palgrave▸pivot

THE NEW ANTI-MONEY LAUNDERING LAW

First Perspectives on the 4th European Union Directive

Domenico Siclari

The New Anti-Money Laundering Law

Domenico Siclari
Editor

The New Anti-Money Laundering Law

First Perspectives on the 4th European Union Directive

palgrave
macmillan

Editor
Domenico Siclari
Sapienza Università di Roma
Roma, Italy

ISBN 978-3-319-29098-0   ISBN 978-3-319-29099-7 (eBook)
DOI 10.1007/978-3-319-29099-7

Library of Congress Control Number: 2016939224

Printed on acid-free paper

This Palgrave Macmillan imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Contents

Notes on Contributors

Roberto Formisani currently works at the Bank of Italy in the Organisation Directorate (focusing on internal regulations of the Bank) and is currently reading for a PhD in Corporate and Securities Law at the University of Bologna. Previously, he worked for the Italian Banking Association, where he dealt with the reform of the European system of financial supervision and got a five-month research internship in the Banking Supervision Department of the Bank of Italy. He published some articles in Italian legal journals and participated, as contributor, to a commentary on Italian Corporate Law.

Pierpaolo Fratangelo is Deputy Head of the AML/CFT Unit in the Banking and Financial Supervision Department at the Bank of Italy. He is a member of the Italian Delegations to FATF and to Council of Europe/Moneyval. He is the representative of the Bank of Italy to the Basel Committee AML Expert Group. He was formerly a teaching assistant at the University of Rome "La Sapienza" (2011–2012) and at LUISS—Guido Carli (2007–2009). He has served as co-editor of the *International Encyclopaedia for Labour Law and Industrial Relations*. He has written numerous articles on anti-money laundering, monetary and financial law, cyber law, and European law. He received a DES in European Law from the Université Libre de Bruxelles, 1997. He graduated *summa cum laude* in Law from the University of Siena.

Elena Giacone is a public official of the Italian Tax Administration. She works at the Legislative Office of the Ministry of Economy and Finance where she is in charge of all national and EU dossiers on public games. She previously lent his work, in defence of the Italian Tax Administration, in the field of labour disputes (2004–2009). She practised as a professional lawyer in a major law firm, mainly dealing with civil matters with a focus on public tendering law (2000–2004). She collaborates with the Department of Law, University of Roma “Tor Vergata” where she earned a PhD (2015) in Civil Procedural Law.

Domenico Siclari is Associate Professor of Economic and Financial Markets Law at Rome Sapienza University, Department of Economics and Law. He had previously worked as officer at Bank of Italy in Rome (1999–2003), in the field of banking and financial supervision, focusing on payment system oversight and has attended several meetings for study and research at the European Central Bank, in Frankfurt am Main. He was later a Counselor of the Italian Parliament-Chamber of Deputies (2003–2013), where he has been in charge of the Finance Division of Research Department since 2004. In 2013, he received the National Academic Qualification as Full Professor. He is member of the scientific committee at PhD in “Public, Comparative and International Law” in Rome Sapienza University, of Referees Committee of “Rivista Trimestrale di Diritto dell’Economia”, of Advisory Board of “Law and Economics Yearly Review”, of Italian Association of Professors and scholars of Economic and Financial Markets Law (ADDE).

Pierluigi Tonnara is a PhD candidate in Public Law of Economy at Rome Sapienza University, Department of Economics and Law. He graduated in Law and, since then, has been providing legal assistance on several matters, such as administrative law, economic regulation, public procurement, public companies, public services, town planning and building regulation, energy and environment. He currently works at the Legislative Office of the Ministry of Economic Development.

Andrea Zaccagna is Research Assistant in Economic and Financial Markets Law at Rome Sapienza University, Department of Economics and Law. Currently, he is tax and legal consultant for several multinational companies based in Italy. He had previously worked as Human Capital consultant at the international law firm *Ernst&Young* in Rome (2012–2015), in the field of Taxation and Labour Law, focusing on advisory services for expatriated employees.

CHAPTER 1

Introduction

Domenico Siclari

Abstract This book gives a first critical comment of the changes introduced by the new Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (the Fourth anti-money laundering (AML)/counter terrorism financing (CFT) Directive).

This book aims to provide a first critical comment of the changes introduced by the new Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering (ML) or terrorist financing (TF) (the Fourth anti-money laundering/counter terrorism financing (AML/CFT) Directive),[1] 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 (the Third AML/CFT Directive).[2]

Fortunately, it has been gaining increasing awareness of the need to combat, through appropriate provisions, the criminal phenomenon of ML, which is assuming ever larger dimension[3] capable of threatening the stability of the global financial system:[4] as has been authoritatively stated, "effective anti-money laundering and combating the financing of terrorism regimes are essential to protect the integrity of markets and of the global financial framework as they help mitigate the factors that facilitate financial abuse."[5]

D. Siclari (ed.), *The New Anti-Money Laundering Law*,
DOI 10.1007/978-3-319-29099-7_1

In the "Europeanisation" of the fight against crime within the EU area of freedom, security, and justice,[6] the new EU Directive represents a further step towards the setting up of common rules, methods, and practices[7] for combating crimes which, if not properly prevented and punished, can lead to consequences of subverting the proper functioning of financial markets.

The new regulatory framework welcomes the risk-based approach (RBA): it acknowledges that the levels and types of action required to be taken by Member States, supervisors, and firms will differ according to the nature and severity of risks in particular jurisdictions and sectors, clarifying the types of situations in which simplified customer due diligence (CDD) will be appropriate, as well as those situations where it is necessary for firms to conduct enhanced checks.

We have new rules concerning the extended definition of politically exposed persons—PEPs (here is clarified that enhanced due diligence will always be appropriate where transactions involve PEPs), inclusion of tax crimes as predicate offences, national- and Europe-wide risk assessments, reinforcement of sanctioning powers and requirements to coordinate cross-border action, lower exemptions for one-off transactions and expansion of the perimeter, meet new requirements on beneficial ownership information, increase transparency by requiring companies and trusts to hold information on their beneficial ownership, and make this information available to supervisors and parties conducting due diligence on them.

In this book, Chap. 2 explains the changes to the current EU AML/CFT requirements on CDD, increasing the emphasis on the RBA. The new design is motivated by the changing nature of ML and TF threats: facilitated by the constant evolution of technology and of the means at the disposal of criminals, the variables associated with ML/TF risks are such that it is impossible to sketch a single regulatory taxonomy and to impose a "one size fits all" solution. Thus, the idea is to affirm a model where obliged entities have to understand the ML and TF risks they face and adopt the most cost-effective and proportionate way to manage and mitigate them, calibrating adequate countermeasures.

By illustrating the new set of CDD requirements, describing how the new architecture would work, Chap. 2, in particular, emphasises that obliged entities should take appropriate steps to identify and assess the risks of ML and TF, taking into account risk factors including those relating to their customers, countries or geographic areas, products, services, transactions, or delivery channels. Those steps must be proportionate to the nature and size of the obliged entities. Obliged entities should also have in place policies, controls, and procedures to mitigate and manage effectively these risks of ML and TF.

The broad objective is that obliged entities should know who their customers are, what they do, and whether or not they are likely to be engaged in criminal activity. In this respect, obliged entities must decide, on the basis of their assessment of the risks posed by different customer/product combinations, on the level of verification that should be applied at each level of risk presented by the customer. Thus, according to the risk level, obliged entities have to decide whether to apply simplified, normal, or enhanced due diligence controls. Public authorities will support the private sector in applying the RBA with a risk assessment conducted both at national and at supranational level in order to identify major risks that pose a threat to single Member States as well as to the Internal Market as a whole and to elaborate adequate policies and countermeasures. In parallel, these findings will be made available to obliged entities to help them conduct their own risk assessment.

Chapter 3 deals with the regulation of beneficial ownership assessment, as part of the new "customer due diligence" duties set forth by the Fourth EU AML Directive. After a discussion on the relevance of identifying the actual owner behind legal and corporate schemes, so as to overcome some of the most common "layering" and "placement" laundering techniques, it focusses on the provisions embodied in the Financial Action Task Force (FATF) Recommendations, comparing the 2003 edition and the revision occurred in 2012 (and all the related interpretative documents), which concern not only the definition of beneficial ownership but also the performance of CDD duties in this regard: the main point of interest is the new "progressive approach" in ascertaining actual owners of the schemes. With reference to the European legislation, Chap. 3 describes how the FATF Recommendations (2003 ed.) have been implemented by the European legislator under the repealed Third Directive in 2005, with brief reference to some Member States' national implementing measures. As far as the Fourth EU AML Directive is concerned, the new provisions on beneficial ownership are described, with a special emphasis on the new disclosure requirements aimed at providing public bodies and to the business community as a whole, especially by means of the reporting of data disclosed in a "central public register," so as to strengthen the public supervision and to ease the CCD duties' performance. In the end, it discusses the main options for national legislators regarding the implementation of the new beneficial ownership legislation, with a view to possible changes in the role of central business registers.

Chapter 4 faces with the relevant problem of supervision of payment institutions that operate across borders by agents. In fact, most Member States result host some agents operating on a European passport under the EU Payment System Directive (PSD); a large number of Member States act as the home regulator for cross-border payment institutions. Risks associated with the money transfer sector, especially operating through agents, are considered very high.

In this framework, various criminal investigations found out that the money transfer networks are misused for ML purposes or for TF purposes by criminal organisations. Payment System (PS) agents, whenever they are not financial institutions, are considered as presenting an inherent ML/FT high risk, due to their absence of control mechanisms in terms of the prevention of AML/CFT on the overwhelming number of agents operating in these conditions (gas stations, subway stations, supermarkets).

In EU Member States, there have been reported some cases of countries where the requirement of a central contact point (CCP) has been set up by their national legislation. From this new system of rules derive various problems related to the supervision of the money services agents. For example, a very relevant issue concerns which jurisdiction's (home or host) AML/CFT law should apply when such delegated inspections took place.

We would need—just to avoid reduced competition between the laws of the Member States in the implementation of the new EU Directives—as fast as possible harmonisation of procedures for the supervision of payment institutions by agents. It will be a crucial common approach to the regulation of cross-border PS agents within Europe at present, to counter the risk of violation domestic law and distortion of competition within a local market because of uncontrolled AML/CFT measures by using a huge network of agents. The justified interests of the PS industry to get predictable regulatory conditions need a "standardised" and uniform regulatory approach.

Chapter 5 details a new strategy of risk-based regulation introduced by the Fourth EU AML Directive—risk assessment—structured on three levels: the supranational/EU level (Article 6), the national level (Article 7), and the obliged entities' level (Article 8). These levels are linked to and fed by each other in a dynamic way, even though a supremacy role is attributed, to some extent, to the European Commission. More specifically, the European Commission is entitled to (a) prepare a risk assessment report, also on the basis of European Supervisory Authorities (ESAs') opinion, Member States' and obliged entities' information, and international organisations' report; (b) recommend the Member States to adopt specific measures with a "comply-or-explain" mechanism; and (c) individuate high-risk third countries and adopt the relevant measures to avoid AML/CFT policies be jeopardised. The Member States are entitled to (a) designate an authority or establish a coordinating mechanism to address ML; (b) carry out periodical risk assessments; and (c) identify any areas where obliged entities are to apply enhanced measures and, where appropriate, specifying the measures to be taken. The obliged entities have to conduct their own risk assessments and adopt the relevant AML/CFT policies.

