Directive and the Supervision of Payment Institutions* (Bankpedia Review 2014) 4.

¹⁷⁶ *ibid*.

¹⁷⁷ 4th AML Directive, Article 7.

¹⁷⁸ Mitsilegas V, *Money Laundering Counter-Measures In The European Union*(Kluwer Law International 2003)

¹⁷⁹ 4th AML Directive, Article 57.

It is of great importance that acting in line with the FATF Recommendations is done so in a manner fully compliant with Union law, especially in terms of EU data protection law and the Charter of Fundamental rights of the European Union.¹⁸⁰

The European Commission adopted its proposal for a General Data Protection Regulation (GDPR) in January 2012, to replace Directive 95/46/EC, which will see the biggest change to data protection and privacy within the EU since 1995.¹⁸¹

The Council aims to formally adopt this regulation early this year, which is aimed at unifying and strengthening data protection of individuals within the EU and will entail greater penalties for non-compliance.¹⁸²

This may mean that mandatory risk assessments take place within companies with additional personnel hired to ensure data protection in-house, creating extra financial burden on companies, especially those operating on a smaller scale.¹⁸³

From time to time, the restrictions arising from data protection regulations are at odds with the requirements concerning KYC, especially in cases whereby information on customer identity attained via non-F2F means vis-à-vis ID documentation, has to be finalised by acquiring additional information from third parties, such as public registers.¹⁸⁴ This is also true in situations where further means to authenticate the ID documents supplied are needed.¹⁸⁵ Consequently, this could render the KYC process rather burdensome.¹⁸⁶

Third Party Dependence

In order to mitigate the higher risk of conducting KYC non-F2F, relying on a third party may be essential according to the requirements of national law.¹⁸⁷ However, when third parties are

¹⁸⁰ Charter of Fundamental Rights of the European Union.

¹⁸¹ De Hert P and Papakonstantinou V, 'The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System For The Protection Of Individuals' (2012) 28 Computer Law & Security Review.

¹⁸² *ibid.*

¹⁸³ *ibid.*

¹⁸⁴ Naheem M, 'AML Compliance – A Banking Nightmare? The HSBC Case Study' (2015) 12 International Journal of Disclosure and Governance.

¹⁸⁵ McGuire L, 'Banking On Biometrics: Your Bank's New High-Tech Method Of Identification May Mean Giving Up Your Privacy' (1999) 33 Akron Law Review 441.

¹⁸⁶ *ibid.* 441.

¹⁸⁷ Ioannides E, *Fundamental Principles Of EU Law Against Money Laundering* (Ashgate Publishing Limited 2014).

relied upon to identify and verify customers, the ultimate responsibility of conducting accurate KYC still lies with the bank.¹⁸⁸

Although there are certain benefits of relying on third parties to conduct KYC, such as speeding up customer onboarding and improving customer experience, there are a number of negative impacts of such reliance.¹⁸⁹

Relying on third parties does not mean obtaining less extensive data on the customer. KYC requirements remain the same whether conducted directly by the banks or through third parties.¹⁹⁰ Additionally, using third parties is not always permissible or fitting to certain situations given by national law.¹⁹¹

The transfer of data between various institutions is necessary to guarantee the sharing of relevant and potentially confidential information on customer identity and risk profiles.¹⁹²

Nevertheless, the obstacles concerning customer data protection limitations are twofold. Firstly, banks are not forced to give out information concerning customer accounts to other obliged entities. Additionally, although banks may be permitted to do so, banks predominantly refuse to for commercial reasons such as giving other market participants advantages in terms of competition.¹⁹³

Secondly, if banks are keen on information sharing with other institutions, there are data protection regulations that they have to comply with, which may be an obstacle to such data transfer in the first place.¹⁹⁴ This is both with regard to situations where information from a third party is requested as well as the information associated with a monetary transfer from an already existing account in the customer's name with another bank located in the EU.¹⁹⁵

¹⁸⁸ 4th AML Directive, Article 29.

