Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

European Union Law Working Papers

No. 34

The Fourth European Anti-Money Laundering Directive: A Critical Review of the Interaction between the Risk Based Approach, Customer Due Diligence and Beneficial Ownership

Wouter ter Bogt

2018

European Union Law Working Papers

Editors: Siegfried Fina and Roland Vogl

About the European Union Law Working Papers

The European Union Law Working Paper Series presents research on the law and policy of the European Union. The objective of the European Union Law Working Paper Series is to share "works in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The working papers can be found at http://ttlf.stanford.edu.

The European Union Law Working Paper Series is a joint initiative of Stanford Law School and the University of Vienna School of Law's LLM Program in European and International Business Law.

If you should have any questions regarding the European Union Law Working Paper Series, please contact Professor Dr. Siegfried Fina, Jean Monnet Professor of European Union Law, or Dr. Roland Vogl, Executive Director of the Stanford Program in Law, Science and Technology, at:

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Wouter ter Bogt studied Belgian Law and European and International Business Law in Brussels and Vienna. He is currently pursuing a career within the financial services industry in Vienna. His main areas of interest are regulatory banking compliance, international affairs, and lobbying.

General Note about the Content

The opinions expressed in this student paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This European Union Law Working Paper should be cited as:
Wouter ter Bogt, The Fourth European Anti-Money Laundering Directive: A Critical Review of the Interaction Between the Risk Based Approach, Customer Due Diligence and Beneficial Ownership, Stanford-Vienna European Union Law Working Paper No. 34, http://ttlf.stanford.edu.

Copyright

Abstract

This paper focuses on the widespread problem of money laundering which is seen as a prominent threat to the European and global economy. Since the creation of the European Union, the Member States, in cooperation with the European Commission, have taken measures to fight money laundering in the EU. Over the years, the EU presented itself as a fervent opponent of money laundering by implementing several anti-money laundering directives and taking measures to counter the financing of terrorism. The latter is an important current issue in the EU, as exemplified by the latest terrorist attacks in Paris, London, and Brussels. The implementation of new directives with an emphasis on the prevention of money laundering and terrorist financing became one of the priorities of the EU. In June 2015, the European Union finalized a highly ambitious project by voting on the Fourth Anti-Money Laundering Directive. This new directive seems to be necessary, but it is also subject to criticism by academics and others for being insufficient in many regards. This thesis will investigate the relevance and importance of former Anti-Money Laundering Directives, and will especially focus on the *ratione legis* behind the Fourth Anti-Money Laundering Directive. More precisely, it will clarify the new features of this directive and their interaction with each other. Moreover, possible deficiencies will be critically analyzed before a conclusion is provided on the adequacy of the new directive.

Table of Contents

Introduction

'Money laundering is giving oxygen to organised crime'.

Enrique Pena Nieto

Following the Second World War, the European continent has been subject to several drastic changes. The creation of the European Coal and Steel Community (followed by the European Economic Community, the European Community, and the European Union) changed European society in a positive way. Nowadays, the European Union (EU) is one of the wealthiest and most developed regions in the world, thanks in large part to its creation of a robust internal market. However, progress is almost always accompanied by undesired results; the creation of this internal market has also facilitated money laundering and the financing of terrorism through complex corporate vehicles. The internal market allows for the free movement of goods, services and people, which creates the perfect conditions for criminal organisations to launder money or finance terrorism. Consequently, the systematic creation of an internal market has required far-reaching measures and legislation on a European-wide level. The criminal organisations operating in and via the EU try to build different kinds of complicated systems whose goal is to hide the illicit source of proceeds in order to bring these proceeds back into the legal financial system. Although this paper will mainly focus on European legislation, the activities of terrorism financing and money laundering occur all over the world.

Indeed, money laundering and the illegal financing of terrorism organizations are a problem today in the EU and worldwide. The EU is one of the strongest and largest entities in the world in many fields such as economics, developmental assistance, and the protection of fundamental rights. With this kind of power comes responsibility. The EU has for years maintained and nurtured its vision of creating an immensely powerful internal market, which

is a process being realized in steps. But several shortcomings have emerged throughout the years. One of the problems inherent in the creation of the internal market, as mentioned above, is the emergence of opportunities for money laundering and terrorism finance through corporate vehicles. Organized crime syndicates and terrorist cells are becoming more creative and ruthless. In order to finance their criminal activities, they resort to sophisticated financing strategies. Such crime syndicates and terrorist cells need to convert proceeds from their criminal activities into 'legitimate' earnings from businesses. This is, by and large, the concept of money laundering. It occurs worldwide, and it affects economies, countries, companies, and citizens. Due to their ingenuity and expertise in in business strategy, criminals are able to construct creative methods to launder money. This concept of corporate crime will be discussed in-depth, but suffice it to say that it infringes upon the furtherance of European principles.

Since the very beginning, the European Community (EC) has taken an active role in the development of regional and international measures against money laundering. Some of the first steps taken were those of the United Nations (UN) in 1988, concerning drug trafficking, as well as those of the Council of Europe in 1990, with the 1990 Money Laundering Convention. Moreover, in that same period, the EC decided to take part in the Financial Action Task Force (FATF) and even played a leading role in the creation of the original Forty Recommendations[1]. The creation of these international standards was a very important starting point in the fight against money laundering.

The term 'organized crime' is subject to on-going revisions, and there are different categories of organized crime. Furthermore, organized crime is composed of many different criminal activities. The different kinds of criminal activities grouped under the term 'organized crimes' are characterized by a certain level of sophistication, rationality and continuity.

[1] Bill Gilmore, Dirty Money: the evolution of international measures to counter money laundering and the financing of terrorism *(*3rd edition, Council of Europe Publishing, 2004) 89-90.

When it comes to the modus operandi of money launderers, financial and credit institutions are usually the first-level contact point. Banking institutions are the most frequently used instruments by money launderers due to several factors. These include the range of services provided by financial institutions such as deposits, loans, and foreign exchange. With the help of banking institutions, criminals move illegal money through transferring accounts, and the source of illegally obtained money can be concealed.[2] The latest KPMG Global Anti-Money Laundering Survey of 2014 acknowledges that money laundering continues to be significant and poses increasing risks to the financial sector, in particular.[3] This survey attests to the fact that money laundering is a real problem in the financial sector and its risk should not be underestimated; therefore banking institutions should equip themselves with adequate infrastructure to screen for and identify money-laundering risks, for example by developing criteria capable of identifying 'suspicious transactions'.[4] Money laundering is a severe problem for banking institutions and for the EU as a whole. It is the lifeblood of crime, as without banks, criminals would have no mechanism by which to launder their money and claim it as clean.

Chapter 1: Definitions

1 Money Laundering

"Money laundering refers to a financial transaction scheme that aims to conceal the identity, source, and destination of illicitly-obtained money. The money laundering process can be broken down into three stages. First, the illegal activity that garners the money places it in the launderer's hands. Second, the launderer passes the money through a complex scheme of

[2] Abiola Idowu, Kehinde Obasan, 'Anti-Money Laundering Policy and its Effects on Bank Performance' (2012) 5 Business Intelligence Journal, 372.
[3] KPMG, 'Gbobal Anti-Money Laundering Survey 2014' (2014), 10. <https://assets.kpmg.com/content/dam/kpmg/pdf/2015/03/global-anti-money-laundering-survey-latest.pdf> accessed 26 Juli 2017.

[4].Garrigues Favarel, Thomas Godefroy, Pierre Lascoumes, 'Sentinels in the Banking Industry: Private Actors and the Fight against Money Laundering in France', (2007) British Journal of Criminology, 1.

transactions to obscure who initially received the money from the criminal enterprise. Third, the scheme returns the money to the launderer in an obscure and indirect way."[5]

There are several definitions of money laundering, depending on whether it is being approached from a legal, economic or political point of view. Several institutions have created comparable definitions, and all mainstream definitions have a similar main concept. Every definition identifies money laundering as a crime that is not easily tracked down by authorities. This is because there is no physical entity that is able to provide information which would help the authorities to discover that an asset has been obtained in an illegal way.[6] A selection of definitions will now be presented.

The European Union defines money laundering as follows;

> 3. *For the purposes of this Directive, the following conduct, when committed intentionally, shall be regarded as money laundering:*
>
> *(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*

[5] Money Laundering, <https://www.law.cornell.edu/wex/money_laundering> accessed 6 April 2017.
[6] Guy Stessens, 'Money Laundering a New International Law Enforcement Model' (Cambridge University Press, 2000) 160.

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).[7]

Interpol created a rather similar definition: *'[A]ny act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources'.*[8]

The FATF defines the activity as: '*[T]he processing of…criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source'.*[9]

The definition used by the FATF is held as the international standard, although it is stated in a very brief way. The EU states in its explanatory memorandum the importance of the combat against money laundering and recognizes the transnational aspect of the activity. Therefore, the EU aims for cooperation with other institutions such as Interpol, the UN and the FATF. All institutions acknowledge the far-reaching consequences of the illegal activity.

1.1 Stages of Money Laundering

The activity of money laundering is generally characterized by the following three stages. Firstly, cash with an illegal source is placed into the financial system. Secondly, this money is converted into book money through different sophisticated transactions designed to, in the

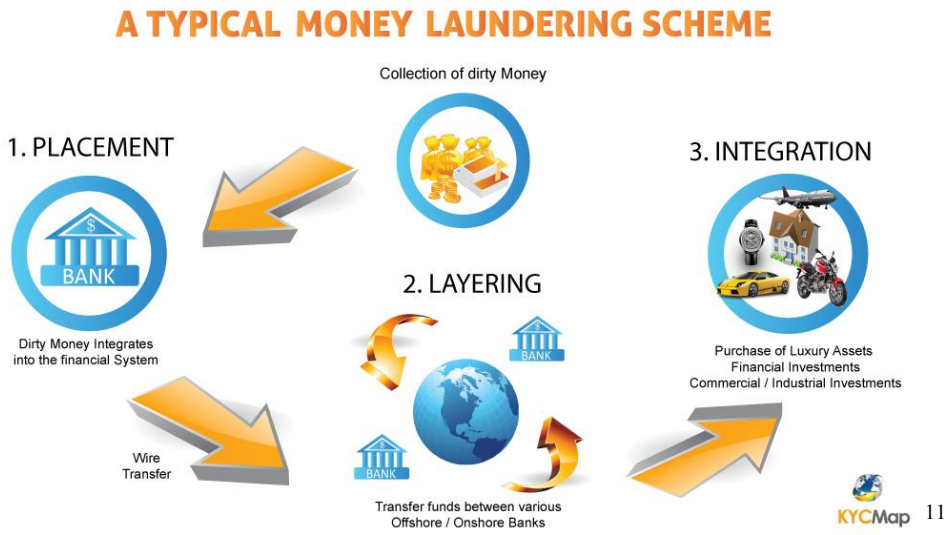
---

[7] Council Directive 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L141/73.

[8] International Criminal Police Organization, 'Money Laundering', <https://www.interpol.int/Crime-areas/Financial-crime/Money-laundering> accessed 9 April 2017

[9] Financial Action Task Force, 'What is money laundering?', <http://www.fatf-gafi.org/pages/faq/moneylaundering> accessed 9 April 2017.

third stage, reintegrate the money coming from crime into the formal economy. This is often accomplished by investing the 'washed' money into businesses, industrial enterprises or tourism projects.[10]



[11]

1.1.1 Placement

By looking at the modus operandi of money launderers throughout the last decades, it becomes apparent that financial institutions are the first contact point.

At this first stage, the illegally obtained assets are worked into the legal economic system. This is the phase in which the risk of being caught is the highest. This first stage can itself be split up into two stages, namely the *primary deposit* and the *secondary deposit.*[12]

The *primary deposit* is the stage where the illicit income will be placed into the legal bank system without attracting the attention of the compliance departments of financial institutions. Usually money launderers split up the sum into smaller amounts of money in order to circumvent identification, as no reporting mechanisms will be activated by depositing relatively small amounts of money. For example, in Austria generally no control mechanisms

[10] Friedrich Schneider, Ursula Windischbauer, 'Money laundering: some facts', (2008) Eur J. Law Econ., 387.
[11] What is Money Laundering, the Three Stages in Money Laundering, <http://kycmap.com/what-is-money laundering> accessed 11 April 2017
[12] Friedrich Schneider, Ursula Windischbauer, 'Money laundering: some facts' (2008) Eur. J. Law Econ., 387-395.

will be activated when sums below EUR 15.000 are deposited. Besides the method of splitting up money in partial amounts, there are also other commonly used methods, such as purchasing a relatively small bank in offshore 'bank havens'. Bribery and fraud are other well-known methods used by criminals.[13]

While the primary deposit is a direct infiltration of illicit assets, the *secondary deposit* is an indirect infiltration of illegal revenues through a conversion of these revenues into book money. This indirect infiltration is executed by a natural or legal interconnection between the bank at issue and the money launderer.

An example of the secondary deposit technique is the establishment of front companies, which are legal entities infiltrating black money into their banking accounts and thus into the legal fiscal system by creating a fictitious turnover. A condition sine qua non is that the business must be cash-intensive. Examples include business within the catering industry, the hotel sector or art trade. It is important to note that since only specific documents proving the foundation and turnover history are being affected by fraud, the company itself is not a phantom company.[14]

1.1.2 Layering

In this second stage, criminals aim to conceal the source of their illegal funds by transferring the black money via several, typically sophisticated, transaction structures. The layering of criminal money has become easier with the introduction of electronic payments because they increase the speed of the transactions, in addition to expanding cross-jurisdictional possibilities.