Moreover, the Fourth EU AML Directive boosts the international cooperation. More specifically, all involved institutions are called to act jointly to achieve common AML/CFT objectives and Member States are called to supervise on and ensure AML/CFT compliance of obliged entities, regardless to where such obliged entities operate their establishments. Finally, the new EU Directive gives some guidance on the relations between data protection and risk assessment and on the accuracy of statistics. Actually, only accurate, precise, and updated statistical data may lead to credible risk assessments. Risk assessment is to be welcomed since it may significantly boost AML/CFT policies. However, flows of information are useful only when they are well selected and, above all, when policies really take place. In this regard, recent experiences teach that a lot is yet to be done.

Chapter 6 faces to tax crimes inclusion in "criminal activity" definition as relevant for AML purposes. The main category of predicate offences from which ML arise is related to tax crimes. They are money evaded from the State balance, saved and hidden by those who do not pay taxes. It is easy to understand how this situation affects severally the economy of the States, already weakened by European sovereign debt crisis that has been taking place in the EU since the end of 2009. On the basis of these considerations, the EU Member States have felt the need to combat ML with any tools. Already in its 12 February 2012 Recommendations, FATF-GAFI included expressly Tax crimes in the category of *predicate offences* in order to extend the application field of Anti-Money Laundering Law.

The 2012 April Paper from the European Commission proposed to examine if the current approach of use of "all serious offences" could be sufficient to include also tax crimes or if they should be included in the specific category of "serious offences" according to art. 3, n. 5 or if it would be better to give a more precise definition of tax crimes. The solution chosen by Directive IV is the second one such as the inclusion of tax crimes in a specific category of “serious offences” to art. 3, n. 4 letter f. The new EU Directive includes tax offences in the range of predicate offences that qualify criminal activity, such as to constitute the basis of ML.

The Directive IV highlights that “tax crimes” relating to direct and indirect taxes includes tax crimes in the broad definition of “criminal activity,” in line with the revised FATF Recommendations. Given that different tax offences may be designated in each Member State as constituting “criminal activity,” national law definitions of tax crimes may diverge. While no harmonisation of the definitions of tax crimes in Member States’ national law is sought, Member States should allow, to the greatest extent possible under their national law, the exchange of information or the provision of assistance between EU Financial Intelligence Units (FIUs).

The tax crimes inclusion in the definition of criminal activity is undoubtedly an important innovation of the Fourth Directive, especially considering that the most part of ML arise from tax crimes activities. The entry into force of the new joint European standards raises a crucial information asset of European states contributing to the international fight against tax evasion.

Chapter 7 considers the effects of new rules on gambling sector. Article 2 of the Fourth EU AML Directive clearly specifies that it applies not only to casinos, already affected by the previous Directive, but also to “providers of gambling services,” including those online. In fact, unlike the Third Directive which generically referred to casinos without giving a specific definition of them, Article 3, paragraph 14 of this Directive defines “gambling services” as those services which involve wagering a stake with monetary value in games of chance, including those with an element of skill such as lotteries, casino games, poker games, and betting transactions that are provided at a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services.

The approach of the new Directive is always based on risk—that is, the nature of the relationship, constant monitoring, and detection of suspicious transactions—although this approach presents major difficulties for its application in the field of gambling, since it presupposes a knowledge of the player which it is not comparable to that possessed by credit institutions and/or financial institutions in general.

However, the European legislator took into account the specificities of this activity, allowing the appropriate supervision that the Member

State will decide to apply to public gambling, in particular, for transactions amounting to EUR 2000 or more, without providing, however, any exemption for casinos. The goal, in fact, is to have an impact again on the obligations to conduct CDD, having considered it necessary to increase the clarity and transparency of the related rules in order to have adequate controls and procedures to enable a better knowledge of the customer and greater understanding of the nature of the activities performed by him.

The Directive therefore extends the scope of the obligation to apply appropriate CDD also to all the entities offering goods or providing services against payment in cash of amounts of EUR 15,000 or more, as well as to operators of public gambling who conduct financial transactions amounting to over EUR 2000, both in the case where the movement takes place in a single transaction and in the case where it is attained through multiple transactions connected to each other.

There remains, however, the need to proceed in each case to an adequate verification, regardless of any threshold, exemption, or derogation, in all suspicious cases of ML or TF, as well as whenever there are doubts as to the data obtained during the identification of customers previously performed.

An important novelty of the new EU Directive is the introduction of the principle that allows Member States the possibility to exempt, with the exception of casinos, gambling operators of lower risk situations from the rules transposing the Directive in question, according to the lower risk proven by the nature and, as appropriate, by the operating size of such services. In these cases, it will be necessary for the national legislators to seize the main aspects because, if it is true that the sectors/individual types of lower risk gambling should not be subject to obligations relating to ML, it is also undeniable that the verification of customers should not be the only pivot on which to base the fight against ML from illegal activities. In this regard, the Commission itself suggested as a method of monitoring the supply chain of the incentive to use alternative means of payment other than cash for all types of game, even land-related ones.

Another important new feature of the Directive is that relating to the clarification that the competent authorities should ensure that, with regard to currency exchange offices, cheque cashing offices, trust or company service providers, or gambling service providers, the persons who effectively direct the business of such entities and the beneficial owners of such entities are fit and proper. The criteria for determining whether or not a person is fit and proper should, as a minimum, reflect the need to protect such entities from being misused by their managers or beneficial owners for criminal purposes.

An analysis of the new Directive displays, therefore, the highly ambitious objectives which it intends to achieve, primarily the attention to the consistency between European and international approaches, the consistency between national rules and a certain degree of flexibility in their application by strengthening and clarifying the obligations, and ensuring that the standards are focused on risk and adequate to the new emerging threats. However, it would have been advisable to have, within the gambling sector, a higher degree of effectiveness and specificity for the actions permitted, along with an equal expansion of the tools made available notably to provide more certainty to the so-called CDD.

Notes

1. Published in *Official Journal of the European Union* of 5 June 2015 (L 141/73).
2. About the repealing of the Third AML/CFT Directive see J. Komárek (2008) "Legal Professional Privilege and the EU's Fight Against Money Laundering," in *Civil Justice Quarterly* Vol. 27; M. Bergstrom, K. Svedberg Helgesson and U. Morth (2011) "A New Role for For-Profit Actors? The Case of Anti-Money Laundering and Risk Management" *Journal of Common Market Studies* Vol. 49, 5, 1043; P.J. Ruce, Anti-Money Laundering: The Challenges of Know Your Customer Legislation for Private Bankers and the Hidden Benefits for Relationship Management ("The Bright Side of Knowing Your Customer"), in *Banking Law Journal*, 2011, Vol. 128, No. 6, 548; M. van den Broek, The EU's preventive AML/CFT policy: asymmetrical harmonisation, in *Journal of Money Laundering Control*, 2011, Vol. 14, 2, 170; J. Simser, Money laundering: emerging threats and trends, in *Journal of Money Laundering Control*, 2013, Vol. 16, 1, 41; P. Fratangelo, International anti-money laundering policies and the protection of financial integrity, in R. Miccù and D. Siclari (ed.), *Advanced Law for Economics. Selected Essays*, Turin, Giappichelli, 2014; D. Masciandaro, A. Volpicella, Economics and Politics in Designing Supervision: The Case of the FIUs Against Money Laundering, Baffi Center Research Paper No. 2014-156, 2014; M. Usman Kemal, Anti-money laundering regulations and its effectiveness, in *Journal of Money Laundering Control*, 2014, Vol. 17, 4, 416.
3. See, in this regard, Walker, J. (1999), "How Big is Global Money Laundering?," *Journal of Money Laundering Control*, 3(1), 25 ss.; Unger, B. (2007), The Scale and Impact of Money Laundering, Cheltenham, UK: Edward Elgar; Walker, J., and Unger, B. (2009), "Measuring Global Money

Laundering: The Walker Gravity Model," *Review of Law and Economics*, 5(2), 821 ss.
4. See D. Masciandaro (1999), "Money Laundering: the Economics of Regulation," *European Journal of Law and Economics*, No. 3, p. 225; R. Bowles, M. Faure and N. Garoupa (2005), "Forfeiture of Illegal Gain: An Economic Perspective" *Oxford Journal of Legal Studies*, Vol. 25, No. 2, p. 275; D. Masciandaro, E. Takatz and B. Unger B. (2007), Black Finance. The Economics of Money Laundering, Edward Elgar, Cheltenham.
5. Min Zhu, Deputy Managing Director of the International Monetary Fund (www.imf.org).
6. E. Herlin-Karnell, The EU's anti-money laundering agenda: built on risks?, in C. Eckes and T. Konstadinides (eds.), *Crime within the Area of Freedom, Security and Justice. A European Public Order*, Cambridge University Press, 2011, p. 76.
7. See, *ex multis*, E. Ioannides (2014), *Fundamental Principles of EU Law Against Money Laundering*, Ashgate.

CHAPTER 2

The CDD Obligations Following a Risk-Based Approach

*Pierpaolo Fratangelo**

Abstract The Fourth Directive on anti-money laundering and counter terrorism financing advocates the risk-based approach to customer due diligence (CDD) measures. The article illustrates the new set of requirements, describing how obliged entities should take appropriate steps to identify and assess the risks associated with the customer and decide the adequate CDD regime.

2.1 Introduction

With the adoption of a Fourth Directive on anti-money laundering (AML) and counter terrorism financing (CFT),[1] the European Union (EU) confirms its engagement to protect the Internal Market against such criminal activities. Money laundering (ML) and terrorist financing (TF) have in fact the potential to threat the integrity, proper functioning, reputation, and stability of the European financial system, with likely devastating outreach for the economic and social system as a whole.

The Fourth Directive is built upon the framework designed by Directive 2005/60/EC[2] (the so-called third AML Directive), but far from being a simple update, the new text introduces important changes to the current architecture, increasing the emphasis on the risk-based approach (RBA)

*Banca d'Italia – banking and financial supervision department. The views expressed are those of the author and do not necessarily represent those of the Banca d'Italia.

D. Siclari (ed.), *The New Anti-Money Laundering Law*,
DOI 10.1007/978-3-319-29099-7_2

and moving away from the current system of exemptions from customer due diligence (CDD) requirements based on third-country equivalence.

The new design is motivated by the changing nature of ML and TF threats: facilitated by the constant evolution of technology and of the means at the disposal of criminals,[3] the variables associated with ML/TF risks are such that it is impossible to sketch a single regulatory taxonomy and to impose a "one size fits all" solution, especially to 28 different national contexts; neither it is imaginable for a permanent adaptation of the legal framework to counter such threats. The idea is then to affirm a model where obliged entities have to understand the ML and TF risks they face and adopt the most cost-effective and proportionate way to manage and mitigate them,[4] calibrating adequate countermeasures.

Public authorities will contribute to the effective implementation of this RBA with a risk assessment conducted both at national and at supranational level in order to identify major risks that pose a threat to single Member States as well as to the Internal Market as a whole and to elaborate adequate policies and countermeasures. In parallel, these findings will be made available to obliged entities to help them conduct their own risk assessment.

To a large extent, EU rules are based on AML international standards set by the Financial Action Task Force (FATF). According to the FATF Recommendations of February 2012, the RBA allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures in order to target their resources more effectively and apply preventative measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way.[5] The application of an RBA is therefore not optional, but a prerequisite for the effective implementation of the FATF Standards.