¹⁸⁹ PricewaterhouseCoopers LLC, 'FinCEN: Know Your Customer Requirements' (*Corp.gov.law.harvard.edu*, 2016) <<https://corp.gov.law.harvard.edu/2016/02/07/fincen-know-your-customer-requirements/>> accessed 15 March 2016.

¹⁹⁰ *ibid.*

¹⁹¹ *ibid.*

¹⁹² European Commission, *Staff Working Document* (SEC 1792 2006), page 12.

¹⁹³ *ibid.* paragraph 22.

¹⁹⁴ *ibid.*

¹⁹⁵ *ibid.* subparagraph 2.

Impracticability of Access to Information

There are sometimes obstacles in terms of obtaining information in order to complete the KYC process, especially in the final stages of customer ID verification.¹⁹⁶

Attaining some documentation is cumbersome, for example, the sourcing of information on the identity and power of attorney of those acting on behalf of legal persons. This is specifically true for large enterprises, which employ a number of persons to act on their behalf in conducting financial transactions through bank accounts.¹⁹⁷

There are many challenges involved with the identification and verification of the identities of natural persons who exercise effective control. An illustration of this would be a situation in which a company makes use of the financial institution to set up an account.

Companies usually have many strata of ownership, which may be established in order to conceal the identities of natural persons, who actually possess ownership of those companies.¹⁹⁸ Reasons for creating these ownership layers, which could actually be completely legal, could be to avoid legal and tax implications.¹⁹⁹

The structures of these companies are complex, and this is especially so when they are deliberately made to secrete the identities of certain natural persons, which could be a hindrance in the KYC process.²⁰⁰

¹⁹⁶ Naheem M, 'AML Compliance – A Banking Nightmare? The HSBC Case Study' (2015) 12 International Journal of Disclosure and Governance.

¹⁹⁷ European Commission, *Staff Working Document* (SEC 1792 2006), page 12.

¹⁹⁸ Mitsilegas V and Gilmore B, 'The EU Legislative Framework Against Money Laundering And Terrorist Finance: A Critical Analysis In The Light Of Evolving Global Standards' (2007) 56 International and Comparative Law Quarterly.

¹⁹⁹ *ibid.*

²⁰⁰ *ibid.*

Conclusion

Providing banking products and services on a non-F2F basis entails heightened risks, and banks often go to great lengths to safeguard themselves against abuse and ensure compliance with AML legal obligations both at national and supranational levels.

Digital banking will create heightened needs for banking security and there are potentially considerable commercial gains for those banks that attain the trust of their customers through their capacity to successfully manage to deliver reliable and secure services. Recently, there has been considerable attention given to the growing amount of cyber crime in terms of regulation by the EU.

Owing to the nature of their product portfolios, banks, and most particularly digital banks, are exceptionally prone to risks of money laundering. The problems involved with *in absentia* customers are, and could potentially be, considerably large. The main problem is the fostering of anonymity that digital banking may create and in turn, the increased risk of money laundering and the financing of terrorism. With the ease at which digital accounts can be opened, regardless of location and time and in a matter of minutes, makes digital banking attractive for criminals. New pieces of legislation, designed to adapt to the new digital age, have emerged, reforming and harmonizing the EU data protection rules as well as addressing cyber crime. IT security is paramount and banks need to ensure this for themselves and not depend on third parties to do so.

The new regulatory regime governing KYC within the EU under the Fourth AML Directive has been a major game changer, resulting in the need for financial institutions to conduct more extensive KYC than ever before in their endeavours in the digitization of their products and services. The AML directive tackles the problem of higher-risk posed by non-F2F dealings, by requiring banks to take enhanced measures of customer due diligence for non-F2F dealings with their customers, as well as puts increasing pressure on banks to reveal more about their corresponding business relationships. This applies beyond the level of due diligence of the customer, and incorporates acquisition of information to a greater extent and involving other persons or entities and other fields of law such as tax.