As an example, illicit proceeds can be 'smurfed' into domestic bank accounts in amounts just below the threshold where financial institutions might report the transaction as suspicious.

13 Ibid 5.
14 Ibid 7.

The funds can be transferred to offshore financial institutions, usually under the control of a representative, where the money will be used in order to create a 'loan' to the criminal in question. These transactions, including the payment of the loan, are seen as layering activities with the goal of concealing the initial source of the funds.[15]

1.1.3 Integration

The aim at this stage is to establish an apparent legal origin for the illicit proceeds. After having followed the necessary processes as explained in the aforementioned two steps, the money launderer can infiltrate the transformed capital into the official economy by making investments in a cash-intensive business.

The use of a '*back-to-back loan'*, as explained in the former example, is a popular method when it comes to the integration of criminal revenues. In this stage of the integration, the loan issued by an offshore-cooperation will, for instance, be used to invest in real estate, luxury goods or other market-based instruments.[16]

1.2 'Medellin Cartel' case study

This case, known as 'Santos Caballero, Maria, and others,' illustrates the foregoing three-staged concept of money laundering. In 1995, the police of Buenos Aires, Argentina organized a raid where they discovered a striking five cubic meters stash of US dollars, as well as many other currencies. The Federal High Court of Buenos Aires concluded that the cash money emanated from cocaine trafficking and other related activities conducted by the notorious Medellin Cartel. The profits derived from their cocaine trafficking can be seen as the first phase (*the placement phase).* The evidence proved that the cartel had transferred a part of their cash money from Colombia to Argentina via unofficial transfer systems and by

[15] OECD, 'Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors', 13 <http://www.oecd.org/tax/exchange-of-tax-information/43841099.pdf> accessed 11 April 2017.
[16] Ibid 14.

carrying the proceeds across the border (*layering phase*). The money transferred to Argentina was mostly used for the purchase of real estate, luxury cars, and investment in offshore companies (*integration phase).*[17]

2 Terrorism Financing

The attacks on 11 September 2001 made governments on both sides of the Atlantic decide to adopt rules to try to prevent the flow of proceeds for terrorist purposes. In a report commissioned by the Council on Foreign Relations in 2002, it was noted that 'as long as Al-Qaeda retains access to a viable financial network, it remains a lethal threat to the United States'.[18] In response to the recent terrorist attacks in Paris and Brussels, the EU has adopted an action plan in which the MS carry out concrete measures to counteract the financing of terrorist organisations, namely 'the Action Plan to strengthen the fight against the financing of terrorism'.

Before going into detail, we should define an act of terrorism. The term 'terrorism' has never been defined in international law, which poses problems when it comes to defining the term 'terrorism financing'. Nonetheless, The United Nations Convention for Suppression of the Financing of Terrorism has defined an 'act of terrorism' and held that the main objective of any act of terrorism is to 'intimidate a population, or to compel a government or an international organization to do or abstain from doing any act'.[19] The essential difference between terrorism and other forms of organised crime is the terrorist's intention to create anxiety and terror in society, in a government, or an international organization for political purposes. On the other hand, the ultimate goal of organised criminal groups is to obtain large

[17] Roberto Durrieu, 'Rethinking Money Laundering and Financing of Terrorism' (PhD, University of Oxford, 2012), 48.
[18] Stephen Kinga, Marieke Zwartjes, 'Regulating money laundering for terrorism financing: EU–US transnational policy networks and the financial action task force', (2015) Contemporary Politics, 341.
[19] UNGA International Convention for the Suppression of the Financing of Terrorism (adopted 9 December 1999, entered into force 10 April 2002), (2000) 39 ILM 270.

financial gains.[20] All the same, terrorist organisations depend upon financial support and a steady stream of funds in order to fulfil their goals. However, it must be noted that the cost of the world-changing event in September 2001 was less than USD 300.000.[21]

We should now take a critical look at the meaning of the *financing* of terrorism activities. A report published by the World Bank and the International Money Fund described it as 'the financial support in *any form* of terrorism or of those who encourage, plan, or engage in terrorism'[22]. This generally acknowledged definition of terrorism financing is very broad and ambiguous. Due to the lack of a clear and detailed definition, academics have long failed to determine the link between money laundering and terrorism financing.[23] It is apparent that money laundering and the financing of terrorism have different sources of proceeds. The funds in the process of money laundering have *per se* an illicit source - namely criminal activities - whereas the funds for financing terrorism can have a legal or illegal source.[24]

As mentioned earlier, the 'Action Plan to strengthen the fight against the financing of terrorism' was launched after the attacks in Paris led the European Agenda for Security to identify several areas to improve the on-going combat against terrorism financing.[25] The proposed plan contains additional measures to address various newly identified challenges, as well as a number of amendments to the Fourth Anti-Money Laundering Directive (4AMLD).[26] Its principal goal is to trace terrorism through financial movements and disrupt the sources of revenue used by terrorist organisations. The measures vary from applying and updating existing laws to helping 'third' countries tackle the issue of terrorist financing. Some

---

[20] Roberto Durrieu, 'Rethinking Money Laundering and Financing of Terrorism' (PhD, University of Oxford, 2012), 41.
[21] Doug Hopton, Money Laundering: A concise Guide for All Business (Gower Publishing, 2006), 4.
[22] Paul Allan Schott,'Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism', 1.
[23] Roberto Durrieu, 'Rethinking Money Laundering and Financing of Terrorism' (PhD, University of Oxford, 2012), 58.
[24] Donato Masciandaro, Black Finance: The Economics of Money Laundering, (Cheltenham 2007), 4.
[25] European Commission, 'Commission presents Action Plan to strengthen the fight against terrorist financing', <http://europa.eu/rapid/press-release_IP-16-202_en.htm> accessed on 13 April 2017.
[26] European Commission, 'Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing', COM (2016/050).

of these additional innovations were immediately put into force while other measures have been executed in 2017.[27]

Chapter 2: The European Anti-Money Laundering and Counter Terrorism Financing Regulatory Framework

3 Historical background

Throughout the years, the EU has developed a comprehensive set of legal instruments with the goal of combating money laundering. The development of the legal regime came hand in hand with the build-out of global standards, most notably by the FATF. The successive EU Anti-Money Laundering Directives consist of three main elements: the criminalization of money laundering and terrorist finance; the prevention of money laundering via the imposition of a series of duties in the private sector; and the focus on financial intelligence. When delving into the Anti-Money Laundering Directives (AMLD), it is of great importance to be mindful of the fact that the development of standards in the field demonstrates an exceptional combination of global and regional standard-setting. The EU has played an important role in international conventions on the combat against money laundering and terrorism financing, including *inter alia* numerous UN Conventions.[28]

The FATF has played an even more important role regarding the evolution of the EU AML regulatory framework. The FATF is an impromptu body established in 1989 by the G7, with the cooperation of the OECD. Among the members of the FATF are all fifteen initial EU Member States (EU MS). However, it is striking that none of the MS which joined the EU in

[27] European Commission, 'Action Plan to strengthen the fight against terrorist financing 2016', <http://ec.europa.eu/justice/criminal/files/aml-factsheet_en.pdf> accessed 13 April 2017.
[28] Valsamis. Mitsilegas, 'Global Governance of Crime "The European Union and the Global Governance of Crime"', in V. Mitsilegas, P. Alldridge and L. Cheliotis (eds.), Globalisation, Criminal Law and Criminal Justice. Theoretical, Comparative and Transnational Perspectives (Hart, 2015), 153–198.

2004 and 2007 are members of the FATF. Consequently, these MS have no say in the shaping of FATF standards and the creation of systems to ensure compliance.[29]

The first FATF initiatives proposed to combat money laundering date from 1990 when the original FATF Forty Recommendations were drawn up.[30] The Recommendations were revised in 1996 and, due to the grave threat of the funding of terrorist activities, expanded in scope in 2001. From 2001 onwards, the FATF recognized the on-going changes in crime, and thus created Eight Special Recommendations on Terrorist Financing.[31] The 1990 Forty Recommendations - together with the Eight Special Recommendations - were altered once more in 2003. Most importantly, in that same year, the revised Recommendations were endorsed by over 180 countries. The FATF recommendations are universally perceived as the international standard regarding the combat against money laundering activities and the financing of terrorism. Additionally, the Recommendations guide countries and the EU in the implementation of the proposed measures in order to attain the outlined objectives.[32] Despite the fact that FATF guidelines are soft law, their effect on national and EU legislation has been considerable.

From the EU perspective, the initial Recommendations were in fact very influential in the development of the Community response against the misuse of the financial system by individuals. Shortly after the 1990 Recommendations, the EC adopted the first EC AMLD, which encompassed the countermeasures and international standards published by the FATF. Since then, many amended and revised Directives have been put in place with a two-pronged approach in response to criminal innovations with regard to money laundering and terrorism

---

[29] Valsamis Mitsilegas, Niovi Vavoula, 'The evolving EU anti-money laundering regime; challenges for fundamental rights and the rule of law' (2016) 23 MJ, 261.

[30] Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, [1991] OJ L166, 2.

[31] Later expanded to Nine Special Recommendations on Terrorist Financing.

[32] FATF Recommendations, 'International Standards on Combating Money Laundering and the Financing of Terrorism & proliferation, February 2012, updated October 2016, <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 13 April 2017.

finance. The European Union has established a whole set of countermeasures throughout the years, by way of Directives, which are generally in line with the FATF Recommendations.[33]

The consecutive Directives will be examined in the following chapter. Along with reviewing the record of Directives, the role of the FATF Recommendations and Standards will be discussed.

3.1 European Legislation

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

The First Directive (1AMLD) was adopted in 1991 to ensure a homogeneous approach by the MS in the fight against money laundering, with the main objective of protecting the EU Single Market. This Directive implemented the Forty FATF Recommendations of 1990 by creating obligations for, *inter alia*, financial and credit institutions, such as imposing duties to identify their customers (Know Your Customer or KYC); abstain from suspicious transactions with links to money laundering; and commit to reporting dubious financial transactions to the relevant national authorities. Moreover, the EEC forbid the financial and credit institutions from *tipping off* customers. Formerly, it was a commonly used practice to *tip off*. In other words, banks warned their customers instantly when they were under investigation in relation to their money laundering activities. The MS have discretion to determine adequate sanctions in cases of infringement of the Directive. In brief, the first AMLD was a great first step towards the prevention of the misuse of the financial system by way of money laundering. The EU not only followed the FATF Recommendations of 1990 but also went one step further

[33] Valsamis Mitsilegas, Bill Gilmore, 'The EU Legislative Framework Against Money Laundering and Terrorist Finance: A Critical Analysis in The Light of Evolving Global Standards', (2007) 56(1) International and Comparative Law Quarterly, 120.

by obliging the financial institutions to proactively report suspicious transactions.[34]

3.1.2 Council Directive 2001/97/EC of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering

The European Parliament passed the second Anti-Money Laundering Directive (2AMLD) in 2001. After the introduction of the 1AMLD, European institutions - jointly with the FATF – had been monitoring very closely the adequacy of the 1AMLD in response to new trends in money laundering. This resulted in the awareness that the European anti-money laundering regulation was neither up to date nor adequate for tackling the upcoming technological advances in the field.[35]

The Commission expressed their concerns in its explanatory memorandum[36];

> Just as the 1991 Directive moved ahead of the original FATF 40 Recommendations in requiring obligatory suspicious transaction reporting, the European Union should continue to impose a high standard on its Member States, giving effect to or even going beyond the 1996 update of the FATF 40 Recommendations. In particular, the EU can show the way in seeking to involve certain professions more actively in the fight against money laundering alongside the financial sector.

In short, the 2AMLD extended the definition of money laundering by (1) including other offences - such as corruption, (2) putting in place an up to date customer identification process in light of new technology, (3) expanding the duties of the financial institutions, and (4) most controversially, introducing the *ratione personae* scope of the Directive.[37] Indeed,

---

[34] Ibid 120.
[35] Ibid 123.
[36] Official Journal C177E, 27/06/2000, P.0014-0020.
[37] Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering,

certain legal professions - for instance lawyers[38] or notaries - were from that point on subject to the rules of the new Directive when involved in specific financial activities.[39]

3.1.3 Council Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

<...[T]he misuse of the financial system to channel criminal or even clean money to terrorist purposes poses a clear risk to the integrity, proper functioning, reputation and stability of the financial system.>[40]

Due to events happening in society, new developments in money laundering, and the fact that the 2001 2AMLD did not come into force until 2003, the European Commission undertook action by preparing a third AMLD. The main goal of the Third Anti-Money Laundering (3AMLD) was to adjust the regulatory framework in the EEA in order to counteract money laundering as well as terrorism financing, whilst taking into consideration the new FATF recommendations. The 3AMLD brings important changes to the previous regime of anti-money laundering measures adopted by the European Parliament.[41] This subchapter will focus on the most significant features that were refined by the introduction of the 3AMLD.

Firstly, the 9/11 terrorist attacks, followed by the declaration of the 'war on terror', was the

---

(16).

[38] 2AMLD, Art 6(3) exempts lawyers, auditors and tax advisors 'with regard to information they receive or obtain on one of their clients, in the course of ascertaining the legal position for their client or performing their task of defending or representing their client in, or concerning, judicial proceedings, including advice on instituting or avoiding proceedings, whether such information is receiver or obtained before, during or after such proceedings'.

[39] Valsamis Mitsilegas, Bill Gilmore, 'The EU Legislative Framework Against Money Laundering and Terrorist Finance: A Critical Analysis in The Light of Evolving Global Standards', (2007) 56(1) International and Comparative Law Quarterly, 124.