Hence, a correct understanding and implementation of the RBA will be key in the successful enforcement of the Fourth Directive. For this purpose, each obliged entity should have in place policies, controls, and procedures to mitigate and manage effectively the risks of ML and TF identified at the level of the EU, the Member State, and the obliged entity itself in order to properly apply the CDD requirements set by the Directive.

2.2 A New Approach to ML and TF Risks

AML legislation requires financial intermediaries to have a thorough knowledge of their customers as well as a fully understanding of the transactions they put in place. To this end, obliged entities have to design a

CDD process that allows them to monitor customers' activities and detect possible suspicious transactions. As soon as this happens, financial intermediaries should file a Suspicious Transaction Report to competent authorities that will further investigate in the matter. This is particularly evident for the financial sector where, as pointed out by the Basel Committee on Banking Supervision, these requirements are to be seen as a specific part of the general obligation to have in place sound risk management programmes so as to address all kinds of risks, including ML and FT risks.[6]

According to the RBA, the intensity and scope of the obligation to carry out adequate CDD are to be determined in accordance with the risk of ML and TF as it arises from factual circumstances.[7] This means that intermediaries should thoroughly analyse the concrete case under management, assess the associated ML/TF risks, define a proper risk profile and, thus, the appropriate level of mitigation to be applied.

This understanding should be based on specific operational and transaction data and other internal information collected by the obliged subject as well as on external sources of information such as national risk assessments and country reports from international organisations.

The implementation of a RBA in AML/CFT mirrors the adoption of risk-sensitive requirements in other financial regulatory domains and is intended to address the problems inherent in prescriptive regulatory approaches: over-regulation, rigidity and consequently poor regulatory performances, and a focus on formalism rather than regulatory effectiveness.[8]

The RBA allows obliged entities to be more efficient and effective in their use of resources and minimise burdens on customers. Focusing on higher risk threats should mean that beneficial outcomes can be achieved more effectively. In addition, an RBA allows financial institutions to more efficiently and effectively adjust and adapt as new ML and TF methods are identified.

At the same time, the RBA makes more difficult for launderers to employ the financial system due to the increased focus on the identified higher risk activities that are being undertaken by these criminal elements.

However, such an approach requires resources and expertise to gather and interpret information on risks, both at the country and institutional levels, to develop procedures and systems and to train personnel. It further requires that sound and well-trained judgement be exercised in the implementation within the institution and its subcomponents of such procedures, and systems.

Implementing an RBA requires that obliged entities have a good understanding of the risks and are able to exercise sound judgement. This requires the building of expertise within financial system, including, for example, through training, recruitment, taking professional advice, and "learning by doing."

This also means that no two institutions are likely to adopt the exact same detailed practices. Such potential diversity of practice will require that authorities make greater effort to identify and disseminate guidelines on sound practice, and may pose challenges to supervisory staff working to monitor compliance.[9]

An RBA is not aimed at preventing obliged entities from engaging in transactions with customers or establishing relationships with potential customers, but rather it should assist them to effectively manage potential ML and TF risks.

2.3 The CDD

The Fourth Directive requires obliged entities to perform CDD when establishing a business relationship or when carrying out occasional transactions that amounts to EUR 15,000 or more, regardless of whether the transaction is carried out in a single operation or in several operations that appear to be related, or that constitutes the transmission or transfer of funds, as defined in Regulation (EU) 2015/847, exceeding EUR 1000. CDD is also required in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 10,000 or more, or for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2000 or more, whether the transactions are carried out in a single operation or in several operations which appear to be linked. Regardless of any applicable derogation, exemption, or threshold, CDD should also be performed when there is a suspicion of ML or TF or when there are doubts about the veracity or adequacy of previously obtained customer identification data (article 11).

CDD implies the identification and verification of the customer and, where applicable, of the beneficial owner (i.e., the natural person who ultimately owns or controls an account and/or the person on whose behalf a transaction is being conducted);[10] it is also required to obtain information on the purpose and intended nature of the business relationship. Financial intermediaries must ensure ongoing monitoring of the relationship in accordance with the ML/TF risk profile assigned to each customer on the basis of the information acquired. CDD procedures should allow an ongoing monitoring of customers in order to periodically review their risk profile (article 13).

When financial institutions are unable to comply with CDD requirements laid down by Directive, they may not establish the relationship or carry out transactions or professional services or they have to terminate the continuous relationship or professional service and must assess whether to make a report to the Financial Intelligence Unit (FIU) (article 14).

Obliged subjects should have in place policies and procedure to detect unusual or potentially suspicious transactions (articles 15 and 18). To this end, it is very common to see the use of electronic screening software dedicated to the monitoring of transactions.

2.4 Risk Assessment and the Risk Profile of Customers

Article 8 of the Fourth Directive requires Member States to ensure that obliged entities take appropriate steps to identify and assess the risks of ML and TF, taking into account risk factors including those relating to their customers, countries or geographic areas, products, services, transactions, or delivery channels. Those steps must be proportionate to the nature and size of the obliged entities.

This risk assessment has to be documented, kept up to date, and made available to the relevant competent authorities and self-regulatory bodies concerned. Competent authorities may decide that individual documented risk assessments are not required where the specific risks inherent in the sector are clear and understood.

The Fourth Directive also requires obliged entities to have in place policies, controls, and procedures to mitigate and manage effectively the risks of ML and TF identified at the level of the Union, the Member State, and the obliged entity. These policies, controls, and procedures must be proportionate to the nature and size of the obliged entities.

These policies, controls, and procedures shall notably include the development of model risk management practices, CDD, reporting, record keeping, internal control, compliance management including, where appropriate with regard to the size and nature of the business, the appointment of a compliance officer at management level, and employee screening. In addition, where appropriate with regard to the size and nature of the business, an independent audit function should test the internal policies, controls, and procedures.

The broad objective is that obliged entities should know who their customers are, what they do, and whether or not they are likely to be engaged in criminal activity. This risk profile of customers will build up over time, allowing the firm to identify transactions or activity that may be suspicious. In this respect, obliged entities must decide, on the basis of their assessment of the risks posed by different customer/product combinations, on the level of verification that should be applied at each level of risk presented by the customer. Consideration should be given to all the information a firm gathers about a customer, as part of the normal business and vetting processes. Consideration of the overall information held may alter the risk profile of the customer.

Obliged entities have to obtain approval from their senior management for the policies, controls, and procedures that they put in place and to monitor and enhance the measures taken, where appropriate.

2.5 Simplified Due Diligence and Exemptions

The simplified due diligence is a case in point for the new RBA adopted under the Fourth Directive. The provisions of the Third Directive on simplified due diligence were found to be overly permissive, with certain categories of client or transaction being given outright exemptions from due diligence requirements. The Fourth Directive therefore tightens the rules on simplified due diligence and does not permit situations where exemptions apply. Instead, decisions on when and how to undertake simplified due diligence have to be justified on the basis of risk, while minimum requirements of the factors to be taken into consideration would be given.

In particular, the Fourth Directive allows the use of simplified CDD measures when obliged entities ascertain that the business relationship or the transaction presents a lower degree of risk (article 15). This assessment shall be based taking into account factors of potentially lower risk situations set out in Annex II of the Directive: (i) customer risk factors such as public companies listed on a stock exchange and subject to disclosure requirements, public administrations or enterprises, and customers that are resident in geographical areas of lower risk; (ii) product, service, transaction, or delivery channel risk factors such as life insurance policies for which the premium is low, insurance policies for pension schemes and pensions, superannuation or similar schemes that provide retirement benefits to employees, financial products or services that provide appropriately defined and limited services for financial inclusion purposes, and products where the risks of ML and TF are managed by other factors such as purse limits or transparency of ownership; and (iii) geographical risk factors such as activities in Member States or in third countries having effective AML/CFT systems, third countries identified by credible sources as having a low level of corruption or other criminal activity, and 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 ML and TF consistent with the FATF Recommendations and effectively implement these requirements.

In all these cases, however, obliged entities have to carry out sufficient monitoring of the transactions and business relationships to enable the detection of unusual or suspicious transactions.

In addition, article 12 of the Fourth Directive recognises that electronic money may be considered as low risk when specific risk-mitigating conditions are met: (i) the payment instrument is not reloadable, or has a maximum monthly payment transactions limit of EUR 250 which can be used only in a specific Member State;[11] (ii) the maximum amount stored electronically does not exceed EUR 250; (iii) the payment instrument is used exclusively to purchase goods or services; (iv) the payment instrument cannot be funded with anonymous electronic money; and (v) the issuer carries out sufficient monitoring of the transactions or business relationship to enable the detection of unusual or suspicious transactions.

According to the FATF Recommendations, examples of simplified CDD measures include verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g., if account transactions rise above a defined monetary threshold); reducing the frequency of customer identification updates; reducing the degree of ongoing monitoring and scrutinising transactions, based on a reasonable monetary threshold; and not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

2.6 Enhanced Due Diligence

At the opposite side of the risk spectrum, it should be recognised that certain situations present by definition a greater risk of ML or TF. In these cases, enhanced due diligence (EDD) measures should be applied (articles 18–24).

The Fourth Directive replicates the Third Directive in requesting EDD measures for cross-border correspondent relationships with a third-country respondent institution or for correspondent relationship with a shell bank. But the Fourth Directive adds other situations such as, in the first place, relationships with natural persons or legal entities established in high-risk third countries identified by the Commission. The country risk assessment is conducted by the Commission taking into account the legal and institutional AML/CFT framework of the third country, the powers and procedures of the third country's competent authorities for the purposes of combating ML and TF and the effectiveness of the AML/CFT system in addressing ML or TF risks of the third country. Countries not included in the list should not be automatically considered to have effective AML/CFT systems and natural persons or legal entities established in such countries should be assessed on a risk-sensitive basis. Reliance on third parties established in such high-risk third countries is prohibited.

Enhanced CDD measures need not be invoked automatically with respect to branches or majority-owned subsidiaries of obliged entities established in the EU which are located in high-risk third countries, where those branches or majority-owned subsidiaries fully comply with the group-wide policies and procedures.

Obliged entities are also required to examine, as far as reasonably possible, the background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. In particular, obliged entities shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious. To this end, the following high-risk factors should be taken into account: (i) customer risk factors such as the business relationship is conducted in unusual circumstances, customers that are resident in higher risk areas, legal persons or arrangements that are personal asset-holding vehicles, companies that have nominee shareholders or shares in bearer form, businesses that are cash intensive, and the ownership structure of the company appears unusual or excessively complex given the nature of the company's business; (ii) product, service, transaction, or delivery channel risk factors such as private banking, products, or transactions that might favour anonymity, non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures, payment received from unknown or unassociated third parties, 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; and (iii) geographical risk factors such as countries identified by credible sources as not having effective AML/CFT systems, countries identified by credible sources as having significant levels of corruption or other criminal activity, countries subject to sanctions, embargos, or similar measures issued by, for example, the EU or the United Nations (UN), countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

Another important area of EDD concerns relationships with individuals who hold or who have held important public functions, within the Union or internationally, and particularly individuals from countries where corruption is widespread, the so-called politically exposed persons (PEPs). Such relationships may expose the financial sector in particular to significant reputational and legal risks. The international effort to combat corruption also justifies the need to pay particular attention to such persons and to apply appropriate enhanced CDD measures with respect to persons who are or who have been entrusted with prominent public functions domestically or abroad and with respect to senior figures in international organisations.