The complete eradication of bank branches in the EU has been achievable so far with low cost, less technical barriers and feasibility of non-F2F KYC on condition that bank obligations

under the Directive appropriately address and reassess AML/CFT risk profiles of the customer, beneficial ownership and tax status among other things. Greater understanding of digital identity results in enhanced provision of services by banks as well as evidence of fulfilment of KYC obligations.

Together with the advancement in digital banking, banks are currently pushing to innovate and simultaneously make sure that they comply with their new AML/CFT obligations. Despite the arduous nature of trying to innovate whilst remain within the boundaries of the Fourth AML Directive; the development of new technologies in the field of digital banking in the recent years has made this possible.

Notwithstanding the Directive imposing complete restructuring of bank policies and KYC procedures, especially in terms of beneficial ownership, in an era where innovative smartphone technologies are accessible regardless of location and time, the barriers to entry have been significantly lowered.

Procedural measures that EU member states have proposed as solutions to the problems arising out of digital KYC, in order to mitigate the risks of non-F2F transactions, has varied across the EU, but some of the most prevalent measures of tackling potential KYC problems in non-F2F dealings within the member states include the use of electronic signatures, requiring supplementary documentation to verify identities, making use of video KYC to scan ID documents and compare them to the faces of customers in real time using facial and age recognition software, using RFID and NFC chips in smartphone technology to identify tags associated with authentic ID documentation as well as requiring first payments to be made through already existing accounts in the customer's name at other financial institutions who have already performed KYC.

The Directive also enables the outsourcing of customer due diligence to reliable third parties, acknowledged by the regulator, as a unique method of conducting KYC. In a current digital era, demonstrating evidence of the fulfilment of different stages of KYC can be performed by the use of block chain technology, for example.

Problems arising from such application of the above digital KYC methods, however, consist of three major legal concerns, namely:

- i. Protecting the data of customers,
- ii. Being reliant on third parties, and

iii. Difficulty and impracticability of obtaining information on customers.

With regard to their adequacy and extent to which these main procedural measures taken by most member states as part of their digital KYC processes, ensure the prevention of money laundering and terrorist financing, such processes in practice have proven to be rather successful. Many banks within the member states are already making use of this new technology, and have been, for a number of years.

There has been a very limited amount of EU case law on with regard to digital KYC within the union, as such digital phenomena are still rather new and haven't been submitted to the courts. Regulators within the EU also have yet to build up experience with regulating this new 'digital market', and will be in need of a certain amount of time in order to get acquainted with such a market in terms of regulation. However, after the transposition of the new AML Directive in 2017, we expect to see various interpretations from the Court of Justice of the EU with regards to these matters.

With harsher penalties being the result of inadequate KYC, and the introduction of personal liability for senior management personnel, banks will be further compelled to ensure that KYC is carried out appropriately and as accurately as possible, both by themselves and through the use of third parties when operating in non-F2F situations. The new enhanced KYC requirements for digital clients, reporting obligations and record keeping requirements will force banks to employ a plethora of mechanisms and data fields that cater for diverse situations and the quality of data collected as part of the KYC process is expected to be much more thought-out than ever before. Information of bank clients will be subjected to greater control through the multiplicity of reporting systems required in order to efficiently counter the increased risks of money laundering and terrorist financing associated with the digitalisation of banking. With the new AML regime provided in the directive, regardless of whether it involves tax issues, commerce, or suspicious transactions reporting, government watchdogs will obtain more customer data than in the past.

How banks cope with KYC, and other issues with regard to compliance, in the upcoming years is yet to be seen, however, banks can leverage on the present regulatory framework in order to aid innovation in digital banking technology as well as gain competitive advantages over other market participants.