[40] Council Directive 2005/60/EC of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, [2005] OJ L309/15.

[41] Etay Katz, 'Implementation of the Third Money Laundering Directive - an overview', (2007), 3, Law and Financial Markets Review, 207, <http://www.tandfonline.com/doi/abs/10.1080/17521440.2007.11427880> accessed 20 April 2017.

signal for members of the FATF to extend its mandate and include the combat against terrorism financing.[42] The FATF considered it necessary to review the international standards set out and extend these standards to terrorist financing.[43] After conducting a review, the FATF published the 2003 Forty Recommendations jointly with the Special Recommendations on terrorism financing.[44] These Special Recommendations require states worldwide to regulate all sorts of financial transactions in order 'to detect, prevent and suppress the financing of terrorism and terrorist acts' (FATF, 2001). Shortly after the publishing of the Special Recommendations, the EU manifested several of the Recommendations as Directives and Regulations. The 3AMLD was, at that time, the key EU legislation regarding the combat against the financing of terrorism. These European measures have a broad impact on financial and credit institutions, as well as the day-to-day transactions of EU Citizens.[45] The aforementioned legislative intervention undermined some privacy rights of EU citizens; for that reason, the Council insisted on bringing the definition of serious crime - outlined in the 2AMLD - in line with the definition in the 2001 Framework Decision on confiscation.

The following provisions incorporated in the 3AMLD are worth pointing out, for analytical purposes of the 4AMLD:

- *The Directive extends its scope to activities related to or associated with terrorist financing.*
- *Adding trust and company service providers to the list broadened the scope of*

[42] 'Text of George Bush's speech', The Guardian (London, 21 September 2001), <https://www.theguardian.com/world/2001/sep/21/september11.usa13> accessed 19 April 20.
[43] Mariano Fernandez Salas, 'The third anti-money laundering directive and the legal profession', <http://www.anti-moneylaundering.org/Document/Default.aspx?DocumentUid=7B528765-CB1F-4748-9733-68935E2C4745> accessed 19 April 2017.
[44] FATF, 'The Forty Recommendations of 2003' <http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf> accessed 19 April 2017.
[45] Mara Wesseling, The European fight against terrorism financing: Professional fields and new governing practices, (PhD thesis, University of Amsterdam, 2013) 267.

individuals subject to the new regulation.[46,47]

- *More specific and detailed stipulations regarding the verification, as well as the identification, of customers and beneficial owners. The 1AMLD already mentioned this process without going into detail or setting our concrete procedures, which needed to be followed by the financial institutions. By means of an example: Article 7, jointly with Article 3(9) of the 3AMLD defines in which circumstances a CDD should be conducted.*
- *The CCD proceedings should be based on a risk assessment made by the credit or financial institutions. This is the so-called Risk-Based Approach, which is a key point of this Directive. The risk of money laundering and/or terrorist financing is calculated by taking into account several parameters such as the type of customer, the business relationship, or the transaction in question.*[48] *Furthermore, countries facing higher chances of being affected by money laundering or terrorism financing need to take more efficient measures in order to lower their risks, and will have the opportunity to conduct preventive procedures adapted to the specific activities or sector.*[49]
- *In addition, Reduced and Enhanced CDD measures have been developed. Article 8 of the Directive defines the situations in which enhanced CDD is necessary and when simplified CDD could be allowed.*
- *The matter of Beneficial Ownership is clarified and defined with much more of an eye*

[46] Etay Katz, 'Implementation of the Third Money Laundering Directive – an overview', (2007), 3 Law and Financial Markets Review, 207.

[47] "any natural or legal person which by way of business provides any of the following services to third parties: (a) forming companies or other legal persons; (b) acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons25; (c) providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement; (d) acting as or arranging for another person to act as a trustee of an express trust or a similar legal arrangement; (e) acting as or arranging for another person to act as a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in conformity with Community legislation or subject to equivalent international standards."

[48] David Rogozinski, 'Fourth Anti-Money Laundering Directive: Backbone or back-fire of the European business environment?' (Thesis, Tilburg University, 2004) 32.

[49] European Commission, 'European Commission report on the application of the Third Anti-Money Laundering Directive- Frequently asked questions' 1, <http://europa.eu/rapid/press-release_MEMO-12-246_en.htm?locale=en> accessed 20 April 2017.

for detail in comparison to the 1AMLD. The definition approved by the Council consists of two parts: a broad catch-all clause and a minimum threshold with reference to legal arrangements, legal entities and corporate entities.[50] *In relation to the matter of Beneficial Ownership, Article 8 requires the identification of beneficial owners for legal persons.*

- *Introduction of a new definition for politically exposed people.*
- *Requirement to not disclose any information to the customer or third parties concerning investigations undertaken by national authorities (in other words, a prohibition on tipping off customers).*[51]

These are the principal innovations and modifications introduced by the 3AMLD, adopted in October 2005 and transposed into national laws across the EEA by 15 December 2007. The Directive was a great step forward concerning the combat against the financing of terrorism and the misuse of the financial system for money laundering. Besides clarifying certain ambiguous provisions of the two former Directives, it also gives a clear explanation on how the relevant institutions should carry out their pertinent duties. Most importantly, there is no longer space for legal uncertainty on the practice of *tipping off* clients once an investigation on suspicious transactions has been commenced.[52]

The following chapter will thoroughly study the changes and features inherent in the 4AMLD, which was adopted in May 2015, as well as explain the rationale behind it.

[50] 3AMLD Article 3(6).
[51] 3AMLD Article 28(1).
[52] Mariano Fernandez Salas, 'The third anti-money laundering directive and the legal profession' 7, <http://www.anti-moneylaundering.org/Document/Default.aspx?DocumentUid=7B528765-CB1F-4748-9733-68935E2C4745> accessed 19 April 2017.

Chapter 3: The Fourth Anti-Money-Laundering Directive

'*According to an estimate of the European Commission based on reports by the IMF and UNODC €330 billion are laundered in the EU per year*'[53]

4 General

The Council and the European Parliament signed the most recent AMLD on the 20th of May 2015, and it was published in the Official Journal of the EU on the 5th of June the same year. The implementation deadline for the MS to enact the Directive in their respective national regulations was set on 26 June 2017.[54]

Once more, new FATF recommendations were the inspiration for the proposal of the 4AMLD. In its explanatory statement, the EC acknowledged the fact that criminal organizations keep seeking new methods to misuse the financial system in order to launder illicit proceeds or finance terrorism. By an on-going adjustment and improvement of the current norms and standards, the FATF, EC and the individual MS continue to try to eliminate the vulnerabilities of their respective financial systems, and the financial system as a whole. The explanatory memorandum does not describe the correlation between the new methods employed by illegal organisations and the new recommendations of the FATF. However, one of the reasons for more vigorous measures might be the increase in criminal cross-border financial transactions. As a matter of fact, the internationalisation of money laundering activities had already been mentioned in the explanatory statement of the 1AMLD, but since

[53] Janos Böszörmenyi, Erich Schweighofer, 'A review of tools to comply with the Fourth EU anti-money laundering directive', (2015) International Review of Law, Computers & Technology, 65, <http://dx.doi.org/10.1080/13600869.2015.1016276> accessed 26 April 2017.

[54] Council Directive 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, [2015] OJ L141/73.

then no decrease had been noted; in fact the contrary has occurred.[55] Thus, in order to safeguard the internal market and market integrity the new 4AMLD was crucial.

The following chapters and sub-chapters will mainly focus on the headlines and the most recent modifications of some concepts outlined in the 4AMLD, namely the risk based approach, customer due diligence, ultimate beneficial ownership (RBA, CDD, UBO) and the interaction between these three concepts. Before that, we will take a closer look at the new FATF recommendations, examine the proportionality of the Directive, and assess the so-called Third Country Equivalence.

4.1 The FATF Recommendations

The revisions to the FATF Recommendations in February 2012 address new and emerging threats, in addition to clarifying existing provisions. Despite a significant number of amendments made to the Recommendations, the respective provisions stay coherent, and the advisory body safeguarded the stability of the Recommendations as a whole. The revised FATF standards created guidelines that allow states to respond appropriately in areas where high risks are common: '*Countries should first identify, assess and understand the risks of money laundering and terrorist finance that they face, and then adopt appropriate measures to mitigate the risk'*.[56]

The FATF Recommendations provide key changes to the following aspects:

- Assessing risk and applying a risk-based approach

[55] Rutger de Doelder, Musa Elmas, 'De Vierde Anti-wiswasrichtlijn', (2016) Jaarboek Compliance, 224, <https://repub.eur.nl/pub/79289/JBC-2016_R-de-Doelder-en-M-Elmas_De-Vierde-Anti-witwasrichtlijn.pdf> accessed 21 April 2017.

[56] FATF, 'The FATF Recommendations; International standards on combating money laundering and the financing of terrorism and proliferation' (2012) 7 <http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 20 April 2017.

- National cooperation and coordination
- Customer due diligence
- Recordkeeping
- Politically exposed persons
- Transparency and beneficial ownership of legal persons

In brief, the updated Recommendations now include the RBA. They also aim to increase the transparency of financial transactions and to clarify some concepts such as PEPs. These improvements adopted by the FATF can be identified in the 4AMLD.[57]

5 Risk Based Approach

5.1 General

'Adopting an RBA implies the adoption of a risk management process for dealing with money laundering and terrorist financing. This process includes recognizing the existence of the risk(s), undertaking an assessment of the risk(s), and developing strategies to manage and mitigate the identified risks'.[58]

The RBA was implemented in EU legislation for the first time with the publication of the 3AMLD and was enhanced in the newest AMLD. Before the implementation of this system, the EU made use of the *rule-based approach*, which was characterized primarily by its shortcomings. According to the Paolo Baffi Centre on Central Banking and Financial Regulation, the former approach is static and passive[59]. Indeed, legislators and professionals

[57] Gary W. Sutton, 'The New FATF Standards', (2012) J.Int'L, 68.
[58] FATF, 'Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing' (2007) 2,<http://www.fatfgafi.org/media/fatf/documents/reports/High%20Level%20Principles%20and%20Procedures.pdf> accessed 26 2017.
[59] Lucia Dalla Pellegrina, Donato Masciandaro, 'The Risk Based Approach in the New European Anti-Money

had created a set of rules applicable in all situations and cases, which gave money launderers the opportunity to adapt their techniques in such a way as to be compliant with the AML regulation. This leads to a situation where illicit transactions can look nearly identical to legal operations.[60] The past has thus proven that the rule-based approach is insufficient in the combat against money laundering.[61]

Whereas the rule-based approach is rather static, the RBA is dynamic and flexible, which makes it tricky for money launderers to misuse the financial systems through shifty transactions. By utilizing the RBA approach, financial institutions create a process which is less predictable to criminals because banking and finance professionals can use their professional judgment to develop an AML model suitable for the business activity, organisation or structure in question.[62] The rationale for the RBA lies in the fact that financial institutions should be responsible for monitoring and managing the risks linked to certain activities of their clients, whereas formerly, the regulatory institutions were the responsible party.[63]

All in all, the purpose of the RBA is defined by the FATF in 2007 as follows: *[B]y adopting a risk-based approach, competent authorities and financial institutions are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the risks identified. This will allow resources to be allocated in the most efficient ways. The*

Laundering Legislation: a Law and Economics View', Paolo Baffi Centre Research Paper Series No. 2008-22, 5, <http://www.anti-moneylaundering.org/Document/Default.aspx?DocumentUid=F834E956-A423-4448-972D-204D03BBDDFC> accessed 27 April 2017.

[60] Lucia Dalla Pellegrina, Donato Masciandaro, 'The Risk Based Approach in the New European Anti-Money Laundering Legislation: a Law and Economics View', Paolo Baffi Centre Research Paper Series No. 2008-22, 5, <http://www.anti-moneylaundering.org/Document/Default.aspx?DocumentUid=F834E956-A423-4448-972D-204D03BBDDFC> accessed 27 April 2017.

[61] Brigit M. Hutter, 'The attractions of risk based regulation: accounting for the emergence of risk ideas in regulation, Discussion Paper', (2005) LSE Centre for Analysis of Risk and Regulation 15 <http://eprints.lse.ac.uk/13309/> accessed 27 April 2017.

[62] Lucia Dalla Pellegrina, Donato Masciandaro, 'The Risk Based Approach in the New European Anti-Money Laundering Legislation: a Law and Economics View', Paolo Baffi Centre Research Paper Series No. 2008-22, 5, <http://www.anti-moneylaundering.org/Document/Default.aspx?DocumentUid=F834E956-A423-4448-972D 204D03BBDDFC> accessed 27 April 2017.

[63] Stuart Ross, Michelle Hanan, 'Money laundering regulation and risk-based decision-making' (2007) 10 JMLC, 106.

principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention[64].