It is important to note that the Fourth Directive goes beyond FATF requirements as it abolishes the distinction between "foreign" and "domestic" PEPs, and results in automatic enhanced due diligence measures to be required in the case of any PEP, regardless of where they originate from.

However, the requirements relating to PEPs are of a preventive and not criminal nature, and should not be interpreted as stigmatising PEPs as being involved in criminal activity. Refusing a business relationship with a person simply on the basis of the determination that he or she is a PEP is contrary to the letter and spirit of this Directive and of the revised FATF Recommendations.

According to the FATF Recommendations, examples of enhanced CDD measures that could be applied for higher risk business relationships include obtaining additional information on the customer (e.g., occupation, volume of assets, information available through public databases, internet), and updating more regularly the identification data of customer and beneficial owner; obtaining additional information on the intended nature of the business relationship or on the reasons for intended or performed transactions, on the source of funds or source of wealth of the customer; obtaining the approval of senior management to commence or continue the business relationship; conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination; and requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

2.7 To Risk or Not to Risk?

In the aftermath of the recent financial crisis, many financial intermediaries conducted a review of their business activities in order to assess their profitability against the increasing costs imposed by new regulatory requirements. These costs refer to the implementation of more stringent regulations as well as the changes in the prudential regulations and capital requirements, including the Basel III international regulatory framework for banks, the European Union Payment Services Directive, and so on. Costs also include the increased AML/CFT compliance costs for higher risks customers and products (e.g., compliance staff costs, enhanced ongoing monitoring, review of existing records to keep CDD information up to date). As a result of these factors and the pressure on financial institutions to increase profitability and cut costs, intermediaries might choose to withdraw primarily from high-risk, low-return customers.

In addition, the fines levied in recent years in enforcement actions have increased significantly across countries. Significant fines were applied for serious and often systemic and wilful failings by banks to comply not only with AML/CFT rules and controls but also with the sanction regimes as required at the national level or by the EU or the UN Security Council Resolutions. Overall, major and highly publicised enforcement actions, including significant penalties, do harm the image and reputation of even the largest international banks—factors which contribute to the trend of banks taking a more conservative approach to risks.

All this leads to situations in which single or a small group of relationships are terminated by a financial institution to avoid, rather than manage, risk in line with the RBA (so-called de-risking). In other words, financial institutions deny or restrict entire classes of customers from access to financial services without taking into account, seriously and comprehensively, their level of risk or risk mitigation measures for individual customers within a particular sector.

This issue is of concern because of the potentially negative impact on legitimate business, as well as the danger of pushing certain business and customers into unregulated or less regulated channels thereby reducing financial sector transparency, raising financial crime risk eroding the integrity of the international financial system, and impeding the effective implementation of AML/CFT measures.

In October 2014, FATF issued a public statement with the objective of clarifying the appropriate scope of implementation of the RBA in AML/CFT area.[12] The document states that "de-risking" should never be an excuse for a bank to avoid implementing an RBA, in line with the FATF standards. According to FATF, its *Recommendations* only require financial institutions to terminate customer relationships, on a case-by-case basis, where the ML and TF risks cannot be mitigated. What would not be in line with the FATF standards is the wholesale cutting loose of entire classes of customer, without taking into account, seriously and comprehensively, their level of risk or risk mitigation measures for individual customers within a particular sector.

Indeed, however, when properly applying the RBA, terminating the business relationship is, in fact, the right decision to make if the customer ML/TF risks cannot be effectively mitigated (e.g., circumstances involving factors such as reluctant or uncooperative customers, firms operating in high-risk environments such as in countries subject to international sanctions, companies with weak internal controls, etc.).

As a consequence, obliged entities should adopt a balanced view, basing their business strategy on an accurate risk assessment.

2.8 Limitations to the RBA

The RBA cannot lead to failure to comply with the obligations that law or regulations clearly and expressly establish for addressees, without leaving them any room to assess the actual situation. This is the case when obligations impose the freezing of assets or funds belonging to individuals or entities entered in official lists of terrorists, including those issued in accordance with the resolutions of the UN Security Council to CTF and the activity of the countries that threaten peace and international security. It follows that it will not be possible to enter into or continue business relations with persons included in such lists, except within the limits and at the conditions expressly laid down.

The same applies in the case of embargoes against specific third jurisdictions. In the EU, these restrictive measures are used to pursue objectives in accordance with the principles of the Common Foreign and Security Policy and they are often imposed pursuant to Resolutions adopted by the

UN Security Council under Chapter VII of the UN Charter. The EU may however decide to apply autonomous measures in addition to the UN's measures or to adopt restrictive measures autonomously.[13] Such sanctions could namely include bans on the provision of specific services (brokering, financial services, technical assistance) and restrictions on investments, payments, and capital movements.

2.9 Concluding Remarks

The Fourth Directive is a major turning point for the AML/CFT strategy of the EU. It provides the Union, the Member States, and obliged entities with state-of-the-art tools to effectively combat ML and TF. At the same time, it poses new challenges since it will require an intense involvement of public authorities and private sector in devising new AML/CFT policies and methodologies.[14]

In this framework, the RBA is crucial to the effective implementation of the Fourth Directive since the entire structure of AML/CFT requirements is built leveraging on risk-sensitive policies. When assessing ML/TF risk, countries, competent authorities, and financial institutions should analyse and seek to understand how the ML/TF risks they identify affect them; the risk assessment therefore provides the basis for a flexible and proactive application of AML/CFT measures. This will also help manage the changing nature of ML/TF techniques.

Indeed, the RBA is not a "zero failure" approach; there may be occasions where an institution has taken all reasonable measures to identify and mitigate AML/CFT risks, but it is still used for ML or TF purposes. At the other side of the spectrum, there is also a danger of over-reporting by obliged entities that try to avoid running the risk of being fined for not promptly detect suspicious transactions.[15]

However, the main objective of the Directive could be successfully reached if it prevents obliged entities from applying AML/CFT requirements unthinkingly, as a checklist of steps to be taken. On the contrary, obliged entities should encourage their staff to "think risk" as they carry out their duties within the legal and regulatory framework governing AML/CTF.

To a large extent, the successful implementation of the Fourth Directive also depends on the enhanced collaboration between public authorities and private sector. The exchange of relevant information and the publication of the national/supranational risk assessments will be necessary to allow obliged entities to calibrate their policies and procedures. In this respect, the Fourth Directive lays the foundation for a more collaborative path that will more effectively engage all involved actors to deliver a consistent solution for the sake of the whole system's integrity.

Notes

1. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering and 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, 5.6.2015, p. 73.
2. OJ L309, 25.11.2005, p. 15.
3. As correctly pointed out, "the evolution of money laundering techniques has made their detection more complicated, precisely because they have made the separation and concealment of the three components of the laundering transaction increasingly effective," Dalla Pellegrina L., Masciandaro D., *The Risk-Based Approach in the New European Anti-Money Laundering Legislation: A Law and Economics View*, in Review of Law and Economics, 2009, 941.
4. S. Ross and M. Hannan, *Money laundering regulation and risk-based decision making*, in Journal of Money Laundering Control, Vol. 10, n. 1, 2007, 107–108.
5. FINANCIAL ACTION TASK FORCE, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations* (2012), Paris.
6. BCBS, *Sound management of risks related to money laundering and financing of terrorism* (2014), Basel.
7. P. Costanzo, *The risk-based approach to anti-money laundering and counter-terrorist financing in international and EU standards: what it is, what it entails* in B. Unger and D. van der Linde (eds.), *Research Handbook on Money Laundering*, Edward Elgar, 2013, 352–356.
8. B.M. Hutter, *The attractions of risk-based regulation: accounting for the emergence of risk ideas in regulation*, Discussion Paper 33, London School of Economics and Political Science, Economic & Social Research Council Centre for Analysis of Risk and Regulation, London, 2005.
9. For some scholars, compared to the rule-based approach, this new judgemental element implies some challenges as it entails the "privatization and marketization" of regulatory requirements with a possible impact on legal certainty and democratic accountability. See M. Bergström, K. Svedberg

Helgesson and U. Mörth, *A New Role for For-Profit Actors? The Case of Anti-Money Laundering and Risk Management*, in Journal of Common Market Studies, Vol. 49, n. 5, 2011, 1045–1047.

10. According to the Directive (article 3, para. 1, point 6), to uncover the existence of a beneficial owner, obliged entities should consider the natural person(s) who ultimately owns or controls a legal entity through direct (e.g., 25 % plus one share) or indirect ownership of a sufficient percentage of the shares or voting rights, including through bearer shareholdings, or through control via other means. If no person is identified following these criteria, then the beneficial owner may be the natural person(s) who hold the position of senior managing official(s). Similar criteria are also listed for other legal entities and arrangements, such as foundations and legal trusts.
11. Member States may increase the maximum amount to EUR 500 for payment instruments that can only be used in their territory.
12. See the following link http://www.fatf-gafi.org/topics/fatfrecommendations/documents/rba-and-de-risking.html
13. For a list of third countries under embargo by the EU please refer to website of the European External Action Service (EEAS).
14. See the interesting analysis of E. Tsingou, *Money Laundering*, in D. Mügge (ed.), *Europe and the Governance of Global Finance*, Oxford University Press, 2014, 153–154.
15. See B. Unger and F. van Waarden, *How to dodge drowning in data? Rule- and risk-based anti-money laundering policies compared*, in B. Unger and D. van der Linde (eds.), *Research Handbook on Money Laundering*, cit., 405.

CHAPTER 3

Beneficial Ownership and Effective Transparency

Roberto Formisani

Abstract This chapter deals with the regulation of beneficial ownership assessment, as part of the new "customer due diligence" (CDD) duties. After discussing the relevance of such provisions in the anti-money laundering (AML) modern regulations, the chapter focuses on the repealed Third Directive and then to the legislation in force, together with a short presentation of the main issues for the national implementation.