Bibliography

1. Directive 2015/849/EU of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing [2015] OJ 2 141/73.
2. Duhaime C, 'What Is Money Laundering? Duhaime's Anti-Money Laundering Law In Canada' (*Antimoneylaunderinglaw.com*, 2014)
<<http://www.antimoneylaunderinglaw.com/aml-law-in-canada/what-is-money-laundering>> accessed 12 March 2016.
3. Bantekas I., 'The International Law Of Terrorist Financing' (2003) 97 The American Journal of International Law.
4. Mulligan D., 'Know Your Customer Regulations and the International Banking System: Towards a General Self-Regulatory Regime' (1998) 22 Fordham International Law Journal.
5. Byrne J, 'Know Your Customer: What Happened And What Happens Next?' (2000) 3 J of Money Laundering Control.
6. Sullivan K, *Anti-Money Laundering In A Nutshell* (Springer 2015).
7. 'International Guide To Money Laundering Law and Practice, 4th Edition' [2016] Commonwealth Law Bulletin
<<http://www.tandfonline.com/doi/full/10.1080/03050718.2015.1019689>> accessed 12 March 2016.
8. Chong A and Lopez-De-Silanes F, 'Money Laundering And Its Regulation' (2015) 27 Economics & Politics.
9. BCBS, *Sound Management of Risks Related to Money Laundering and Financing of Terrorism* (BIS 2014) 10.
10. Meijling M, 'Whitepaper: Identification And Verification Of Natural Persons In Case Of Non-F2F Acceptance' (*Kycnetblog.blogspot.co.at*, 2014) <
https://docs.google.com/document/d/1wyCt-JpRQQ8QEF_cPccqn0etAhjnLSpM6clF6AeQ3vA/edit > accessed 12 March 2016.
11. De Nederlandsche Bank, 'DNB Guidance On The Anti-Money Laundering And Counter-Terrorist Financing Act And The Sanctions Act Preventing The Misuse Of The Financial System For Money Laundering And Terrorist Financing Purposes And Controlling Integrity Risks' (DNB 2015) 17.

12. Financial Action Task Force, 'About The FATF' (*Fatf-gafi.org*, 2012)
<<http://www.fatf-gafi.org/trash/aboutfatf/whatisfatf/aboutthefatf.html>> accessed 12 March 2016.
13. Financial Action Task Force. 'About the Non-Cooperative Countries and Territories (NCCT) Initiative' (*Fatf-gafi.org*, 2009) <<http://www.fatf-gafi.org/publications/fatfgeneral/documents/aboutthenon-cooperativecountriesandterritoriesncctinitiative.html>> accessed 12 March 2016.
14. Muller W., Kalin C. and Goldsmith J., *Anti-Money Laundering* (John Wiley & Sons / Henley & Partners 2007) 78.
15. Rodriguez R.M., *Is the European Union Doing Everything It Can to Force the Banks and the Financial Institutions to Comply With the Law?* (Lulu Press 2015) 5.
16. Gilmore W.L.M., 'Terrorist Finance, Money Laundering and the Rise of Mutual Evaluation: A New Paradigm for Crime Control?' (2002) 4(2) *European Journal of Law Reform* 337–364.
17. 'Council of Europe, 'About MONEYVAL' (*Coe.int*, 2016)
<https://www.coe.int/t/dghl/monitoring/moneyval/About/About_MONEYVAL_en.aspx> accessed 12 March 2016
18. Canestri D, 'Fourth EU AML Directive: What Is Missing? Section 319 Patriot Act And The New EU AML Directive' (2015) 23 *European Journal of Crime, Criminal Law and Criminal Justice* 214-240.
19. Verhage A, *The Routledge Handbook Of White-Collar And Corporate Crime In Europe* (Routledge 2015) 481.
20. CIMA, 'Anti-Money Laundering Regulations' (*Cimaglobal.com*, 2015)
<<http://www.cimaglobal.com/Members/Members-handbook/Licencing-and-monitoring/Anti-money-laundering/Regulations/>> accessed 12 March 2016.
21. PwC Financial Services Regulatory Practice, 'AML global alignment: Two steps forward, one step back' (*PwC.com* 2015) <<http://www.pwc.com/us/en/financial-services/regulatory-services/publications/aml-global-alignment.jhtml>> accessed 12 March 2016.
22. Regtechfs, 'The 2015 Challenge: Hurdling The KYC Bar' (*Regtechfs.com*, 2015)
<<http://regtechfs.com/the-2015-challenge-hurdling-the-kyc-bar/>> accessed 12 March 2016.
23. Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments [2014] OJ L173/349.