National authorities in the respective MS need to implement legislation in line with the 4AMLD. In other words, they need to incorporate risk-based mechanisms in their legislative provisions. The obliged entities need to act in compliance with the national provisions by creating internal mechanisms to detect and prevent money laundering and terrorism financing. In spite of these mechanisms designed by the obliged entities, the way of assessing the risk, and the conceptualization of these risks by the EU Commission, remains ambiguous.[65]

5.2 Assessing and managing risks; high and low risk factors

In 2005, the concept of *risk* was brought for the first time into the European AML legislation. It is a central concept within the current Anti-Money Laundering and Counter Terrorist Financing (AML/CTF) regime, but the way of defining risk remains ambiguous and vague. This creates a certain level of uncertainty for the financial and credit institutions dealing with the assessment of high or low risk factors.[66] In fact, the notion *risk* does not have a generally acknowledged or recognized meaning. The International Organisation for Standardisation has defined *risk* as "the effect of uncertainty on objects."[67] On the other hand, Holzer and Millo suggest that regulatory risk should be calculated in a way that it is linked to decision-making outcomes.[68] It seems inherent to the concept of *risk* that, at the moment of decision-making, one cannot know beforehand whether the costs will be greater than the losses.[69] Throughout

---

[64] FATF, 'FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing – High Level Principles and Procedures', 2, <http://www.fatf-gafi.org/media/fatf/documents/reports/High%20Level%20Principles%20and%20Procedures.pdf> accessed 27 April 2017.
[65] Ibid 6.
[66] Ibid 4.
[67] ISO, 'ISO 31000 – Risk Management', 1, < https://www.iso.org/iso-31000-risk-management.html> accessed 27 April 2017.
[68] Boris Holzer, Yuval Millo, 'From risks to second-order dangers in financial markets: unintended consequences of risk management systems, (2004) ESRC, 227, <http://eprints.lse.ac.uk/36101/1/Disspaper29.pdf> accessed 27 April 2017.
[69] Ibid 228.

the entire AML/CTF legal framework, there is the idea that the efforts to avoid money laundering or the financing of terrorism should be in line with the risks faced by the financial institutions. However, this is very difficult to assess since the money launderers operate by using financial services that are not *in se* in violation of the law. Thus, *'an activity that in one context is money laundering may in another context be entirely legal'.*[70]

As it has been outlined earlier on, the concept of *risk* is very vague and has not been defined by, for instance, the FATF or a European institution. In the case of money laundering, financial institutions must not only spot risks in relation to money laundering and terrorist financing, but also identify whether the risk is relatively high or low. The distinction between *low* and *high risk* needs to be clarified before we can delve into the RBA. Some authors, such as Stewart, identify three features for identifying high or low risks associated with money laundering.[71] The first feature is the strength of the relationship between the peculiarities that the financial institutions observe and the act that the institution aims to identify. In cases where there is a strong relationship between these two elements, one could conclude the existence of a *high risk,* also known as the 'probabilistic risk'.[72] For example, if the financial institution knows that group investments are very likely to be associated with money laundering, then this suggests a high risk. Secondly, the notion of 'consequence risk' indicates the potential threats of those transactions which are subject to review. This is the situation in which the financial institution is more concerned about the high amount of cash originating from, for instance, a second-hand car dealer than from a better-regulated and smaller-cash-flow enterprise. Moreover, the so-called 'reputational risk' also falls under the category of 'consequence risk'.[73] The reputational risk covers the risk of financial institutions failing to

[70] Stuart Ross, Michelle Hanan, 'Money laundering regulation and risk-based decision-making' (2007) 10 JMLC, 106.
[71] Sam Stewart, 'Coping with the FSA's risk based approach', (2005) 13(1) Journal of Financial Regulation and Compliance, 43.
[72] Stuart Ross, Michelle Hannan, 'Money laundering regulation and risk-based decision-making', (2007) 10 JMLC, 106.
[73] Ibid 110.

identify and report activities related to money laundering or terrorist financing.[74] Lastly, financial institutions also face a 'regulatory risk', which encompasses the risk of being vulnerable to business activities which are high-risk but difficult to monitor. Together, these three forms of risk should be taken into account when developing any AML/CTF strategy.[75]

In situations where the risk of money laundering or terrorist financing is high, the institutions are supposed to take additional measures, or enhanced due diligence (EDD).[76] The necessary measures depend on the circumstances. All in all, high-risk situations require risk management controls, and low risk situations require only basic controls.[77]

5.3 National Risk Assessment

Furthermore, the EC introduced a new requirement for EU MS, namely the 'National Risk Assessment' (NRA). This allows the individual MS to assess, identify, and address the risks they face that might create a threat to their national system or the European economy more broadly.[78] As a result of this new NRA, the Commission will be able to review particular cross-border threats by assembling the various NRAs and analysing which of these threats could damage the internal market. The supranational function of the EC is increasingly important as some issues and threats cannot effectively be solved and combated by the EU MS on their own initiative.[79]

The EC also deemed it necessary for the stability of the internal market to create a non-

---

[74] Charlie Weston, 'Embarrassment for AIB as bank fined €2.3m for breach of money laundering rules', The Independent (Dublin, 26 April 2017), <http://www.newsjs.com/url.php?p=http://www.independent.ie/business/embarrassment-for-aib-as-bank-fined-23m-for-breach-of-money-laundering-rules-35654882.html> accessed 28 April 2017.

[75] Stuart Ross, Michelle Hanan, 'Money laundering regulation and risk-based decision-making', (2007) 10 JMLC, 106, 111.

[76] Infra, 5.2.2.

[77] 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' (April 2015), 25, <http://www.toezicht.dnb.nl/en/4/6/51-204766.jsp> accessed 28 April 2017.

[78] Bridge Consulting, 'Fourth EU Anti-Money Laundering Directive' (2016), 2, <https://bridgeconsulting.ie/wp-content/uploads/2016/06/Bridge-Consulting-EU-4th-AMLD-Jun-2016.pdf> accessed 2 May 2017.

[79] Recital 23 4AMLD.

exhaustive list of factors that signal a higher risk, as laid out in Article 18:[80]

(1) Customer risk factors:

(a) the business relationship is conducted in unusual circumstances;

(b) customers that are resident in geographical areas of higher risk as set out in point (3);

(c) legal persons or arrangements that are personal asset-holding vehicles;

(d) companies that have nominee shareholders or shares in bearer form;

(e) businesses that are cash-intensive;

(f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

(2) Product, service, transaction or delivery channel risk factors:

(a) private banking;

(b) products or transactions that might favour anonymity;

(c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;

(d) payment received from unknown or unassociated third parties;

(e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;

(3) Geographical risk factors:

(a) without prejudice to Article 9, countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;

(b) countries identified by credible sources as having significant levels of corruption

[80] Art 18(3) 4AMLD.

or other criminal activity;

(c) countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;

(d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country

Article 16 refers to the non-exhaustive list, created by the EC, of factors and types of evidence that indicate potentially lower risks:[81]

(1) Customer risk factors:

(a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;

(b) public administrations or enterprises;

(c) customers that are resident in geographical areas of lower risk as set out in point (3);

(2) Product, service, transaction or delivery channel risk factors:

(a) life insurance policies for which the premium is low;

(b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;

(c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;

(d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;

[81] Art 16 4AMLD.

(e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money);

(3) Geographical risk factors:

(a) Member States;

(b) third countries having effective AML/CFT systems;

(c) third countries identified by credible sources as having a low level of corruption or other criminal activity;

(d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements

Risk Based Approach Elements

Customer Risk •Overall background and reputation •Business interests and practices-Mgt •Business associates and networks/ Business Link •Political Affiliations (PEPs) •Beneficial ownership and control •Source of funds	**Country Risk** •Political stability •Legal status •Economic situation •Standing of the financial services industry •Exposure to organised crime and Money laundering •Corruption
Sector Risk •Weapons and Metal trading •Precious metals •Art •Real Estate •Exchange Dealership	**Product Risk** •Private Banking •Correspondent Banking •Structured Finance •Commodities

82

The factors shown in this table are indicators which need to be taken into account by the entities subject to the 4AMLD whilst carrying out their obligations with respect to the RBA.

[82] ICBC Doha Branch, 02/14/2012, < https://www.slideshare.net/bachirelnakib/icbc-aml-riskbased-approach-jan-2011-by-bachir-el-nakib> accessed 28 April 2017.

Chapter 4: Customer Due Diligence

6 General

The concept of Customer Due Diligence (CDD), also known as 'Know Your Customer' or 'Counterpart', is an essential instrument used to detect potential money laundering activities or schemes to finance terrorism. The concept of CDD refers to the situation in which financial institutions, such as banks, are obligated to know the situation of their customer in detail. By knowing their detailed situation,[83] the counterparty will be treated differently depending on the category of risk they were placed in. With the 4AMLD, the CDD measures are much more thorough and far-reaching than in the former Directive.[84] An important amendment to the 3AMLD requires *ongoing* monitoring throughout the whole business relationship and, most importantly, the relevant data on the counterparty is supposed to be kept up-to-date until the business relationship comes to an end. These two innovations implemented in the most recent Directive require much effort on the part of the banks in order to comply.[85] The examination of the new legal obligations within the framework of the CDD will allow us to observe its close affiliation with the aforementioned RBA.

The following provisions allow us to identify the main objectives of the European legislator. Article 11 of the same Directive stipulates in which circumstances a CDD should be conducted by the respective financial institution:

---

[83] ESMA, Joint Guidelines under Article 17 and 18(4) of Directive (EU) 2015/849 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, JC 2015/061 <https://eiopa.europa.eu/Publications/Consultations/JC%202015%20061%20(Joint%20Draft%20Guidelines%20on%20AML_CFT%20RFWG%20Art%2017%20and%2018).pdf> accessed 2 May 2017.

[84] Maria Bergstrom, Karin Svedberg Helgesson, Ulrika Morth, 'A New Role for For-Profit Actors? The Case of Anti-Money Laundering and Risk Management', (2011) 49(5) JCMS, 1043.

[85] Etay Katz, 'Implementation of the Third Money Laundering Directive – an overview', (2007) 1(3) Law and Financial Markets Review, 208, <http://www.tandfonline.com/doi/citedby/10.1080/17521440.2007.11427880?scroll=top&needAccess=true> accessed 3 May 2017.

(a) when establishing a business relationship;

(b) when carrying out an occasional transaction that: (i) amounts to EUR 15 000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked; or (ii) constitutes a transfer of funds, as defined in point (9) of Article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council (1), exceeding EUR 1 000;

(c) in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(d) for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(e) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;

(f) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Notably, the CDD/KYC process consists of two phases. The first phase is a *pre-business relationship* phase. It commences with due diligence on the customer and possible beneficiaries before the establishment of an ongoing business relationship; in the case of an intermittent transaction, it requires due diligence on customers seeking to deposit amounts above a specific threshold.[86,87] The second phase is conducted once the business relationship between the financial institution and the counterparty has been established. As stated in the

[86] Art 11 4AMLD: '...amounts to EUR 15.000 or more...'.

[87] Art 14 4AMLD: 'Member States shall require that verification of the identity of the customer and the beneficial owner take place *before* the establishment of a business relationship or the carrying out of the transaction'.

4AMLD, the financial institution must monitor the transactions of the client or third party throughout the course of the business relationship.[88]

6.1 Simplified and Enhanced CDD and RBA

The 4AMLD provides two possibilities for the banking and finance institutions – to conduct a simplified or an enhanced CDD. The option must be based on the assessment of the risk, prior to the CDD. Thus, it shows the significant interaction between the RBA and the conduct of the CDD. The evaluation of the risk is prior to the stage where the financial entity determines whether a simplified or an enhanced CDD should be applied.

According to the FATF Recommendations up to 2016, the general rule should be that customers are, in principle, subject to the full range of CDD measures. However, in circumstances characterized by a lower risk of money laundering or terrorist financing, a simplified CDD (SDD) is justified. For instance, this applies in situations where the identity of the counterparty and the beneficial owner of the counterparty are publicly accessible.[89]

6.1.1 Simplified Customer Due Diligence[90]

In contrast to preexisting AML/CTF Directives, the SDD stipulated in the 4AMLD is allowed under strict conditions and in specific circumstances, including an appraisal and assessment of each single case. The decision must rely on a risk-based analysis, in compliance with the aforementioned RBA and supported by specific documentation. The entity subject to the 4AMLD must officially conclude that the business relationship or the transaction present a significantly lower degree of risk. Customer risk factors, product/service/transaction or

---

[88] Janos Böszörmenyi, Erich Schweighofer, 'A review of tools to comply with the Fourth EU anti-money laundering directive', (2015) International Review of Law, Computers & Technology, 67, <http://dx.doi.org/10.1080/13600869.2015.1016276> accessed 2 May 2017.

[89] FATF, 'The FATF Recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation' (2012) 67, <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf> accessed 3 May 2017.

[90] Art 15, 16 4AMLD.

delivery risk factors, and geographical risk factors must all be taken into account.[91]

By way of comparison, under the 3AMLD, the entities instantly applied the SDD in certain circumstances, without a case-by-case assessment of the situation of the counterparty. [92]

6.1.2 Enhanced Customer Due Diligence[93]

Formerly, under the 3AMLD, the financial and credit institutions were obliged to carry out the EDD in situations where the counterparty was physically absent whilst performing identification audits (or at the commencement of a business relationship involving PEPs and other situations in which there might be a higher risk of money laundering or terrorism financing).[94]

The regulatory framework under the 4AMLD is much more comprehensive and detailed regarding its EDD requirements. In the following circumstances, the entities subject to the Directive are required to perform an EDD[95]:

'When being involved with entities established in the Union which are located in high-risk third countries;[96]

In situations where the background and purpose of all complex and unusually large transactions or patterns of transaction, have no obvious economic or lawful purpose;

When the circumstances are covered by the situations listed in Annex III of the Directive and might suggest potentially higher risk factors, such as;

- *Customer risk factors.*

---

[91] Annex II 4AMLD.
[92] Art 11 3AMLD.
[93] Art 18 4AMLD.
[94] Darren Allen, 'Comparison Table; Fourth Money Laundering Directive-Changes from 3MLD' (Thomson Reuters Regulatory Intelligence, 2016) 5, <https://smartsales.thomsonreuters.com/exLink.asp?111968458OB67R57I344295266> accessed 3 May 2017.
[95] Art 18 4AMLD.
[96] Art 9 4AMLD.