3.1 Reasons Behind a New AML Directive

It is nowadays quite clear that an effective legal regime, set up to avert money laundering and the financing of terrorism, is a crucial part of the regulation of the financial system. In other words, it is common sense that hindering such criminal phenomenon cannot rely only on criminal sanctions upon the "launderettes", but also requires the provision of organizational and administrative measures upon financial intermediaries, professionals, and public bodies: from a policy standpoint, fighting money laundering and the financing of terrorism calls for the enactment of ex ante, and not only, ex post measures.[1] This new approach, as a consequence of the ever growing awareness of the harms to the real economy and to the smooth functioning of the financial system,[2] in time lead to a constant development of new tools and instruments by legislators and regulators, both at the European[3] and national levels. Moreover, the increasing importance in anti-money laundering (AML) regulation in the

D. Siclari (ed.), *The New Anti-Money Laundering Law*,
DOI 10.1007/978-3-319-29099-7_3

broader context of domestic and international financial regulation is also due to the globalization of financial markets and the setup of the European Monetary Union (EMU): in fact, repealing the control mechanisms over international capital flows actually lead to a material increase in the ways that "dirty money" could be laundered, as a consequence of the greater freedom of capital movement and of the new opportunities for their use as a result. Even the rise of Information and Communication Technologies (ICTs), as a means that can provide new opportunities for money laundering, cannot be underestimated.[4]

In order to counteract this, since 1991 the European Union enacted a series of Directive set up to create a highly harmonized AML framework. In particular, it is widely known that a major change in the AML regulatory approach occurred by the signature into law of the Directive 2005/60/CE of the Parliament and of the Council, in October 2005 (so-called Third Directive).[5] It is well renowned, in fact, the introduction of the so-called *risk-based approach* in the fulfillment of the "customer due diligence" (CDD)[6] duties (Art. 8 par. 2 Directive), under which the financial intermediaries and other individual subject to the application of the Directive (auditors, lawyers, public notaries, etc.), may vary the compliance of such duties according to the "AML risk" posed by specific categories of customers, business activities, or financial products. Therefore, under the current framework, the risk assessment takes place at an earlier stage than the previous one, since it occurs at the moment of customer identification and not when the suspect transaction is reported to the national competent Financial Intelligence Unit (FIU).[7]

After almost ten years, the European legislator took action to revise AML regulation. The main drivers were, on the one hand, the necessity to implement the amendments to the Financial Action Task Force (FATF) Recommendations[8] and, on the other, to strengthen the clarity of the provisions and to reinforce the consistency and uniformity in the enforcement by national bodies and subject covered by the Directive.[9] In particular, with regard to the first aspect, the revised version the FATF Recommendations consists of several novelties: among others, the main ones are the strengthening of the risk-based approach (Recc. Nos. 1, 26) so as to let the States use more flexibility in the resource allocation according to the different kinds of risk;[10] a broader definition of "Political exposed persons" (Recc. Nos. 12, 22) that now encompasses national, and not only foreign, politically exposed persons (PEPs), and stronger forms of cooperation between national authorities (Recc. Nos. 38, 40), with specific regard to seizure and confiscation of the proceeds of such crimes.

3.2 The Need to Identify Beneficial Owners of the Transactions as an Indispensable Tool in AML Regulation

A main overhaul of the Recommendations concerns the "beneficial ownership" issue (Recc. Nos. 24, 25). Before discussing in depth the reasons behind the reform, it is extremely important to understand *what* is the beneficial ownership and *why* it is key to an effective AML regulation. Under the earlier version of FATF Recommendations (issued in 2003), "beneficial owners" have been identified as "natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted [and] those persons who exercise ultimate effective control over a legal person or arrangemen*t*".[11] In other words, AML regulation calls on the covered subjects to figure out who is the owner of the actual interest behind legal formalities, with specific regard to the agents exploited by its principal. It is quite obvious, therefore, how much this information is crucial in the AML context: typically, the capability of tracing the beneficial owner of the transaction is key to overcoming both the "layering" and the "placement" stage of the laundering activities, bearing in mind that corporate vehicles and legal arrangements (such as trust, *fiducie*, *fidecoimiso*) are employed especially in these phases of such a process.[12] The Recommendations outlines the two interests at stake: on the one hand, the "ownership" concerns the natural persons that actually take advantage or profit of the assets of the legal persons (without taking into account, consequently, criteria set out by legislation to determine legal ownership of such entities), while "control" concerns the identification of who is, in practice, exerting effective management powers over the entity (without having regard for legal entitlements to such rights).[13]

That is extremely relevant as far as corporate entities are considered, given that in these cases there are plenty of methods by which the ultimate owner can "layer" his or her interests in transactions, due mainly to the fact that the corporate entity is, from a legal standpoint, a separate person from the actual beneficiary of the scheme. This feature, common to several kinds of juridical entities, is not a danger in itself, for money laundering policing purposes. To the extent that the legal and regulatory regimes are so well designed that the persons that ultimately own or control the entities can be easily detected by the subject covered by AML regulation (while performing CDD or similar duties prescribed by other non-European legislations) or by the competent national authorities,[14] the possible dissociation between legal and beneficial ownership and control is not a matter of concern. In particular, as observed in many policy papers adopted by international AML standard-setters, the main point to be addressed is providing adequate sources of information, so as to avoid any possibility of anonymity.[15] Apart from that, it is undeniable that some peculiar schemes may pose a significant laundering risk, insofar as they are capable of hampering the beneficial owner detection capability. In this regard, according to the international standard-setters, the structuring of complex multi-jurisdictional corporate entities and relations may be highly capable of concealing beneficial owners, especially when such schemes are able to use loopholes at a national level for their illicit purposes. Moreover, even at a merely domestic level, some corporate law provisions—such as the possibility of issue bearer shares, the unlimited use of legal persons as directors or the allowance of "nominee" shareholders and directors—may lead to a level of secrecy challenging to overcome.[16] Another instrument that can be easily employed in criminal activities is the use of "shelf companies", that is, corporate entities that neither perform any business nor own any assets and, consequently, are used as a vehicle for other persons' business operations.[17] This last issue calls attentions to the role exerted by people involved, as consultants on a professional basis, in the establishment and management of corporations (company service providers, CSPs) and the need to regulate their role (with possible options ranging from imposing a license to requiring specific AML responsibilities).[18]

At the same time, we have seen that the FATF Recommendations address not only corporate entities but also a wide array of legal agreements under which someone places certain assets under the management of another person for his/her or someone else's benefit or for the achievement of a specific goal.[19] The broad category of "legal arrangements" is modeled on the common law figure of trust, but can be easily applied to other civil law instruments that share the same rationale: a transfer of power and control over assets on fiduciary basis, so as to satisfy a transferor's need. Here again, what is a matter of interest for AML regulation is the possibility to understand the ultimate controller of the scheme (the "director") or the person on whose behalf the transaction takes place (the "owner").

Under FATF Recc. No. 5 (2003 edition), States were required to impose on financial intermediaries to identify the beneficial owner of the transaction, and "[to take] reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is", taking care in particular of understanding, in case, the ownership and control structures of legal entities.

The identification of the beneficial owner was, in other words, part of the broader CDD obligation, and a particular emphasis was placed on figuring out the ownership and control structures of the business operation. Recommendation 33 and 34 called on countries to assure that the access to beneficial ownership information by competent authorities could happen on an "adequate, accurate and timely" basis. In particular, as far as corporate entities are concerned, Countries were requested to adopt all the necessary measures to avoid the use of bearer shares for illicit purposes, while—with respect to legal arrangements—the main point of interest is the accessibility "in a timely fashion" of express trusts,[20] and in particular, information about parties involved (settlor, trustee, and beneficiaries).

The repealed European legislation (the already mentioned Directive 2005/60/CE) was fully adherent to the FATF Recommendations. In particular, the implementation of the FATF soft law gives the European legislator the opportunity to introduce a precise definition of beneficial ownership, in order to strengthen the CDD provisions:[21] in this regard, Art. 3 par. 6 states that "natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted" shall be deemed to be a beneficial owner of a corporate or, more generally, a legal entity. In particular, with reference to the first case, such notion shall comprise, at least, "natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity"[22] or "natural person(s) who otherwise exercises control over the management of a legal entity". With regard to the other legal entities and arrangements that distribute or administrate funds, the "legal minimum" is set to be above 25% of the property of the arrangements, whether as beneficiary or as person exerting control over it.[23] Again, in the latter case, it is noteworthy that, even if the "legal arrangements" notion embodied in the FATF Recommendations concerns mainly fiduciary relationships, Recital 13 clearly states that the fiduciary nature of trust relationships employed as commercial products in wholesale financial markets does not impose automatically an obligation to verify the beneficial owner's identity: such recital wants to emphasize that in peculiar cases, especially since the business environment is already heavily regulated, AML regulation does not require automatisms that may in some respect harm the freedom of business activities and, in the other respect, may cause prejudice to the risk-sensitivity of the regulatory regime. Just in case, it should be up to the financial intermediary or to the other professionals covered by the Directive to assess whether there are elements or circumstances that may require a deeper understanding of ownership and control structures of the trust relationship.

With reference to trusts, there are some other aspects that need to be pointed out. Firstly, the threshold set out in the Directive refers to capital, and not profit interests in the trust.[24] Secondly, discovering who, among the various parties involved in a trust scheme, can qualify as the beneficial owner is largely dependent upon the single trust under scrutiny. The first lesson to be drawn is that the beneficiary is not always the trust's beneficial owner, given that in case of a discretionary trust (i.e., trusts under which the settlor stipulates in the trust deed a class of beneficiaries, leaving to the trustees' discretion the selection of the recipients of the trust income or property—among the aforesaid class[25]) before any decision by the party entitled to select the beneficiary, the former shall qualify as the controlling party and therefore as beneficial owner. Moreover, the European rules attribute, to a certain degree, relevance whether the stipulated rights are vested or not: in fact, if the beneficiary's rights are conditional or effective only for a certain time frame—just like in the case of potential beneficiaries in discretionary trusts[26]—he or she cannot qualify as beneficial owner, while if the rights of a class of beneficiaries are so structured, the entire class shall be deemed to be the beneficial owners of the trust under CDD.[27]

It is noteworthy that the repealed Directive took a slightly different approach from the FATF Recommendations: while the latter are focused on a "substance-over-form" approach, asking States to require subjects covered to check on the economic substance of the transaction, the Directive's definition took a "middle ground" approach, when integrating FATF stance with formal requirements (a certain percentage of "legal" ownership, as seen above).[28]

Subjects covered by the Directive (financial intermediaries and persons performing the professions enlisted in Art. 1 par. 2 lett. c) were required to identify, "where applicable", beneficial owners, adopting "adequate and risk-based measures" so as to attain a reasonable guarantee of such identification ("the institution or person covered by this Directive is satisfied that it knows who the beneficial owner is"), taking into account particularly the "ownership and control structure of the customer" (Art. 8 par. 1 (b)). The provision states, as noted above, that such identification should occur only if necessary: some Authors argued, in this regard, that the norm at stake may be read as rebuttable "presumption of coincidence" of the customer and the beneficial owner.[29] In other words, if there are no elements that raise doubts on the actual interests behind the legal ownership of the scheme—through the medium enlisted in the Directive or the relevant implementing acts, there is no need to further "investigate" on possible beneficial owners.[30]

Without binding effect, Recitals 10 of the Directive offers, anyway, some guidance on how to perform beneficial ownership assessment, naming "use of public records of beneficial owners, ask their clients for relevant data or obtain the information otherwise": by this way, the Directive's intention was not to limit professional judgment by the subject covered (as it would have happened, in case of enactment of a binding provision), and in that way limiting the effectiveness of a risk-based AML regulation:[31] in fact, in some national implementing legislation the possibility to make use of such data from public registers and the like are expressly stated (see, for instance, in Italian legislation: see Art. 18 par. 1 (b) of the Legislative Decree 231/2007[32]). Since, as noted above, AML regulation does not impose a "duty to investigate", it seems reasonable that obliged entities may perform their due diligence obligations by checking what was conveyed by customers and data in public registers. If all the circumstances gathered are not satisfactory to the covered subject's professional judgment, the next step is not moving forward with verifications, but reporting to the national FIU.[33]

Even if this was not imposed by the Directive, some national implementing legislation (such as, the Italian one) imposed specific duties on customers to convey all the information necessary for CCD purposes and, expressly, "necessary and up-to-date" knowledge to identify the beneficial owner: in both cases, under criminal sanctions for failure to comply.[34] As seen above, this is one of the main sources of information, especially as far as beneficial ownership is concerned. This tool can prove to be particularly effective if such national implementing measures can be interpreted—as in a recent Italian case[35]—to oblige beneficial owners themselves to disclose their status to controlled entities in their business relationship with obliged entities.[36]

As part of the CDD, the "on-going monitoring" of the transaction undertaken during the customer-subject covered business relationship[37] could have been extremely useful in ascertaining beneficial ownership in a dynamic approach, especially while allowing the persons or institutions covered to gather, in case, some other information and, as a result, verify the veracity of the identification performed at the beginning of the business relation. Together with all the remaining data collected by means of the CDD assessments, persons, and institutions covered by the Directive were required to keep records of beneficial owners' information, under Art. 30 Directive.