24. Regulation No 600/2014/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments [2014] OJ L173/84.
25. Regulation 648/2012/EU on OTC derivatives, central counterparties and trade repositories [2012] OJ L201/1.
26. Regulation No 596/2014/EU of the European Parliament and of the Council of 16 April 2014 on market abuse [2014] OJ L 173/1.
27. Directive 2014/57/EU on criminal sanctions for market abuse [2014] OJ L 173/179.
28. De Vido, S., 'Anti-Money Laundering Measures versus European Union Fundamental Freedoms and Human Rights in the Recent Jurisprudence of the European Court of Human Rights and the European Court of Justice' (2015) 16 German Law Journal 1271-1292.
29. Joint Committee of the European Supervisory Authorities, 'Joint Guidelines under Article 17 and 18 (4) of Directive 2015/849/EU on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions' (2015) 061 Joint Consultation Paper.
30. 'Branchless Banking Diagnostic Template' (<https://www.cgap.org/>, 2010) 1 <<https://www.cgap.org/sites/default/files/CGAP-Branchless-Banking-Diagnostic-Template-Feb-2010.pdf>> accessed 14 March 2016.
31. PwC 'Rebooting The Branch: Branch Strategy In A Multi-Channel, Global Environment' (<http://www.pwc.com/>, 2012) <<http://www.pwc.com/us/en/financial-services/publications/viewpoints/reinventing-branch-banking-network.html>> accessed 14 March 2016.
32. European Commission, 'The Application Of Directive 91/308/EEC On The Prevention Of The Use Of The Financial System For The Purpose Of Money Laundering In Relation To The Identification Of Clients In Non-Face To Face Transactions And Possible Implications For Electronic Commerce' (2006) SEC 1792 Commission Staff Working Document.
33. Financial Action Task Force, 'International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation - FATF Recommendations' (FATF updated 2015).
34. de Koker L, 'Money Laundering Control And Suppression Of Financing Of Terrorism' (2006) 13 Journal of Financial Crime, page 26.

35. Böszörményi J and Schweighofer E, 'A Review Of Tools To Comply With The Fourth EU Anti-Money Laundering Directive' (2015) 29 *International Review of Law, Computers & Technology*.
36. Kingah S and Zwartjes M, 'Regulating Money Laundering For Terrorism Financing: EU–US Transnational Policy Networks And The Financial Action Task Force' (2015) 21 *Contemporary Politics*.
37. Isaacs M and Wilding R, 'Banks And Money Laundering– Certainty At Last?' (2015) 1 *Law and Financial Markets Review*, page 427-433.
38. Chance C, 'EU Regulatory Developments' (2015) 9 *Law and Financial Markets Review*.
39. Froomkin A, 'From Anonymity To Identification' (2016) 1 *J. Reg. & Self-Reg.*
40. Vaithilingam S, Nair M and Thiyagarajan T, 'Managing Money Laundering In A Digital Economy' (2015) 16 *Journal of Asia-Pacific Business*.
41. Bilali G, 'Know Your Customer - Or Not' (2012) 43 *University of Toledo Law Review*.
42. Prableen Bajpai C, 'Blockchain Definition | Investopedia' (*Investopedia*, 2014) <<http://www.investopedia.com/terms/b/blockchain.asp#ixzz40c41h4fy>> accessed 14 March 2016.
43. Barber N, 'Privacy: Can You Know Your Customer But Not Break The Rules' (2002) 10 *Bank Accounting and Finance Journal*.
44. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [1999] OJ L 13/12.
45. Schroeder A, Hodge R and Morse E, 'Electronic Payments: Winnowing The Network And Avoiding The Shadows' (*Papers.ssrn.com*, 2015) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567806> accessed 14 March 2016.
46. Gill M, 'Preventing Money Laundering Or Obstructing Business?: Financial Companies' Perspectives On 'Know Your Customer' Procedures' (2004) 44 *British Journal of Criminology*.
47. Joyce B, 'E- Diligence: Money Laundering Risks In The Electronic Arena' (2001) 5 *J of Money Laundering Control*.
48. ACAMS Today, 'Europe's Upcoming Fourth AML/CFT Directive' (www.acams.org, 2015)