- *Product/service/transaction or delivery risk factors,*
- *Geographical risk factors'.*

Chapter 5: Guidelines for retail banks

7 Distinct alterations

The European Securities and Market Authority, in cooperation with the European Banking Authority, considered it appropriate to set out specific guidelines for retail banks and other financial institutions in the EU.[97]

Their paper highlights once more that the SDD may be applied only in low-risk relationships and by no means acts as an exemption from the stipulated CDD measures. However, there are provisions allowing the retail banks to alter the *timing, amount,* or *type* of the respective CDD measures.[98]

We will now turn to the adjustments that can be made by banks, which will allow us to see how the retail banks put the relevant regulation into practice.

First of all, retails bank can adjust the *timing* of the CDD. The adjustment of timing can be applied in cases where the transaction of the counterparty has characteristics that drastically limit the risk of money laundering and the financing of terrorism by its nature. The financial entity can, for instance, decide to 'verify the customer's or beneficial owner's identity once

[97] Joint Committee of the European Supervisory Authorities, 'Joint Guidelines under Article 17 and 18(4) of Directive (EU) 2015/849 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), JC 2015/061, <https://esas-joint-committee.europa.eu/Publications/Guidelines/Final_RBSGL_for_publication_20161115.pdf> accessed 8 May 2017.

[98] Joint Committee of the European Supervisory Authorities, 'Joint Guidelines under Article 17 and 18(4) of Directive (EU) 2015/849 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), JC 2015/061,19, <https://esas-joint-committee.europa.eu/Publications/Guidelines/Final_RBSGL_for_publication_20161115.pdf> accessed 8 May 2017.

transactions exceed a defined threshold or once a reasonable time limit has lapsed'.[99]

Secondly, retail banks can opt for an adjustment of the *quantity* of information necessary for an adequate verification or identification of the customer. Such a simplified measure can have different forms, depending on the subject and nature of the business relationship. The retail bank can, for instance, decide to adjust the quantity of information depending on the specific nature of the product and in accordance with the relationship between the retail bank and the counterparty (for example, in the case of gift cards for bookshops or coupons to be used in shopping centers).[100]

Thirdly, the retail bank can decide to adjust the *quality* of the information or source, in comparison to the standard CDD or the EDD.

An example can be found in the practice of some retail banks to accept information delivered by the customer himself, instead of by an independent source, at the moment of conducting the research on the identity of the beneficial owner.[101]

Lastly, a consumer bank can decide to make an adjustment regarding the *frequency* of reviews of the transactions of the counterparty and their business relationship. For example, the bank can decide to gather information only if suspicious transactions are carried out or when a specified monetary threshold has been surpassed.[102]

The aforementioned paper seems essential in order to give consumer banks precise guidelines for ways in which they can simplify their CDD; these guidelines may be implemented in the aftermath of the financial crisis or in response to the failures occurring in regard to the 3AMLD.

---

[99] Ibid 17.
[100] Ibid 18.
[101] Ibid 18.
[102] Ibid 18.

7.1 Retail banks and Enhanced Due diligence

Following the above-mentioned SDD-model, the same institutions prepare detailed guidelines for consumer banks in the event that enhanced due diligence is deemed necessary. In this paper, we will focus on the guidelines intended for retail banks concerning *politically exposed persons (PEPs).*[103]

From the moment a financial institution identifies a customer as a PEP, it shall take the following measures[104]:

- First, it should undertake measures in order to determine the source of proceeds the counterparty will bring to a potential future business relationship. The disclosure of the source of wealth allows the retail bank to ensure that this source is non-illicit. The source must be based on relevant data and reports provided by independent and reliable entities.

- Secondly, the senior management will approve the start of a business relationship between the PEP and their bank. The senior management should be kept aware of the risks regarding the PEP in question; they must ultimately decide whether they are capable of managing the risks.[105]

- Subsequently, after approval by the senior management, the retail bank should implement enhanced, ongoing monitoring of the transactions carried out by the PEP,

[103] Infra, Chapter 7.
[104] Joint Committee of the European Supervisory Authorities, 'Joint Guidelines under Article 17 and 18(4) of Directive (EU) 2015/849 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), JC 2015/061, 26, <https://www.eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf > accessed 8 May 2017.
[105] Ibid 26.

with an eye to any potential future risks related to the business relationship. In the case of suspicious transactions, the bank must take appropriate measures. The level of risk associated with the PEP in question establishes the frequency of the ongoing audit. Lastly, the firm should apply the latter measures to relevant family members and close associates in an identical way, taking into account the risks linked to their profile.[106]

- Additionally, it is worth mentioning that in both cases third parties can execute the CDD. Article 25 of the 4AMLD explicitly sets out under which circumstances such representation is allowed. Notwithstanding that, it is the obliged entity which remains ultimately liable.[107] The subsequent article in the Directive underlines, once again, the link between CDD and the RBA by prohibiting third parties in high-risk third countries to conduct the SDD or EDD.[108]

7.2 Consequences in the event of an unsuccessful CDD

Given these points, it is important to remember the following key principles regarding the SDD and EDD. After the completion of the aforementioned steps, the financial institution should always be aware of the risks they face and never agree to a business relationship if the entity is unable to comply with their CDD requirements. In the event the business relationship was already established, the firm should abort or discontinue the transactions.[109]

Chapter 6: Financial Exclusion

[106] Ibid 26.
[107] Etay Katz, 'Implementation of the Third Money Laundering Directive - an overview', (2007) 1(3) Law and Financial Markets Review, 35, <http://www.tandfonline.com/doi/abs/10.1080/17521440.2007.11427880> accessed 11 May 2017.
[108] Art 26 4AMLD.
[109] Joint Committee of the European Supervisory Authorities, 'Joint Guidelines under Article 17 and 18(4) of Directive (EU) 2015/849 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) JC 2015/061, 95, <https://esas-joint-committee.europa.eu/Publications/Guidelines/Final_RBSGL_for_publication_20161115.pdf> accessed 8 May 2017.

8 The side effect of the 4AMLD

<[The] tightening of money laundering rules in response to terrorist attacks means that many people may face difficulty in getting access to services>[110]

Throughout the years, academics and policymakers have written numerous opinion pieces on the notion of financial exclusion. The EC employs the following definition: *'Financial exclusion refers to a process whereby people encounter difficulties accessing and/or using financial services and products in the mainstream market that are appropriate to their needs and enable them to lead a normal social life in the society in which they belong'.*[111]

Nowadays, access to financial institutions is seen as a need in the EU, as it is a relatively cashless society. Thus, financial exclusion goes hand in hand with social exclusion. For instance, certain types of transactions such as receiving a regular electronic salary or pensions are indicative of being employed. This is what is termed as social inclusion.[112] According to statistics from the year 2013, 10 % of adults in EU countries which joined before 2004, and 47 % of adults in MS who joined the EU since May 2004, had no bank account at all.[113] A range of causes can explain the financial exclusion of certain people. One of the reasons is the trend of AML/CTF measures becoming more stringent. For instance, some people are incapable of fulfilling the identity requirements imposed by the 4AMLD, and are thus faced with an inability to open a bank account.[114]

---

[110] Luisa Anderloni, Emanuele Maria Carluccio, 'Access to Bank Accounts and Payment Services; New Frontiers in Banking Services' (Springer, 2006), 5.
[111] European Commission, 'Report on financial services provision and prevention of financial exclusion' (2008) 9, <http://ec.europa.eu/social/BlobServlet?docId=760> accessed 18 May 2017.
[112] European Commission, 'Report on financial services provision and prevention of financial exclusion' (2008) 50, <http://ec.europa.eu/social/BlobServlet?docId=760> accessed 18 May 2017.
[113] Eurobarometer Surveys 60.2 (EU15) and 2003.5 (EU10).
[114] European Commission, 'Financial Inclusion: Ensuring access to a basic bank account' (consultation document, 2009) 6, <http://ec.europa.eu/internal_market/consultations/docs/2009/fin_inclusion/consultation_en.pdf> accessed 18 May 2017.

As mentioned before, financial institutions are subject to several duties before entering in and throughout a business relationship with a counterparty. Customer due diligence is one of these prescribed requirements.

The requirements set out in the 4AMLD and elucidated above seem to be the main reasons for financial exclusion in EU society.[115] Overall, it appears that there are no easy solutions to the problem of financial exclusion. The EC seems to prefer national solutions over tackling financial exclusion itself; according to the white paper on EU Financial Services Policy, it does not consider dealing with financial exclusion as one of its key tasks.[116]

Chapter 7: Politically exposed persons

The concept of politically exposed persons is a very important one with regards to the combat against money laundering, corruption and terrorist financing. It is also very much related to the CDD process. Due to the position they hold, PEPs have a significantly higher risk of misusing the financial system or being the subject of bribery or corruption, which might contribute to money laundering and the financing of terrorism.[117]

With the 4AMLD, the definition of 'politically-exposed persons' has undergone drastic changes from the definition in the 3AMLD. In the 4AMLD, PEPs are '*persons who have been entrusted with prominent public functions by foreign countries, or domestically, or by an international organization'*.[118] Namely, the European Council dropped the distinction between domestic and foreign PEPs, which resulted in the inclusion of national PEPs into the

[115] CGD, 'Unintended consequences of Anti-Money Laundering Policies for poor countries' 7, <https://www.cgdev.org/sites/default/files/CGD-WG-Report-Unintended-Consequences-AML-Policies-2015.pdf> accessed 10 May 2017.
[116] Santiago Carbo Valverde, Edward P. M. Gardener, Philip Molyneux, 'Financial Exclusion in Europe', (2007) 27(1) Public Money & Management, 26, <http://dx.doi.org/10.1111/j.1467-9302.2007.00551.x> accessed on 31 July 2017.
[117] FATF Recommendations; Press release of 16 February 2012.
[118] FATF, 'Politically Exposed Persons' (FATF Guidance, 2013) 10, <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf> accessed 11 May 2017.

definition incorporated in the 4AMLD.[119]

Moreover, the latter AMLD lists in an exhaustive manner the specific functions a natural person may hold in order to be considered a PEP. The exhaustive list includes, for instance, heads of State or government; minister or members of certain courts; and some of their family members.[120]

The elimination of the conceptual difference between national and foreign PEPs, and the listing of certain high-risk parties, goes far beyond the FATF recommendations. The Commission defends its decision to eliminate the differentiation between domestic and foreign PEPS with the following words: '<...enhanced due diligence…conducted for each category of PEP…would give greater clarity and more consistency to the provisions, while placing the EU ahead of the international standard...>'[121].

Although it is not a new feature implemented by the 4AMLD, it is important to mention that an individual will be treated as a PEP for a period of 12 months after leaving their former position. Moreover, the measures taken by the EC relating to PEPs are supposed to be seen as preventive and have no criminal nature. The same statement underlines the fact that the EC does not approve of financial institutions refusing a business relationship purely based on the counterparty being a PEP.[122]

Policy options	**Comparison criteria**		
	Effectiveness	Efficiency	Coherence
1. No change	0	0	0

[119] Janos Böszörmenyi, Erich Schweighofer, 'A review of tools to comply with the Fourth EU anti-money laundering directive', (2015) International Review of Law, Computers & Technology, 66, <http://dx.doi.org/10.1080/13600869.2015.1016276> accessed 26 April 2017.
[120] Ibid 74.
[121] European Commission, 'Impact assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing and Proposal for a Regulation of the European Parliament' (Staff Working Paper), SWD(2013) 21 final, 37.
[122] Recital 33, 4AMLD.

2. Introduce requirements for domestic PEPs/PEPs in international organisations with risk-sensitive elements	+ Meets objective of widening scope + Complies Operational Objective 1	+ Addresses highest risk (foreign PEPs) and allow a graduated approach to other PEPs - Differential approach may lead to inconsistencies	+ Consistent with international standards
3. Extend provisions for international PEPs to domestic PEPs and PEPs in international organisations	+ Meets objective + Requirement goes some way to Operational Objective 3. - Goes further than objective	+ Clarity in requirement - Costly for industry, without corresponding benefit	- Goes further than international standard

123

The above impact assessment made by the EC clearly demonstrates that the choice to make both national and foreign PEPs subject to 4AMLD has several positive and negative effects. Notably, foreseeing EDD for all the PEPs creates greater expenses for the financial industry and clearly goes further than the recommendations of the FATF. All the same, the elimination of the distinction creates clarity for the financial institutions that have the duty of implementing the measures.

Chapter 8: Third Country Equivalence

The previously examined topic of the RBA is closely related to the so-called Third Country Equivalence. For the purpose of clarification, an RBA means that the obliged entities identify and assess the money laundering and terrorism financing risks to which they are exposed, and act appropriately given the level of risk. One of the elements which may indicate a higher risk of money laundering or terrorism finance is the geographical location of a country.

[123] European Commission, 'Impact assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing and Proposal for a Regulation of the European Parliament' (Staff Working Paper), SWD (2013) 21 final, 79.