3.3 Main Reforms Enacted by the Fourth Directive

After the enactment of the Third AML Directive, the Commission started a review of this legal document, driven mainly by two factors: the issuing of a new, updated edition of the FATF Recommendations in 2012 and the fulfillment of the comprehensive assessment on the Directive implementation requested under Art. 42 and 43.[38] As far as the first point is concerned, in the 2012 version the FATF introduced two new recommendations addressing specifically the beneficial ownership issue: under Recc. Nos. 24 and 25, Countries are required to enact all the necessary measures so as to "ensure that there is adequate, accurate and timely information on the beneficial ownership" of legal persons and arrangements, timely accessible by competent authorities and, at the same time, adopting "measures to facilitate access to beneficial ownership and control information" by subjects covered by AML regulation. While there is no modification in the beneficial owner definition embodied in the Glossary, the Interpretative Notes to the Recommendations follow an innovative "progressive" approach[39] in sketching the beneficial owner identification process, as part of the CDD duties. In fact, according to the Interpretative Notes to Recc. No. 10, covered subjects should, firstly, assess whether there is one or more natural persons holding, in case of legal persons, "a controlling ownership interest" or, with regard to legal arrangements, all the relevant people involved (trustees, settlors, beneficiaries, etc. in non-trust schemes). If it is not possible to find the controlling natural person (from an ownership standpoint), checks shall be focused on "natural persons (if any) exercising control of the legal person or arrangement through other means". As a last resort, identification efforts will concern the "senior managing officer" of the legal person.

With reference to the European legislation, the beneficial ownership has been one of the main points of interest. Apart from the proper quantification of the ownership threshold—as seen above, an issue specifically addressed by the Directive—the April 2012 Commission Report to the European Parliament and Council[40] lists two other subject matters: first of all, a coherent implementation and application by covered subjects of the "otherwise exercising control over the corporate entity" clause in Art. 3 of the Directive and, secondly, the opportunity to enact provisions aimed at gathering beneficial ownership information so as to make it publicly available, for the benefit of public authorities and covered subjects.[41]

The discussion on ownership threshold was mainly focused on the opportunity of lowering the percentage from 25 to 20 %.[42]

In the end, coming to the Directive in force, two main changes concerning the beneficial ownership regime occurred. First of all, while basically maintaining the "traditional" definition of the beneficial owner laid down in the previous Directive (together with the categories that shall "at least" qualify as beneficial owner), the 25 % shareholding percentage is now "evidence" and no longer a criterion to be met to qualify as the beneficial owner. In other words, such a threshold is an element to be taken into account together with any other one that may come up, and not a fact per se leading to this outcome: as seen above, in order to effectively and comprehensively assess the economic substance of the transactions under scrutiny, AML regulation tends to avoid "automatisms" in presumptions, leaving room for the careful evaluation of covered subjects. Besides, it is noteworthy that this new provision seems to get the EU legislation close to the FATF "substance-over-form" approach, in comparison to the Third Directive. In particular, while the holding by a natural person of more than 25 % of the shares—calculated in accordance with the relevant provisions of the Directive 2013/34/EU on annual and consolidated financial statements—is "evidence of direct ownership", an "indication of indirect ownership" arises when a shareholding of more than 25 % in the customer under due diligence is held "by a corporate entity, which is under the control of a natural persons, or by multiple corporate entities, which are under the control of the same natural person".[43] Moreover, Art. 3 of the Directive implements the aforementioned "progressive approach" laid down in FATF Recommendations: in fact, if there are doubts that the controlling person (from the ownership standpoint) is the beneficial owner—or such identification is not feasible at all—covered subjects should look for people who exercise "control over management [...] through other means". In case no natural person is identified, "senior managing official" shall qualify as the "minimum" beneficial owner (in the aforementioned meaning).[44] Besides, with regard to trust, it is now expressly stated that settlors, trustees, beneficiaries, and protectors (in case) shall qualify as "minimum" beneficial owners.

The major overhaul in the beneficial ownership regulation concerns, anyway, the insertion of a new rule providing for a "duty of centralization" of information regarding legal persons "incorporated within their territory". More specifically, under Article 30 par. a, Member States are required to impose to any legal persons the obligation to transmit to a "central register" such information; leaving therefore the possibility, for Member States, to decide whether to create an ad hoc register or to exploit the one already in force. It is noteworthy, in particular, that many changes occurred during the legislative procedure to the location criterion of trusts' competent business registers: while Art. 31 par. 1 makes reference to the obligation of the trustees "of any express trust governed under [Member States'] law" to "obtain and hold information on beneficial ownership regarding the trust"—therefore dealing with trustees' AML duties[45]—the central register in charge of receiving such data is the one set up by the Member States "when the trust generates tax consequences" (Art. 31 par. 4). Despite the opposition of some Member States[46] and the criticisms on the ground of the vagueness of the expression and the possibility to leave room for abuse and circumvention by individuals,[47] the Directive endorsed in this regard the proposal laid down by the Council.

In particular, the information therein embodied—that will probably encompass the typical corporate information available in business register—shall be "adequate, accurate and current". Moreover, specific disclosure requirements are imposed with regard to trusts and to legal arrangements having similar structure or function (Art. 31 par. 8): trustees shall convey the identity "(a) of the settlor,(b) the trustee(s), (c) the protector (if relevant), (d) the beneficiaries or class of beneficiaries, (e) any other natural person exercising effective control over the trust" (Art. 31 par. 1). Furthermore, Member States are asked to impose to trustees to "disclose their status in a timely manner to obliged entities (…) when, as a trustee, the trustee forms a business relationship or carries out an occasional transaction above the threshold set out in points (b), (c) and (d) of Article 11 (i.e., when obliged entities are required to perform CDD)".[48] In cases of legal entities, the central business register will also be the recipient of beneficial owners' data. Just like the other duties imposed by the Directive, Member States are asked to provide "effective, proportionate and dissuasive" both for failure to disclose data required under the (future) implementing national legislation and to avoid any possible abuse (having regard, in particular, to bearer shares).[49] Aiming at easing the cooperation between competent authorities and more generally the circulation of data in the EU—and, as a result, to improve the capability to detect flows of illicit funds—an amendment was introduced to impose the interconnection of the registers by means of a "European platform". This would have lead to the enhancement of the possibility to access such data (that have to be published "in an open and secure format") even at a cross-border level, taking a step forward from the current initiatives, such as the "European Business Register", the network established among the national business registers in the EU, but this rule has not been adopted in the final version of the Directive. The Directive stresses the need of coherence with the European privacy regulations:[50] this is particularly relevant with regard to trusts, given that deeds and letters of wishes may pose greater risks for individuals' privacy than corporate data: in fact, Art. 30 par. 5 states that "access to the information on beneficial ownership shall be in accordance with data protection rules", setting forth a provision applicable to trusts and similar legal schemes. Anyway, apart from supervisory authorities and obliged entities, the access to the register is limited to "persons or organisations that can demonstrate a legitimate interest". Even if the norm at stake does not provide for a full coordination with EU privacy regulation, the "legitimate interest" requirement seems to strike a proper balance between the register's accessibility (especially as far as trusts are concerned) and a proper and effective personal data protection.

Even if, compared to the repealed regulatory regime, there is a massive increase in the magnitude of information available both to competent authorities and to an obliged subject, this circumstance does not result in the distribution of evaluation duties for the latter. More specifically, financial intermediaries and the other professionals cannot "take for granted" the profiling included in the central business register, particularly when beneficial ownership is at stake (given that this is one of the subjects that requires the most the professional evaluative judgment), but they have to use that as evidence for their assessment. In fact, Art. 30 par. 8 (with regard to legal entities) and 31 par. 6 (trusts and similar legal schemes) clearly states that "Member States shall require that obliged entities do not rely exclusively on the central register (…) to fulfill their customer due diligence requirements (…). Those requirements shall be fulfilled by using a risk-based approach".

3.4 Conclusion

It is quite clear, after this short presentation, that the Fourth Directive is strongly focused, as far as beneficial ownership is concerned, on increasing the information set for all the subjects involved. This can be viewed as a shift in the regulatory approach to the issue at stake: the policymakers seem, now, more concerned with providing obliged entities with the largest possible evidence in this matter—giving therefore much more room for the exercise of professional judgment of the latter ones—than focusing on the issues related to the beneficial owner's definition and to the imposition of specific steps in the identification process. Moreover, the already quoted elasticity in the notion at stake, due to the capability to detect beneficial interests behind legal formalities, may lead to a "cross-fertilization" of AML regulation with other branches of law: a clear example is provided by the Italian legal system, where the beneficial owners—as defined in the Legislative Decree implementing the Third AML Directive—are now expressly covered by the tax reporting obligations concerning capital transfer outside Italy.[51]

A major role in the new regulatory framework, at domestic level, will be played by the "central registers" under Art. 30 and 31, and by the organizations that will be in charge of them. It is very likely that, in order to lower the burden of the implementing measures and in the light of the kind of data demanded by the same provision, such roles will be entrusted with the "ordinary" business registers already established under domestic corporate and business law. Therefore, even if indirectly, the holder of the public bodies of such registers are going to "join" the subject covered by AML regulation. Their role, of course, will be quite different from the "traditional" obliged entities: such bodies, in fact, are not going to be subject to the usual "trio" of AML duties (CDD, reporting, and record keeping), but they will be required to (broadly speaking) facilitate the fulfillment of such obligation by the "real" obliged entities. A matter of interest is understanding whether or not such cooperation—sticking to the well-established AML lexicon—will be "active": that is, whether such public bodies will have to assess the veracity of the beneficial ownership information flow, or they will merely collect and register such information without any check on such profiles:[52] this is extremely relevant because in many jurisdictions, public bodies entrusted with registers and the like are able to check only on formal aspects of the documents registered, without having the power to challenge the actual substance of the transaction thereof.[53] This will, in other words, result in major overhaul of the way business registers are kept in many Member States. Moreover, if the first course of action preferred by domestic legislators seems reasonable, as some Author point out, it will be necessary to leave to people registered as beneficial owner the possibility to challenge such identification, subject to the disclosure of what kind of links have been found between that person(s) and the scheme or the entity by the holder of the register:[54] probably, this conclusion can be hardly drawn from the existing legal system, and will require a specific provision on the occasion of the enactment of the national implementing measures.

Lastly, the Fourth Directive implementation will result in major changes for non-trust countries.[55] The new obligations provided under the new Directive will result in the compulsory registration of the information on trusts, laid down in the Directive, in the aforesaid "central register". It will be apt to Member States, in drafting implementing measures, to decide what kind of legal effects such registration will produce. Firstly, it will be extremely important whether trusts information will be conveyed to a specific register or to the business registers, in the light of the already mentioned freedom left to Member States. In case the domestic lawmaker decided to create a "special" register only for AML purposes—but this will create a material duplication, in compliance costs, for corporate entities—there would be no doubt that such registration will serve only informational purposes, in order to facilitate CDD duties performance: of course, domestic legislators could also create a register only for trust—like in some non-EU civil law jurisdictions,[56] but this possibility does not seem feasible in the light of the Directive's provisions, that seem to require a *single* register.