- <http://files.acams.org/pdfs/2015/Europes_Upcoming_Fourth_AML_CFT_Directive.pdf> accessed 14 March 2016.
49. Consolidated Version of the Treaty on the Functioning of the European Union (2010) OJ C 83/47.
 50. Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.
 51. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.
 52. Siclari D, 'The Forthcoming EU 4th Anti Money Laundering Directive and the Supervision of Payment Institutions' (2014) 4 Bankpedia Review.
 53. Chong A and Lopez-De-Silanes F, 'Money Laundering And Its Regulation' (2015) 27 Economics & Politics.
 54. Mitsilegas V, *Money Laundering Counter-Measures In The European Union* (Kluwer Law International 2003).
 55. De Hert P and Papakonstantinou V, 'The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System For The Protection Of Individuals' (2012) 28 Computer Law & Security Review.
 56. Naheem M, 'AML Compliance – A Banking Nightmare? The HSBC Case Study' (2015) 12 International Journal of Disclosure and Governance.
 57. McGuire L, 'Banking On Biometrics: Your Bank's New High-Tech Method Of Identification May Mean Giving Up Your Privacy' (1999) 33 Akron Law Review 441.
 58. PricewaterhouseCoopers LLC, 'FinCEN: Know Your Customer Requirements' (*Corpgov.law.harvard.edu*, 2016)
<<https://corpgov.law.harvard.edu/2016/02/07/fincen-know-your-customer-requirements/>> accessed 15 March 2016.
 59. Naheem M, 'AML Compliance – A Banking Nightmare? The HSBC Case Study' (2015) 12 International Journal of Disclosure and Governance.
 60. Ioannides E, *Fundamental Principles Of EU Law Against Money Laundering* (Ashgate Publishing Limited 2014).
 61. Mitsilegas V and Gilmore B, 'The EU Legislative Framework Against Money Laundering And Terrorist Finance: A Critical Analysis In The Light Of Evolving Global Standards' (2007) 56 International and Comparative Law Quarterly.
 62. Foreign Account Tax Compliance Act of 2009 (US).

63. Basel Committee on Banking Supervision, 'Basel III: A Global Regulatory Framework For More Resilient Banks And Banking Systems' (*www.bis.org*, 2011)
<<http://www.bis.org/publ/bcbs189.pdf>> accessed 16 March 2016.
64. Gardikiotis C and Anitei N, 'Money Laundering. National and European Regulations' [2015] *Jurnalul de Studii Juridice* <<https://www.ceeol.com/search/article-detail?id=290361>> accessed 16 March 2016.
65. 'European Union - EEAS (European External Action Service) | Consolidated List Of Persons, Groups And Entities Subject To EU Financial Sanctions' (*Eeas.europa.eu*, 2016) <http://eeas.europa.eu/cfsp/sanctions/consol-list/index_en.htm> accessed 16 March 2016.
66. Convention drawn up on the basis of Article K.3 (2) (c) of the Treaty on European Union on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union [1997] OJ C195/1.
67. Act LXXXV on the Pursuit of the Business of Payment Services 2009 (Hungary).
68. Act CXXXVI on the Prevention and Combating of Money Laundering and Terrorist Financing 2007 (Hungary).
69. Law No. 89/2012 Coll. Civil Code 2012 (Czech Republic).
70. Act No. 253/2008 on selected measures against legitimisation of proceeds of crime and financing of terrorism 2008 (Czech Republic).
71. PwC, 'Anti-Money Laundering: Know Your Customer Quick Reference Guide And Global AML Resource Map' (PwC, 2016)
<<http://www.pwc.com/gx/en/industries/financial-services/publications/anti-money-laundering-know-your-customer-quick-reference-guide.html>> accessed 16 March 2016.
72. Act 297/2008 on the Prevention of Legalisation of Proceeds of Criminal Activity and Terrorist Financing 2008 (Slovak Republic).
73. Act No. 277/2008 Coll. establishing classification symbols for categorizing and ranking accommodation establishments 2008 (Slovakia).
74. SDW, 'Slovakia To Allow eID Holders To Update Civil Registry | Security Document News' (*Securitydocumentworld.com*, 2016)
<<http://www.securitydocumentworld.com/article-details/i/12145/>> accessed 16 March 2016.