Formerly, under the 3AMLD, the Member states could agree on a list of third countries that imposed regulatory requirements on their national financial institutions that were equal or comparable to the requirements provided in the 3AMLD. This so-called 'Common Understanding between Member States on third country equivalence' listed a catalogue of twelve countries, which had similar AML/CTF mechanisms as the EU, such as Australia and Singapore.[124] Article 11 of the 3AMLD made it possible for financial institutions located in the EU/EEA – as well as the countries listed in the Common understanding - to apply SDD measures. The aforementioned list was subject to updates and frequent revisions at the EU level.[125] The whole concept of third countries being considered equivalent was called into question, since the country risk is only one small factor among many that are relevant for assessing the risk in the field.[126]

In contrast to the 3AMLD, in the 4AMLD, the Commission identifies the third-country jurisdictions that have strategic deficiencies representing a threat to the EU financial system. Instead of a list of third countries with equivalent measures against money laundering and the financing of terrorism, there has been established a 'blacklist', where the EU focuses on regimes which are non-equivalent.[127]

> *Article 9;*
>
> *Third-country jurisdictions which have strategic deficiencies in their national AML/CFT regimes that pose significant threats to the financial system of the Union ('high-risk third countries') shall be identified in order to protect the proper*

---

[124] 'Common understanding between Member States on third country equivalence under the Anti-Money Laundering Directive (Directive 2005/60/EC)', <http://ec.europa.eu/internal_market/company/docs/financial-crime/3rd-country-equivalence-list_en.pdf> accessed 12 May 2017.

[125] The Joint Money Laundering Steering Group, 'Prevention of money laundering/combating terrorist financing' (2013), <http://www.jmlsg.org.uk/download/9006> accessed 12 May 2017.

[126] European Commission, 'Impact assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing and Proposal for a Regulation of the European Parliament' (Staff Working Paper), SWD(2013) 21 final, 19.

[127] Daren Allen, 'Comparison Table: Fourth Money Laundering Directive (4MLD); Changes from 3MLD' (Thomas Reuters Regulatory Intelligence, 2016) 6, <https://smartsales.thomsonreuters.com/exLink.asp?111968458OB67R57I344295266> accessed 17 May 2017.

functioning of the internal market.

The factors relevant in the latest AMLD are set out in paragraph 2 of the same article mentioned above, namely:

(a) the legal and institutional AML/CFT framework of the third country, in particular:

(i) criminalisation of money laundering and terrorist financing;

(ii) measures relating to customer due diligence;

(iii) requirements relating to record-keeping; and

(iv) requirements to report suspicious transactions;

(b) the powers and procedures of the third country's competent authorities for the purposes of combating money laundering and terrorist financing;

(c) the effectiveness of the AML/CFT system in addressing money laundering or terrorist financing risks of the third country

Contrary to the 3AMLD, which was primarily focused on aspects such as the political stability in a country and the level of corruption, the current Directive takes into account factors that are consistent with the principles laid out in the RBA standards. The list of factors and criteria are non-exhaustive, although they are seen as highly relevant by the EC. In particular, the effectiveness of the AML/CTF measures is of great importance. Besides the codification of the relevant measures and requirements, the respective administration must also apply the measures according to the national law of the government.

Referencing the explanatory memorandum of the 4AMLD, the high-risk third countries list is certainly *not* a list to name and shame. Rather it is a list to indicate the third countries with

which the EU is willing to enhance and strengthen their AML/CTF procedures by initiating dialogue with the goal of eliminating deficiencies. In light of what was written in the paragraphs above, it is important to point out that the creation of such a list does not have the objective of limiting trade and financial relations with the listed countries. The legal effect of being included in the list of 'high-risk third countries' finds expression in Article 18 of the 4AMLD.[128] Namely, the obliged entities must evoke EDD measures when dealing with legal or natural entities located in a high-risk third country.[129]

Chapter 9: Safe Interenvios Case, C-235/14

The Safe Interenvios Case (hereafter, Safe Case) is a highly interesting case in light of the CDD measures incorporated in the 4AMLD.[130] This case was initiated at the time the 3AMLD was still in force, but was nonetheless relevant against the background of the most recent AMLD. This case clearly shows the strong interaction between CDD and the RBA.

9. Facts

A financial institution called 'Safe' was established in Spain and received a request by its partner banks to supply additional information on its counterparties and the destination of their transactions for the purposes of CDD. Safe decided not to provide additional information, which led to the closure of the related accounts, executed by the partner banks where Safe held bank accounts. Subsequently, Safe contested the closing of the relevant accounts by saying that the closing of the specific accounts did not comply with the 3AMLD and its CDD provisions. Safe immediately initiated a lawsuit at the Court which was largely unsuccessful, although the Court ruled that the disclosure of the account was not properly

[128] European Commission delegated Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 by identifying high-risk third countries with strategic deficiencies', (2016) OJ L 254/1.
[129] Ibid.
[130] Case C235/14, Safe Interenvíos, (2016) ECL I-154.

justified by the partner banks. All three banks (Safe, Sabadell and Liberbank) appealed the ruling of the Court, and the Provincial Court in Barcelona asked the CJEU for a preliminary ruling.

The *preliminary question* was two-pronged:

- Whether the CDD measures, prescribed in the 3AMLD, could be enforced by a financial institutional even though every financial institution is already under the supervision of competent authorities.
- Additionally, the Court raised the question whether in such a situation the standard, simplified, or enhanced due diligence measures must be applied.

9.1 Decision of the CJEU

The CJEU followed the opinion of the Advocate General in this case, stating that all entities subject to CDD obligations should apply an RBA and thus take CDD measures.[131] This seemed necessary from their point of view, taking into account their exposure to certain risks.[132] The fact that Safe was a financial service provider was of no importance. Other banks could have a legitimate interest in requesting information from Safe about its client. Overall, Sabedell and Liberbank asking for information about the clients of Safe was deemed permissible under the 3AMLD and Payment Service Directive.[133]

With reference to the second matter, the Court acknowledged that when the obliged entities identify a situation with a potentially higher risk of money laundering and terrorism financing, EDD measures should be applied. This statement of the Court is contradictory to the provisions incorporated in the 3AMLD. Namely, the 3AMLD stipulates that SDD shall be

[131] Opinion Advocate General presented 3 September 2015 in the ECJ Case C-235/14, Safe Interenvios.
[132] ECJ, C-235/14, Safe Interenvios, para 72.
[133] Council Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

applied towards other financial institutions. In high-risk cases, the entitled entities need to obtain information about the customers of the financial service provider (such as Safe). Therefore, the bank could have a legitimate interest in asking its client – the insurance undertaker – to provide information about the final policyholders for AML/CDD purposes. Furthermore, personal data protection regulations are not an obstacle to obtaining information about the customers of its client.[134]

9.2 Safe Interenvios Case under the 4AMLD

For the purpose of this paper, we will now analyze the relevant elements of the case in light of the adjusted provisions adopted in the 4AMLD.

First, we should examine the initial question asked of the CJEU, namely, if due diligence can be carried out between financial institutions. The 3AMLD envisaged an SDD between financial institutions.

> <... The fact that Article 11(1) *requires* that covered entities should not be subject to standard customer due diligence measures... allow[s] Member States to authorize simplified due diligence...> [135]

Although Article 11(1) 3AMLD authorizes the MS to implement SDD towards financial institutions, it does not derogate from the former Article 7(c);

> <... The institutions and persons covered by this Directive shall apply customer due diligence measures in the following cases:
>
> (c) when there is a suspicion of money laundering or terrorist financing,

[134] Bonn & Schmitt, 'New AML/CDD requirements following the ECJ's Case C235/14' (2016), 4, <http://bonnschmitt.net/fileadmin/media/Legal_Info_Our_Publications/Our_Legal_Alerts/B_S_Legal_Alert_New_tendencies_of_KYC_after_the_ECJs_case_Safe_Interevios_SA.pdf> accessed 19 May 2017.
[135] Art 11(1) 3AMLD.

regardless of any derogation, exemption or threshold; [136]

The situation has drastically changed under the 4AMLD, which enhanced its RBA and contains more detailed provisions relating to CDD. The 4AMLD strictly allows the application of an SDD once the obliged entity has ascertained that the business relationship or transaction presents a significantly lower degree of risk.[137] Notably, in cases where the obliged entities identify potentially higher risk, MS must entrust the latter to apply EDD in order to 'mitigate the risk appropriately'.[138]

Thus, as seen above, the reading by the Advocate General was already in line with the draft of the 4AMLD at that time.

Since the 4AMLD was put in place, the last traces of a *rule-based approach* have been abolished. Thus, the financial institutions subject to the new AMLD have - within the scope of the Directive - more discretionary power to decide whether or not to apply standard, simplified, or enhanced DD measures. This is the concept of a holistic, risk-based approach via evidence-based decision-making.[139]

9.3 Relevance of the Safe Interenvios Case

Overall, the Safe case has not caused any major revolutions in the fields of AML and CDD. It must be said that all concepts and principles set out in this case were already incorporated in the FATF Recommendations (although they were not all explicitly mentioned in the 3AMLD, which was still in place at the time of the ruling). The Recommendations were, in the course of the lawsuit, seen as guidance for market participants (in other words, soft law).

---

[136] Opinion Advocate General presented 3 September 2015 in the ECJ Case C-235/14, Safe Interenvios, para 93.
[137] Art 15(2) 4AMLD.
[138] Art 18(1) 4AMLD.
[139] Recital 22, 4AMLD.

Moreover, the Advocate General emphasized the importance of interpreting the Directive - and likewise, the future Directives such as the 4AMLD - in accordance with the FATF Recommendations.[140] The CJEU reaffirmed this point of view.[141]

Thus, market participants have the duty not only to comply with the national and EU regulation on AML, but also to take into account the Recommendations of the FATF whilst interpreting relevant provisions and establishing internal rules, policies, and codes of conduct. In some cases, non-compliance with the Recommendations is regarded as a deficiency at the level of the entitled entities, which could even lead to the imposition of sanctions. [142]

Chapter 10: The link between CDD and the RBA

The solution to reducing the risk of money laundering was to establish a standard for risk analysis, namely the RBA. The innovation of this approach has led to the identification and prevention of money laundering activities in a more effective and sophisticated manner. By way of example, Recital 18 states that: '*To ensure effective monitoring of compliance with this Directive [. . .] Member States may focus their monitoring activities in particular on those natural and legal persons trading in goods that are exposed to a relatively high risk of money laundering or terrorist financing, in accordance with the principle of risk based supervision'*.[143]

Article 13 underlines the link between CDD and the RBA. Namely, the identification of the customer and the categorization of the business relationship allows the financial institution to conduct the CDD according to a specific approach, based on the risk of money laundering or terrorist financing.[144]

---

[140] Opinion Advocate General presented 3 September 2015 in the ECJ Case C-235/14, Safe Interenvios, para 7.
[141] ECJ, C-235/14, Safe Interenvios, para 3.
[142] Bonn & Schmitt, 'New AML/CDD Requirements following the ECJ's case 234/14' (2016), 5, < http://bonnschmitt.net/fileadmin/media/Legal_Info_Our_Publications/Our_Legal_Alerts/B_S_Legal_Alert_New_tendencies_of_KYC_after_the_ECJs_case_Safe_Interevios_SA.pdf> accessed 3 May 2017.
[143] Rectical 18, 4AMLD.
[144] Mariano Fernandez Salas, 'The third anti-money laundering directive and the legal profession' (2005), 7,

Article 13:

> *Customer due diligence measures shall comprise:*
>
> *(a) identifying the customer and verifying the customer's identity on the basis of documents, date or information obtained from a reliable and independent source;*
>
> <....>
>
> *(c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;*

Given the nature of the RBA, it is evident that the companies subject to the 4AMLD are obliged to show greater levels of involvement in order to detect risks. Their involvement includes obtaining, analyzing and sharing relevant information about their customers, as well as obtaining access to the initial source of their proceeds. Hence, experts assume that the volume of relevant information will increase by broadening the range of businesses engaged in financial crime prevention, especially since certain sectors - such as the automotive industry - are at a high risk of being used by criminal entities. In line with this, the Directive covers not only financial services actors but a range of other private actors like casinos, real estate firms, lawyers, notaries, company service providers, and providers of goods when payments are made in cash in excess of €15,000.[145]

The link between both notions - RBA and CDD - occurs in different stages and occasions within the process of identifying the relevant risks.

To begin with, attention must be brought to the fact that the RBA generally precedes CDD. It encourages a proper assessment of the AML risk in regards to a person's business and customers; the institution should inform and determine the level of CDD that should be

---

<http://www.anti-moneylaundering.org/Document/Default.aspx?DocumentUid=7B528765-CB1F-4748-9733-68935E2C4745> accessed 3 May 2017.

[145] Maria Bergstrom, Karin Svedberg Helgesson, Ulrika Morth, 'A New Role for For-Profit Actors? The Case of Anti-Money Laundering and Risk Management', (2011) 49(5) JCMS, 1043.

undertaken for each customer.[146]

Second comes the stage where the customers have been divided into low- or high-risk categories and the recently updated RBA is conducted. The CDD measures which will be put in place, EDD and SDD, are much more far-reaching than in the past (and include the documentation of identity and labeling of the ownership structure).

Lastly, the RBA further emphasizes that monitoring must be continuous. Surveillance and (re)categorization are to be on-going processes. This involves a potential adjustment to the sort of CDD carried out by the actors. It is self-evident that this adjustment can shift both ways, from the EDD to SDD or the other way around.[147]

Chapter 11: Beneficial Ownership

10. Definition

The FATF defines an ultimate beneficial owner (UBO) *as*:

> 'the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise the ultimate effective control over a legal person or arrangement' *(FATF 2010, 110)*

Adopting the recently updated EU perspective, reference can be made to the definition

[146] DFSA, 'Applying a risk-based approach' ('RBA'), 1, <https://www.dfsa.ae/Documents/DNFBP%202013/Applying%20a%20Risk%20Based%20Approach.pdf> accessed 18 July 2017.