The second (and the most likely) option, as seen above, is to reform the ordinary business registers and, as a result, to convey trust information. In the latter case, it will be up to domestic lawmakers to coordinate such registration with the "ordinary" legal effect of such filing. In fact, in many jurisdictions (such as the Italian one) the "ordinary" filing into the business register may produce a wide array of legal effects. For example, in the Italian legal system, such effects are contingent on the type of business entities listed in the business registers. For instance, for corporate entities the registration is required in order to grant them legal personality: therefore, the filing itself is essential for the attribution of a peculiar legal status.[57] Instead, with regard to activities that under the law have to be registered (such as, just to quote a few of them, the nomination or the conclusion of the directors' term), the filing produces a "weaker" legal effect: the registration does not affect the validity of the deeds, but by means of a knowledge presumption makes it effective to third parties, impeding them to hold although they were not aware of it.[58] In the end, the Italian legal system requires some other filings only for record-keeping reasons, without legal relevance (e.g., in the case of the registration of individual entrepreneurs, not farmers[59]).

Given the foregoing, it is quite clear that the legal consequences of trust registration is still uncertain, in absence of national implementing measures of the Directive. Certainly, trust registration will serve the already mentioned AML informational purposes—since this aim is, practically, the only one pursued by the European legislation, but determining whether to take this opportunity to introduce specific trust regulation is left to Member States. In any case, as pointed out by certain Authors, the implementation of the Directive could be a chance to implement the duty, already established under Art. 36 of the Third Directive, to impose a registration or the licensing of CSPs;[60] an obligation that some Member States (e.g., Italy) have not complied with yet.[61]

Notes

1. This evolution is well rendered by looking at the approach followed by the relevant international treaties: the earlier conventions, in fact, dealt with the issue at stake focusing only on criminal aspects (like, for instance, the Vienna Convention of 1988), while the last ones tend to regulate also measures preventing the exploitation of the financial system for money laundering (e.g., see the Palermo Convention of 2000). As far as other regulatory tools are concerned, preventive measures are especially dealt with "soft law" issued by international organizations (most notably, Financial Action Task Force (FATF) Forty Recommendations and, from an historical point of view, the Basel Committee Declaration "Prevention of criminal use of the banking system for money laundering purposes" of 1988).
2. It is also important to notice that AML tools are an extremely valuable measure to fight organized crime, in particular bearing in mind the importance of "attacking" the wealth and the sources of revenue of such organizations. At the same time, AML tools (especially, limitations on cash payments) may be extremely valuable in fighting tax evasion.
3. The EU lawmaking competence is based upon Art. 114 of the Lisbon Treaty (Treaty on the Functioning of the European Union), under which the Union is entitled to adopt "the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market".
4. See Razzante, *La regolamentazione antiriciclaggio in Italia*, Turin, 2011, pp. 10–15.
5. Published in the Official Journal of the European Union, 25 November 2005, No. 309.

6. The CDD is in itself a significant evolution of the mere customer identification duties embodied in the Second AML Directive (2001/97/CE), given that it lasts through all the business relationship (and therefore does not concern only its establishment) and, moreover, increases the pieces of information to be collected. See Unità di Informazione Finanziaria, *Relazione annuale per l'anno 2008*, p. 23.
7. Fisicaro, *Antiriciclaggio e terza direttiva Ue*, Milan, 2008, p. 59.
8. The new Recommendations have been adopted on 16 February 2012.
9. Starola, *La proposta di IV direttiva antiriciclaggio: novità e conferme*, *Corriere Tributario*, 2013, pp. 1212–1213.
10. See, in particular, FATF, *Guidance for a risk-based approach: the banking sector*, 2013.
11. See the Glossary annexed to the Recommendations.
12. After analyzing the most typical money laundering techniques, many Authors found out some common features in the way they are performed: firstly, the "placement" of illegal funds into the financial system; secondly the already quoted "layering" and, lastly, the gain of the proceeds generated by the use the laundered funds ("integration"). See Levi-Reuter, *Money laundering*, London, 2011, p. 311. The role played by corporate entities and trusts (together with similar arrangements) is remarked by fatf, *The Misuse of Corporate Vehicles, including Trust and Company Service Providers*, 2006.
13. Fatf, *Guidance on Transparency and Beneficial Ownership*, 2014, p. 8.
14. It is widely known that modern AML regulations are based on the performance, by subject covered, of "active cooperation" duties: this means, in other words, that together with the fulfillment of "passive" provisions (such as customer identification and bookkeeping) subjects covered by AML regulation are required to assess and "supervise" business relationships they are entering into, so as to understand any risk of use by felons of the financial system and therefore being able to report any suspect to competent authorities. See Razzante, *La regolamentazione antiriciclaggio in Italia*, cit., p. 70 ss. (the Author stresses that the active cooperation cannot be interpreted as a "duty to investigate", but merely that to grasp the economic rational of the transaction and, if need be, cooperate by reporting suspected infringements).
15. See, again, FATF, The Misuse of Corporate Vehicles, p. 11.
16. See oecd, *Behind the Corporate Veil—Using Corporate Entities for Illicit Purposes*, 2001, pp. 29–33.
17. This definition is taken from Black's Law Dictionary, 8th edition, St. Paul (MN), 2004, p. 368.

18. See OECD, Money Laundering using Trusts and Company Service Providers, 2010.
19. FATF, The Misuse of Corporate Vehicles, cit., p. 23.
20. Under trust law, the express trust are the ones created by the express intention of the settlor, as opposed to the implied trusts (see, HUDSON, *Equity and Trusts*, Abingdon, 2015, pp. 85 ss. and 497 ss., respectively).
21. See Recital No. 9.
22. Under the same provision, a percentage above 25 % plus one share was sufficient to meet such requirement.
23. In case the individuals are yet to be determined, "the class of persons in whose main interest the legal arrangement or entity is set up or operates" shall qualify as beneficial owners.
24. It is clearly spelled out in some national implementing regulations, such as the Technical Annex to the Italian Legislative Decree No. 231/2007 (Art. 2 par. (b)) and the Money Laundering Regulation issued by the FSA in 2007 (par. 6.3).
25. See RAMJOHN, *Text cases and materials on equity and trusts*, Abingdon, 2008, pp. 91 ss.
26. Since that, in both cases, such persons are entitled to a "proper" legal right, but merely to a *spes*.
27. VICARI, *Dal beneficiario del trust al suo titolare effettivo: percorsi nella Disciplina Antiriciclaggio del trust*, in *Trusts e Attività Fiduciarie*, 2009, pp. 614 ss.
28. FISICARO, *Antiriciclaggio e terza direttiva Ue*, cit., p. 61.
29. See ORLANDO, *Su alcune inefficienze della disciplina antiriciclaggio. Analisi e prospettive*, *Riv. Notariato*, 2009, p. 90.
30. In this regard, a mere declaration in writing provided by the customer, certifying such coincidence, cannot per se exhaust the duty to check any possible split on the ownership of the entity or the scheme (as suggested by ORLANDO, *Su alcune inefficienze*, cit., p. 90). Such a declaration can be, at most, one of the circumstances to be taken into account, together with all the others of the case at stake.
31. In fact, even national implementing legislations were aware of this point, and followed the same approach: for example, the Italian Legislative Decree No. 231/2007 states that, in performing CDD, subjects covered "may recourse to public registers, documents, (…), publicly available" (translation by the Author).
32. This rule is upheld by the CCD Regulation issued by the Bank of Italy on 3 April 2013: see p. 16. A list of documents that may be exploited, according to the Bank of Italy, can be found at p. 17.
33. In this regard, see LICINI, *La* "persona fisica titolare effettivo in ultima istanza" *nel D. Lgs. 231/2007 attuativo della III direttiva antiriciclaggio*, in *Notariato*, 2008, pp. 184 ss.

34. See Legislative Decree No. 231/2007, Art. 21 and 55 par. 1 (as for sanctions). According to some Authors, some issue may arise with reference to a proper distinction between the customers' and the institutions and persons covered liability. In particular, given that the identification takes place—under Italian law—by means of a "non expired" ID document, some doubts may come to mind in case of counterfeit documents, and especially with regard to the institutions and persons' level of care in assessing such veracity. See Ruggiero, *La nuova disciplina dell'antiriciclaggio dopo il D. Lgs. 21 novembre 2007, n. 231*, Turin, 2008, p. 102.
35. Milan *Tribunale* (civil court of first instance), 17 July 2013, in *Società*, 2014, 1089 ss. (with a brief comment by Capolino-Perlingieri-Cavallo, pp. 1097 ss.).
36. It is important to notice, anyway, that this outcome may depend upon other general clauses or specific rules of the legal system at stake: for instance, in the aforesaid case decided by the Milan *Tribunale*, such Court took advantage, in interpreting the Italian provision laid down in Art. 21 Legislative Decree No. 231/2007), of both the general clause of good faith in contract law (embodied in Art. 1375 Civil Code) and of Art. 2497 Civil Code, which holds the controlling entity liable for the damage caused to controlled ones by executing its directives.
37. In accordance with Art. 8 par. 1 (d) Directive, the on-going monitoring is aimed at "ensur[ing] that the transactions being conducted are consistent with the institution's or person's knowledge of the customer, the business and risk profile".
38. While Art. 42 called for a general assessment, Art. 43 was specifically focused on threshold percentages in the beneficial owner identification process.
39. starola, *La proposta di IV direttiva antiriciclaggio*, cit., p. 1215.
40. The Report's main elements are based on the evidence collected by Deloitte in a paper drafted for the benefit of the Commission's Services: *Final Study on the Application of the Anti-Money Laundering Directive*, 2009.
41. See European Commission, *Report on the application of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*, 2012, pp. 8–10.
42. With regard to this specific point, the comments received by Deloitte argued against such lowering, quoting in particular a material increase in compliance costs, as a likely outcome.
43. Art. 3 concedes to Member States the right to impose lower percentages, but still only as "indication of ownership and control".
44. With the aim of easing access to material information by competent authorities, the provision at stake imposes to covered subjects to "keep records of the actions taken in order to identify the beneficial ownership […] in order to prove the inability to identify such persons".