English Abstract

Since the introduction of online banking, innovation within the financial sector has become increasingly apparent. For reasons of efficiency and cost-saving, banks are relying less on conducting their activities in physical branches, and customers are able to open bank accounts and obtain other banking products and services remotely. However, non-face to face interaction with customers fosters anonymity, which entails heightened risks. One of the most important regulatory requirements is for banks to know their customers by conducting customer due diligence (CDD/KYC) in order to mitigate the risks of financial fraud, identity theft and prevent money laundering or the financing of terrorism. Therefore, it is vital that the laws governing KYC, for financial institutions offering online services, adapt in order to mitigate these additional risks. New legislation designed for the new digital age has emerged within the EU and the new regulatory regime governing KYC under the Fourth AML Directive requires financial institutions to conduct enhanced due diligence for higher risk situations. Solutions to the problems associated with digital KYC have varied across the EU, however some of the most prevalent measures include the use of electronic signatures, requiring supplementary documentation to verify identities, making use of video KYC to scan ID documents, using facial and age recognition software, using RFID and NFC chips in smartphone technology to identify tags associated with authentic ID documentation, requiring first payments to be made through already existing accounts in the customer's name at other EU financial institutions, or the outsourcing of customer due diligence to reliable third parties.

German Abstract

Seit Einführung des Online-Bankings haben sich Innovationen im Finanzsektor stark bemerkbar gemacht. Aus Gründen der Effizienz und Kostenersparnis führen Banken weniger Aufgaben in den Filialen aus, was dazu führt, dass Kunden Konten und andere Finanzprodukte aus der Ferne beziehen. Nichtpersönliche Transaktionen mit Kunden fördern Anonymität was auch große Risiken mit sich bringt. Eine der wichtigsten regulatorischen Vorgaben für Banken ist das Kennenlernen ihrer Kunden in dem sie eine Due-Diligence-Prüfung durchführen um Risiken zu mildern die mit Finanzbetrug und Identitätsdiebstahl verbunden sind. Geldwäsche und Terrorismusfinanzierung zu verhindern gehören auch zu den wesentlichsten Aufgaben einer Due-Diligence-Prüfung und somit ist es wichtig, dass sich KYC-Gesetze für Finanzinstitutionen, die Onlinedienste anbieten, anpassen um diese Risiken zu reduzieren. Neue Gesetzgebungen für die neue digitale Ära wurden innerhalb der EU entworfen und die neuen Regulierungsregime der vierten AML-Richtlinie, die das KYC-Verfahren regeln, verlangen von Finanzinstitutionen verstärkte Due-Diligence-Prüfungen für erhöhte Risikosituationen. Lösungen für Probleme die mit dem digitalen KYC-Verfahren verbunden sind, variieren quer durch die EU. Einige der vorherrschenden Maßnahmen umfassen jedoch die Verwendung von elektronischen Signaturen, welche zusätzliche Nachweise verlangen um die Identität festzustellen. Diese verwenden Video KYC um ID-Dokumente einzuscannen, Gesichtserkennung und Alterserkennungssoftware welche RFID und NFC – Chips in Smartphone-Technologie nutzt um Kennzeichen zu identifizieren die mit authentischen ID-Dokumenten verbunden sind. Hier werden zuerst Zahlungen durch existierende Konten im Namen eines Kunden an andere Finanzinstitutionen in der EU oder die Auslagerung der Due-Diligence an zuverlässige dritte Parteien unternommen.