[147] Maria Bergstrom, Karin Svedberg Helgesson, Ulrika Morth, 'A New Role for For-Profit Actors? The Case of Anti-Money Laundering and Risk Management', (2011) 49(5) JCMS, 1043, 1051.

provided by Article 3(6) of the 4AMLD, which defines the UBO 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 and includes at least:

(a) in the case of corporate entities:

(i) 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. A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a natural person shall be an indication of direct ownership. A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership. This applies without prejudice to the right of Member States to decide that a lower percentage may be an indication of ownership or control. Control through other means may be determined, inter alia, in accordance with the criteria in Article 22(1) to (5) of Directive 2013/34/EU of the European Parliament and of the Council (3);

(ii) if, after having exhausted all possible means and provided there are no

grounds for suspicion, no person under point (i) is identified, or if there is any doubt that the person(s) identified are the beneficial owner(s), the natural person(s) who hold the position of senior managing official(s), the obliged entities shall keep records of the actions taken in order to identify the beneficial ownership under point (i) and this point;

(b) in the case of trusts:

(i) the settlor;

(ii) the trustee(s);

(iii) the protector, if any;

(iv) the beneficiaries, or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

(v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means;

c) in the case of legal entities such as foundations, and legal arrangements similar to trusts, the natural person(s) holding equivalent or similar positions to those referred to in point (b);

10.1 General

One of the most groundbreaking obligations incorporated in the 4AMLD is that the aforementioned entities - located in the EU - should hold information on their beneficial ownership in an accurate and adequate way. This means going beyond basic information such

as the company name and address and includes, for example, its legal ownership.[148]

Thus, the 4AMLD puts in place specific parameters in order to provide answers regarding the question of the identity of the beneficial owner. The Directive allows MS to include a great range of entities in any beneficial ownership determination and to consider relevant evidential measures, as well as absolute thresholds for beneficial ownership assessments. For instance, in the case of the ownership of 25 percent or more of a corporation, the beneficial owner will be the natural person with ultimate ownership of the legal entity. In the case of the ownership of 25 percent or more of the legal entity, there will be the legal assumption of beneficial ownership. When dealing with a trust, the beneficial owner will be the settlor, trustees, protector, beneficiaries (or any class of them), and any other natural person with ultimate control over the trust, whether by direct or indirect ownership.[149]

10.2 Register of beneficial ownership

In addition to the measures implemented to enhance transparency, with the goal of combatting the misuse of legal entities, all MS are also obliged to introduce an ultimate beneficial ownership register. This central register – held outside the company - must contain appropriate information on the beneficial ownership. Entities, such as corporations, other legal entities, and trusts, are required to maintain up-to-date and accurate information on beneficial ownership.

Each of the MS, having the choice to use a central database, a business registry or another customized central register, will hold the information on beneficial ownership.

Important to the above is the aspect of the accessibility of the information. Competent

---

[148] ACAMS, 'The Fourth EU AML/CTF Directive: a holistic risk-based approach, 77, <http://files.acams.org/Images/email/2015/bulletin-europe/The_Fourth_EU_AML_CTF_Directive.pdf> accessed 19 July 2017.

[149] Darren Allen, 'Comparison table; Fourth Money Laundering Directive (4MLD); changes from 3MLD' (Thomson Reuters Regulatory Intelligence, 2016), 2, <https://smartsales.thomsonreuters.com/exLink.asp?111968458OB67R57I344295266> accessed 18 July 2017.

authorities, such as national financial intelligence units (FIU), should always be able to access the relevant information when the obliged entity in each case launches CDD measures. The information obtained on beneficial ownership should also be made available to other persons who have a legitimate concern about other threats, such as terrorist financing, corruption, tax crimes and fraud. Nevertheless, the access should be granted in accordance with data protection rules.[150]

10.3 Beneficial owners and data protection

The creation of a register of beneficial ownership involves the gathering of a wide range of different categories of data. Operations important to the assemblage of data are numerous, ranging from collecting, processing, and withholding the relevant data of customers. The abundant amount of relevant data could eventually be used in investigations by law enforcement authorities. In this manner, the CDD procedures could create a conflict with regard to privacy and data protection.[151]

The aspect of privacy and data protection has never been a matter of concern in the combat against money laundering and the financing of terrorism. This has changed with the adoption of the 4AMLD. In an attempt to strengthen the transparency and protection of fundamental rights, the 4AMLD lays down various data protection safeguards.

The MS recognized the necessity of different kinds of safeguards to accompany the key innovation of a central register in each MS.[152] More precisely, the UBO registers must ensure timely and unrestricted access by competent authorities and FIUs, without the need to alert the entity concerned. They must also allow timely access by obliged entities when undertaking CDD.[153] Notably, the 4AMLD stipulates that obliged entities, such as financial service

[150] Ibid 2.
[151] Valsamis Mitsilegas, Niovi Vavoula, 'The evolving EU anti-money laundering regime; challenges for fundamental rights and the rule of law', (2016) MJ, 261.
[152] Art 30(3) 4AMLD.
[153] Art 30(6) 4AMLD.

providers, must obtain and hold '<<... adequate, accurate and current information on their beneficial ownership...>>[154]

Other persons demonstrating a legitimate interest are granted access to the data.[155] However, the Directive does not foresee full public access. MS can make use of their national legislative power in order to create conditions of access that are broader. Thus, Recital 15 could create circumstances where some EU nationals have less data protection rights than others.[156]

Despite the opportunity to broaden the right for some people to access the information gathered, article 30(9)[157] states that MS have the possibility to deny access to not only third parties, but also to obliged entities. Denial is also allowed for any beneficial owner where such access would create a certain risk of fraud, or when he is a minor. This article offers the MS a broad margin of discretion and consequently puts limits on the possibility created by the Directive through Recital 15.[158]

With this set of rules in mind, it is important to note that the Directive contains a direct reference to the 'purpose limitation principle'. Such a principle is crucial for ensuring that the collection and processing of information is compatible with the purpose of the 4AMLD, and limited to what seems to be strictly necessary.[159][160] Hence, collecting and processing data for commercial purposes is prohibited.[161]

Given these points, the data protection provisions included in the 4AMLD represent a

---

[154] Recital 14 4AMLD.
[155] Council, 'Proposal for a Directive of the European Parliament and of the Council, on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing', COD (2013) 0025, 11.
[156] The FATF Guidance on beneficial ownership of 2014 foresees that such data can be made accessible to the public, but it needs to be balanced with privacy concerns.
[157] Art 30(9) 4AMLD.
[158] Valsamis Mitsilegas, Niovi Vavoula, 'The evolving EU anti-money laundering regime; challenges for fundamental rights and the rule of law', (2016) 23 MJ, 261, 279.
[159] Recital 43 4AMLD.
[160] Art 41(2) 4AMLD.
[161] Valsamis Mitsilegas, Niovi Vavoula, 'The evolving EU anti-money laundering regime; challenges for fundamental rights and the rule of law', (2016) 23 MJ, 261, 281.

significant improvement in comparison to the previous Directives. Nonetheless, several matters are left to the discretion of the MS, e.g. the refusal of access for third parties and the extension of the retention period. This margin of discretion given to the MS raises questions with regards to proportionality issues and divergent national legislation.

Chapter 12: Penalties and supervision

The Council has agreed to create a whole range of different administrative sanctions that can be imposed on the obliged entities. The role of the individual MS is also crucial, since they should ensure the administration of these sanctions, as well as take measures regarding provisions of the Directive.

Recital 59 of the 4AMLD emphasizes the importance of combating money laundering and terrorism financing, which should result in MS engaging their authorities to enact effective and proportionate administrative sanctions and measures in their national legislation. This should all be done in compliance with the provisions incorporated in the Directive. More importantly, the range of administrative sanctions should only be enforced in cases of serious, repeated, or systematic breaches of the requirements relating to the key elements of the 4AMLD. These include CDD, reporting of suspicious transactions, and record-keeping. [162].

Moreover, the broad range of sanctions and measures created by the legislator allows MS and national authorities to impose different sanctions that take into account the nature of the business (specifically, the peculiarities between credit institutions, financial institutions, and numerous other entities subject to the Directive). With regards to the imposition of administrative sanctions and measures, the principle of *ne bis in idem* should be respected by

[162] Recital 59 4AMLD.

the respective MS.[163]

Article 59 of the 4AMLD foresees a broad and very detailed provision for cases in which the obliged entities breach specified obligations prescribed by the Directive. This is in contrast to the very narrow and inadequate provisions in the former 3AMLD, which caused divergent administrative sanctions in the MS.[164] As a matter of fact, the 4AMLD harmonizes the administrative sanctions and measures along the different MS, in cases of breaches of certain provisions.

Administrative sanctions and measures can be enforced in the circumstances set out in Article 59:[165]

> 1. Member States shall ensure that this Article applies at least to breaches on the part of obliged entities that are serious, repeated, systematic, or a combination thereof, of the requirements laid down in: (a) Articles 10 to 24 (customer due diligence); (b) Articles 33, 34 and 35 (suspicious transaction reporting); (c) Article 40 (record-keeping); and (d) Articles 45 and 46 (internal controls).
>
> 2. Member States shall ensure that in the cases referred to in paragraph 1, the administrative sanctions and measures that can be applied include at least the following: (a) a public statement which identifies the natural or legal person and the nature of the breach; (b) an order requiring the natural or legal person to cease the conduct and to desist from repetition of that conduct; (c) where an obliged entity is

[163] Recital 59 4AMLD.
[164] Art 39 4AMLD: "...Member States shall ensure that natural and legal persons covered by this Directive can be held liable for infringements of the national provisions adopted pursuant to this Directive. The penalties must be effective, proportionate and dissuasive..."
[165] Art 59 4AMLD.

subject to an authorization, withdrawal or suspension of the authorization; (d) a temporary ban against any person discharging managerial responsibilities in an obliged entity, or any other natural person, held responsible for the breach, from exercising managerial functions in obliged entities; (e) maximum administrative pecuniary sanctions of at least twice the amount of the benefit derived from the breach where that benefit can be determined, or at least EUR 1 000 000.

3. Member States shall ensure that, by way of derogation from paragraph 2(e), where the obliged entity concerned is a credit institution or financial institution, the following sanctions can also be applied: (a) in the case of a legal person, maximum administrative pecuniary sanctions of at least EUR 5 000 000 or 10 % of the total annual turnover according to the latest available accounts approved by the management body; where the obliged entity is a parent undertaking or a subsidiary of a parent undertaking which is required to prepare consolidated financial accounts in accordance with Article 22 of Directive 2013/34/EU, the relevant total annual turnover shall be the total annual turnover or the corresponding type of income in accordance with the relevant accounting Directives according to the last available consolidated accounts approved by the management body of the ultimate parent undertaking; L 141/108 EN Official Journal of the European Union 5.6.2015 (b) in the case of a natural person, maximum administrative pecuniary sanctions of at least EUR 5 000 000, or in the Member States whose currency is not the euro, the corresponding value in the national currency on 25 June 2015.

1. Member States may empower competent authorities to impose additional types of administrative sanctions in addition to those referred to in points (a) to (d) of paragraph 2 or to impose administrative pecuniary sanctions exceeding the amounts

referred to in point (e) of paragraph 2 and in paragraph 3.

Logically, there must be a form of supervision by the competent national authorities, in order to impose the aforementioned sanctions and measures. Articles 47 and 48 of the 4AMLD cover this subject, the importance of which should not be underestimated.

To put it briefly, Articles 47 and 48 stipulate that the competent authorities of the different MS must monitor effectively and take the measures necessary to ensure compliance with the Directive. The MS must grant the competent authorities the adequate powers, as well as human and technical resources to perform their functions according to the Directive. According to the Articles in the Directive, it is crucial that the national authorities maintain high professional standards and take into account the standard of confidentiality in relation to data protection.

Lastly, it is important to mention that the MS can provide the competent authorities with enhanced supervisory powers during the supervision of credit or financial institutions, as well as gambling services. The allowance of enhanced powers demonstrates the higher risk of these institutions being used to facilitate money laundering or the financing of terrorism.

Chapter 13: A symbiosis between the risk-based approach, customer due diligence and the beneficial owner

11. General

From the previous chapters, it is clear that there is a set of regulations, and, more specifically, there are defined guidelines to which the financial services industry needs to adhere. The tools set out in the 4AMLD are created in order to manage and mitigate financial crime. In the following chapters, the importance of the combination of the RBA, CDD, and UBO will be described. This will shed light on the end result of applying these tools and the integration of the tools in the 'compliance duty' of the financial service providers.

Nowadays, 'compliance' is a very common term in the financial services industry and is intrinsic to its operations. From a regulatory point of view, compliance is conforming to a regulation, policy, or relevant law. Compliance has gained a lot of significance for financial service providers worldwide. Compliance is important not only for protecting consumers, but also for reducing the risk of legal and regulatory sanctions, loss in reputation, or financial loss. Thus detection, prevention, and resolution of violations of laws and regulations are the main features of the compliance function of any financial service provider:[166]

Compliance, if done correctly, will impact the functioning of a bank in a positive way. In such cases, one uses a very inclusive term 'positive compliance,' which brings business and governance perfectly together. In other words, the interests of the different stakeholders have been brought together in a harmonious, coexisting model, taking into account the sometimes opposing interests of business and governance. This harmony will only be possible if the organization applies a *three-line defense model*, with the emphasis on a proactive approach.[167]

It is worth pointing out that all three regulated and required processes (RBA, CDD and UBO) are an integral part of the broader compliance process and to the three lines of defense model. Moreover, the interaction and coexistence of those three processes are indispensable for a good outcome of this model.

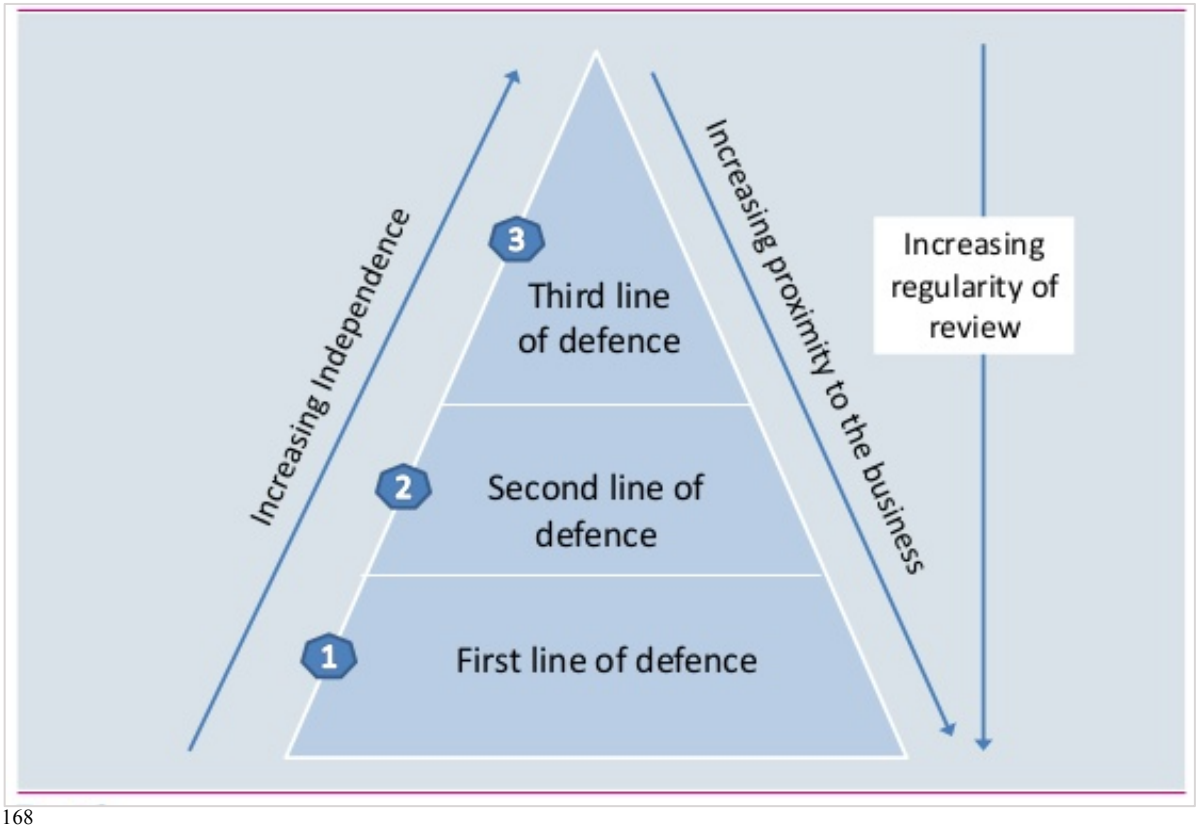
---

[166] Saloni P. Ramakrishna, 'Enterprise Compliance Risk Management: An Essential Toolkit for Banks and Financial Services' (John Wiley & Sons, 2015), 240.
[167] Ibid 240.

11.1 Three lines of defense model

"Money plays the largest part in determining the course of history" Karl Marx

Throughout this paper, various risk and control functions have been explained. However, we must not forget that the existence of the aforementioned legal requirements and processes - such as risk rating, know-your-customer, and the creation of a register of beneficial owners - are not sufficient to combat money laundering and terrorist financing in an efficient way, nor are they sufficient for preventing any reputational risk.



168

The chart above clarifies that responsibilities must be defined by the Board of Directors of the financial services provider in question, so that every professional who makes up one of the three levels knows exactly their position, duty, and boundaries in the risk and control structure

168 Bovill, 'Financial Crime, Anti-Money Laundering' (2014), 8, <https://www.slideshare.net/BovillRegulatory/financial-crime-antimoney-laundering-bovill-briefing> accessed 27 October 2017.

of the organization. This is essential since each of these three 'lines' plays a distinct role within the governance structure of any financial services provider.[169]

The three lines of defense model can enhance clarity regarding money laundering or terrorist financing risks and controls, besides helping to improve the effectiveness of risk management systems already put in place.

11.1.1 First line of defense

The first line of defense for a financial services provider is mainly composed of front-line employees who must have a thorough education in and knowledge of the combat against money laundering and terrorist financing. They are the closest to the customers demanding certain products or services. Therefore, they must apply a systematic risk process and internal controls. These processes and controls, for instance gathering information on the nature of the assets of the customer as well as their wishes (KYC), are elaborated in the relevant policies of the bank. Depending upon the size of the financial services provider, the front-line department may have a risk management committee to conduct the KYC/CDD, which includes a PEP-check and UBO-tracing, along with the risk assessment.

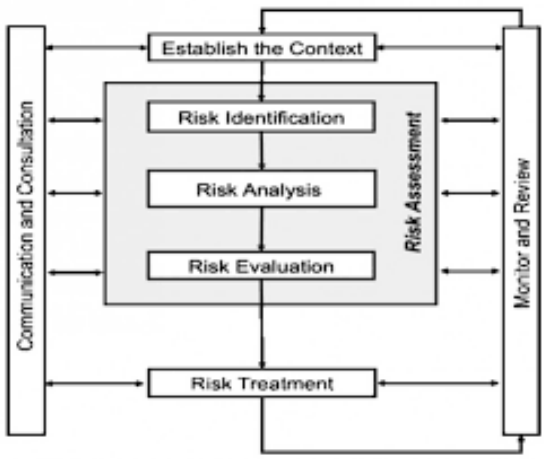
In other words, the front-line management has to gather relevant information, assess the potential risks, and execute the controls according to the organization's policies. Already here, at the first line of defense, we notice the interaction between not only compliance and business, but also between KYC/CDD, RBA, and UBO tracing.[170]

11.1.2 Second line of defense

[169] The Institute of Internal Auditors, 'IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control' (2013), 2, <https://www.theiia.org/3-Lines-Defense> accessed 27 October 2017.
[170] Ken Doughty, 'The Three lines of Defense Related to Risk Governance', (2011) 5 ISACA Journal, 1, <https://www.isaca.org/Journal/archives/2011/Volume-5/Pages/The-Three-Lines-of-Defence-Related-to-Risk-Governance.aspx> accessed 27 October 2017.

The second line of defense of any financial services provider is composed of a compliance and risk division that offers independent oversight and review of the controls and activities of the first line of defense. The second level is known as the 'management assurance' line.

Generally, the second line involves three kinds of challenges. These are termed transactional, regulatory, and risk-related. For the purpose of this paper, only the regulatory and risk-related controls are relevant.



In view of the above, the second line of defense must ensure compliance with, for instance, the 4AMLD; more specifically, it must determine whether the KYC/CDD, UBO and PEP-checks are conducted in accordance to internal policies, which in turn are a reflection of the minimum standards of the 4AMLD.[171]

According to the scheme above, the second line will receive information from the first line and evaluate the possible risk detected by the first line.[172] If necessary, the second line will undertake determined measures. For example, in cases where the first line identifies a customer with previous fraud convictions holding a cash-intensive business, they will escalate it to the second line of defense, who in turn will evaluate the situation. The evaluation of the situation may consist of risk identification; risk analysis; an evaluation towards the end of the process; or a risk treatment. The second line will monitor and review this specific case according to the legal provisions and their internal policies.

[171] Joe Valasquez, 'Setting up a Second Line of Defense and the Art of the Challenge' (2015), 2, <http://rsmus.com/what-we-do/industries/financial-institutions/setting-up-a-second-line-of-defense-and-the-art-of-challenge.html> accessed 27 October 2017.

[172] Note that the first line functions in an independent way, but interacts with the second line, and vice versa.

The challenge of the second line is to successfully review the findings of the first line, meaning there is an ongoing interaction between the two lines.

Furthermore, the risk assessment conducted by the second line will use the KYC/CDD as the basis of their assessment. Based on the information obtained during the KYC/CDD process, the first and second line can identify a possible PEP or classify someone as a UBO. This will result in specific measures outlined in the chapters above.[173]

Thus, there is a certain balance between effective challenge and compliance within the different lines of defense, which brings us to the third level of defense that has an essential position in this chain.

11.1.2 Third line of defense

The third line of defense comprises both an internal and external audit function. Although the first and second lines are ultimately independent, intense interaction between the two levels is necessary. By contrast, the practice is that the third line of defense must be strictly independent. This is achieved by following a specific structure. Generally, financial service providers entrust the Board of Directors with the responsibility of conducting internal audits. Such audits range from quarterly reviews to assessing very delicate matters on a case-by-case basis. The communication is conducted in a formal manner and at all times in writing.[174]

The third line of defense is never involved in the activity of KYC/CCD or the PEP and UBO identification, since this is reserved for the first and - under specific circumstances - second lines. The Board of Directors will only come into play when it comes to proposing and voting on relevant policies and procedures with regard to CDD or the tracing of PEPs.

---

[173] Joe Valasquez, 'Setting up a Second Line of Defense and the Art of the Challenge' (2015), 2, <http://rsmus.com/what-we-do/industries/financial-institutions/setting-up-a-second-line-of-defense-and-the-art-of-challenge.html> accessed 27 October 2017.

[174] G20/OECD, 'Principles of Corporate Governance' (2015), <http://www.oecd.org/corporate/principles-corporate-governance.htm>accessed 27 October 2017.

On a yearly basis, the Board of Directors will audit the organization and assess the functioning of the compliance department in an objective manner. Their audit can, for instance, consist of assessing which business units or processes exhibit a high level of residual risk or backlog.

Though the second line executes ongoing risk-assessments, the third line of defense only performs a periodic, risk–based audit.[175]

Beyond the internal audit team, external auditors focus on the overall governance and control structure, such as the different stages of a PEP or UBO-check. Moreover, they will assess whether relevant regulations are complied with in an adequate manner. Thus, regulatory issues such as compliance with the 4AMLD will take center stage in most external audits. Over the years it became apparent that the results of the risk assessments conducted by the first and second lines of defense are of secondary importance. [176]

In conclusion, the first step in the process of an adequate CDD, RBA, and UBO or PEP identification is the acceptance of compliance requirements both in letter and spirit. All three levels are equally important, since procedures and policies are of no significance if there is no spirit of compliance in the organization. The legally required processes prescribed in the 4AMLD are translated into several organizational structures in order to achieve good results.

CONCLUSION

This conclusion will serve as the answer to the research question: what are the regulatory changes incorporated in the 4AMLD and to what extent is there an interaction between the

[175] Joe Valasquez, 'Setting up a Second Line of Defense and the Art of the Challenge' (2015), 2, <http://rsmus.com/what-we-do/industries/financial-institutions/setting-up-a-second-line-of-defense-and-the-art-of-challenge.html> accessed 27 October 2017.

[176] Isabella Arndorfer, Andrea Minto, 'The Four Lines of Defence Model for financial institutions' (2015), 7-8, <http://www.bis.org/fsi/fsipapers11.pdf> accessed 27 October 2017.

RBA, CDD and UBO?

This study of the EU's Fourth Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing has shown that both public and private actors play a major role in making this Directive a worthwhile undertaking. On one hand, the private actors, or obliged entities, are facing various new requirements ranging from enhanced RBA to an ongoing monitoring of their customers. Additionally, the public authorities are charged with a whole list of duties in order to combat the financing of terrorism and money laundering.

Although significant improvements have been made, such as the issuing of specific guidelines for retail banks and the creation of a list of high-risk third countries, the 4AMLD has many shortcomings. Striking examples of such shortcomings are the relatively unclear provisions on the data protection of EU citizens and the lack of provisions on the cooperation between different MS in the fight against terrorism.

More importantly, throughout the whole Directive there is not one explicit provision on the interaction between the three aforementioned concepts. By looking at the 'Safe Interenvios Case', we have been able to deduce a link between CDD and RBA. Namely, the nature of the counterparty is not relevant; the CDD and a thorough risk assessment are indispensable. Furthermore, the fact that the counterpart is a financial institution is not a legitimate criterion for non-adherence to the CDD/RBA provisions.

There is yet another interaction between both the CDD and RBA, namely, financial institutions are not eligible to allow third parties in high-risk countries to conduct the CDD. This proves that the EU has put a lot of effort into the creation of this Directive, and

proactively thwarted a method to avoid its requirements.

All in all, the chapter on the *three-line defense* is the most illustrative example of the interaction between the three aforementioned concepts. This becomes very apparent by looking at the procedures conducted at every level of a financial services transaction. The different concepts or requirements incorporated in a law suddenly form a cohesive structure where each single line depends on and interacts with the others. On the whole, the Directive is not explicitly referring to any situations where the RBA, CDD and UBO are interacting and melt together as one coherent procedure.

Given the latest series of terrorist attacks in Europe, and the ongoing changes in world politics, the current Directive will be soon subject to amendments and additional counter measures, as the threat of terrorism is closely interlinked with the activity of money laundering. Thus, the challenge for the EU is to ensure that its rules and enforcement keep pace with evolving trends and developments in the society in order to mitigate the risk of terrorist attacks