45. As a result, the national applicable legislation will be determined by the choice of law made under the trust deed.
46. See the declaration issued by the Austrian government, available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205748%202015%20ADD%202
47. Longhi, *IV direttiva antiriciclaggio e trasparenza dei trust: cominciamo bene*, IPSOA Quotidiano, 10.2.2015.
48. Art. 31 par. 2.
49. See Recital 59.
50. See the "Data protection Directive" of the Parliament and the Council (95/46/CE).
51. On this topic, with a specific focus on trusts' beneficial owners see Mione, *Le recenti modifiche alla disciplina del c.d. monitoraggio fiscale: la problematica individuazione del "*titolare effettivo*" del trust*, *Diritto e Pratica Tributaria*, 2014, p. 601 ss.
52. Such bodies are requested, anyway, to supervise the adherence to formal requirements (e.g., the completeness of the data requested by the regulatory framework).
53. See, for instance, the Italian legislation regulating the *Registro delle imprese* (business register): under Art. 2189 par. 2 Civil Code "before the registration, the Register Office shall verify the veracity of signatures and the meeting of all the requirements provided under the law" (Author translation). Such theory is the most followed in the Italian legal literature, especially as far as documents already verified by public notaries are concerned: see M. Campobasso, *Diritto commerciale*, Vol. 1—Diritto dell'impresa, Turin, 2008, pp. 117–118.
54. Longhi, *IV direttiva antiriciclaggio: identificazione anche per i trust?*, IPSOA Quotidiano, 13.1.2015, p. 3.
55. Such term designates countries where trusts are not regulated under private law. Italy, for instance, recognizes trusts only for fiscal purposes, as subject liable to corporate income tax (see Art. 73 par. 1 (b) Consolidated Income Taxes Code) and is party to the *Convention on the Law applicable to Trusts and on their recognition*, done at Hague in 1985. Such international treaty, as widely known, does not concern substantial trust law—that is, providing from uniform rules in this regard—but it is focused on setting specific features that may allow even non-trust countries to recognize such arrangements (see Gambaro, *Trust*, in *Digesto delle Discipline Privatistiche*, Vol. 20, Turin, 1999, pp. 449 ss.).
56. See the San Marino Republic Trust Register, held by the San Marino Central Bank. It should be remarked that San Marino, since the enactment of the Law No. 37/2005 and the consequent regulation of such legal scheme, has become a "trust country", despite its civil law tradition.

57. Art. 2331 Italian Civil Code.
58. See Art. 2193 par. 2 Italian Civil Code and Art. 7 par. 2 Law 29 December 1993, No. 580.
59. See Art. 8 par. 5, Law 29 December 1993, No. 580.
60. For a brief discussion of the role exerted by these professionals, see above Par. 2.
61. Longhi, *IV direttiva antiriciclaggio: identificazione anche per i trust?*, cit., p. 1.

CHAPTER 4

Anti-Money Laundering EU Law and Network of Agents

Domenico Siclari

Abstract In the new regulatory framework introduced by Directive (EU) 2015/849, we have the problem of supervision of payment institutions (PIs) that operate across borders by agents. In fact, most Member States result host some agents operating on a European passport under the Directive 2007/64/EC (the so-called Payment Services Directive or PSD), in the context of the creation of a Single Payments Area in Europe (so-called SEPA); a large number of Member States act as the home regulator for cross-border PIs.

4.1 The AML Supervision of Payment Institutions that Operate Across Borders by Agents

The European Union (EU) Fourth anti-money laundering Directive (AMLD) is now putting in place a framework which focuses on greater effectiveness and improved transparency in order to make it harder for criminals to abuse the financial system. Significant progress has been achieved on the review package the EU Third AMLD,[1] which, as known, consists of two legal instruments: the new Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and a Regulation on information accompanying transfers of funds to secure "due traceability" of these transfers. These two legal instruments take into account the 2012 Recommendations of the Financial Action Task Force (FATF), and go further to promote the

D. Siclari (ed.), *The New Anti-Money Laundering Law*,
DOI 10.1007/978-3-319-29099-7_4

highest standards for anti-money laundering (AML) and counter terrorism financing (CFT).

The new regulatory framework welcomes the risk-based approach:[2] it acknowledges that the levels and types of action required to be taken by Member States, supervisors, and firms will differ according to the nature and severity of risks in particular jurisdictions and sectors, clarifying the types of situations in which simplified customer due diligence will be appropriate, as well as those situations where it is necessary for firms to conduct enhanced checks.

We have new rules concerning the extended definition of politically exposed persons—PEPs (here is clarified that enhanced due diligence will always be appropriate where transactions involve politically exposed persons), inclusion of tax crimes as predicate offences, national and Europe-wide risk assessments, reinforcement of sanctioning powers and requirements to co-ordinate cross-border action, lower exemptions for one-off transactions and expansion of the perimeter, new requirements on beneficial ownership information, to increase transparency by requiring companies and trusts to hold information on their beneficial ownership, and to make this information available to supervisors and parties conducting due diligence on them.

In this new regulatory framework, we have the problem of supervision of payment institutions (PIs) that operate across borders by agents.[3] In fact, most Member States result host some agents operating on a European passport under the Directive 2007/64/EC (the so-called Payment Services Directive or PSD),[4] in the context of the creation of a Single Payments Area in Europe (so-called SEPA);[5] a large number of Member States act as the home regulator for cross-border PIs.

Risks associated with the Money Transfer sector, especially operating through agents, are considered very high.[6]

For example, in Italy, money laundering and financing terrorism risks associated with the Money Transfer sector are considered very high, due also to the size of the Italian money remittance market: amongst the EU countries, the Italian market is the second biggest one in terms of money remittance flows directed abroad (EUR 7.39 mld in the 2011). In 2011, the market share of the money remitters based in another EU country operating in Italy through very extensive networks of agents was equal to 55 %. In this framework, various criminal investigations found out that the money transfer networks are misused for money laundering purposes or for terrorist financing purposes by criminal organisations.

In Portugal, Payment System (PS) agents, whenever they are not financial institutions, are considered as presenting an inherent ML/FT high risk. This is the case due to their absence of control mechanisms in terms of the prevention of AML/CFT on the overwhelming number of agents operating in these conditions (gas stations, subway stations, supermarkets).

According to FATF's new Recommendation 14 on money or value transfer services providers, money or value transfer services (MVTS) providers should be required to be licensed or registered. MVTS providers should be subject to monitoring for AML/CFT compliance. Agents for MVTS providers should be required to be licensed or registered by a competent authority, or the MVTS provider should be required to maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate. According to para. 14.5, MVTS providers that use agents should be required to include them in their AML/CFT programmes and monitor them for compliance with these programmes.

Agents pursuing their activities on the basis of PSD rule, regarding the exercise of the right of establishment and freedom to provide services. According to this rule, any authorised PI wishing to provide payment services for the first time in a Member State other than its home Member State, in exercise of the right of establishment or the freedom to provide services, shall so inform the competent authorities in its home Member State. Within one month of receiving that information, the competent authorities of the home Member State shall inform the competent authorities of the host Member State the name and address of the PI, the names of those responsible for the management of the branch, its organisational structure, and the kind of payment services it intends to provide in the territory of the host Member State. In order to carry out the controls in respect of the agent, branch, or entity to which activities are outsourced of a payment institution located in the territory of another Member State, the competent authorities of the home Member State shall cooperate with the competent authorities of the host Member State. The competent authorities of the home Member State shall notify the competent authorities of the host Member State whenever they intend to carry out an on-site inspection in the territory of the latter. However, if they so wish, the competent authorities of the home Member State may delegate to the competent authorities of the host Member State the task of carrying out on-site inspections of the institution concerned. The competent authorities shall provide each other with all essential and/or relevant information, in particular in the case of infringements or suspected infringements by an agent, a branch, or an entity to which activities are outsourced. In this regard, the competent authorities shall communicate, upon request, all relevant information and, on their own initiative, all essential information.

4.2 The Requirement of Central Contact Points in Some European National Legislations

In EU Member States, there have been reported some cases of countries where the requirement of a central contact point (CCP) has been set up by their national legislation.

In Italy, the reference to CCPs has been included in Article 42 of the Legislative Decree 231/2007 (Italian AML law) after its amendment by the Legislative Decree 164/2012.[7] According to para. 3, the suspicious transaction report (STR) shall be submitted to the Financial Intelligence Unit (FIU) by the agents of the PIs directly or through the CCP created in Italy by the EU electronic money institution (EMI) or PI. The creation of the contact point is mandatory in case of plurality of agents.

PIs' agents operating in Italy are subject to the Italian AML regulations, so they are obliged to comply also with the Italian customer due diligence and record keeping requirements. At the moment, the Italian law provides a role for the CCP only in relation with the STRs. But, in their understanding, PIs are very likely to assign to the CCP also coordination and supervisory role with regard to the other pieces of the AML obligations applicable to the agents operating in Italy.

In Belgium, Belgian AML law applies to PIs/ EMIs "providing payment services in Belgium through a person established there and representing the institution to this end". PIs/EMIs with such an establishment in Belgium are subject to all the provisions of the Belgian AML law, including article 18 which provides that the obliged entities "shall assign responsibility for the implementation of this Law to one or more persons within their institution or profession. These persons shall primarily be responsible for implementing the policies and procedures referred to in Articles 16 and 17, as well as for examining the written reports drawn up in accordance with Article 14, § 2, second subparagraph, in order that appropriate action may be taken, where necessary, in accordance with Articles 23 to 28. […] In the cases referred to in Article 2, § 1, 4ter, c) and 4quater, e) [i.e. in the case of PIs /EMIs providing payment services in Belgium through a person established there and representing the institution to this end] a person responsible for the implementation of this Law should be established in Belgium." This person responsible for the implementation by the EEA PIs/EMIs of the Belgian AML law is the Belgian CCP, even if the Belgian Legislation does not make use of that expression. Belgian AML law applies to all PIs/EMIs providing payment services in Belgium "through a person established there and representing the institution to this end". The wording "through a person established there and representing the institution to this end" is meant to capture any form of establishment in Belgium (other than branches, already mentioned in another subparagraph), provided the establishment has the power to represent the PI/EMI.

Functions of the CCP result from Article 18 of the Belgian AML law. The main functions of an officer responsible for preventing money laundering and the financing of terrorism—and hence of a Belgian CCP—consist in: examining the written reports relating to atypical transactions which are communicated to it and drawn up in accordance with Article 14, § 2, second subparagraph of the Law; deciding if such atypical transactions are suspicious and in filing, if this is the case, an STR to the Belgian FIU (CTIF-CFI) in accordance with Articles 23 to 28 of the Law; implementing the policies and procedures referred to in Articles 16 and 17. This includes the implementation of the internal measures and control procedures set out by the PI/EME in order to ensure compliance with Belgian AML law, the implementation of the group AML policy and the implementation of the measures taken by the EME/PI to train their representatives in terms of AML obligations.

In Spain, according to the Spanish legislation, if an EU payment/e--money institution designates more than one agent in Spain for the provision of payment services, the agents would constitute a network of agents. In accordance with Articles 4.2 and 10.4 of Royal Decree 712/2010, Banco de Espana shall hold a register of persons responsible for the network of agents, and its establishment will be subject to the same procedure established in regard to branches of EU PIs. That means it is necessary for the PIs/EMIs to designate and communicate to Banco de Espana both a person in charge of the agents' network and contact address in Spain. The provisions above are included in the template of communication that Bank of Spain sends to the PI, once it has received notice from the Home Supervisor.

The legislation does not explicitly mention a "central contact point", but since the agents' network are considered similar to a branch, a CCP is therefore a mandatory requirement. Furthermore, according to the regulation, agents of foreign PI must, in the exercise of their activity in Spain, observe the same rules of law that the agents of any Spanish PI must observe.

In Portugal, the draft rule through which the Portuguese Supervisory Authority intend to implement the requirement of the CCP for PIs is an Aviso do Banco de Portugal. A preliminary version was published in March 2013. In a more up-to-date version of the Article 7 of the draft Aviso do Banco de Portugal, which regulates the agents of foreign PIs or e-money institutions, according to its third paragraph, in order to facilitate the exercise of AML/CFT supervision and improve compliance with the related regulation, EU PI or e-money institutions must promote the creation in Portugal of a CCP, whenever they operate in Portugal through one or more agent or third party with operational functions.

The appointment must be done before providing such activities in Portugal through one or more agent/third party with operational functions. This CCP must also be ensured by a natural or legal person who has a physical structure permanently adequate to meet the functions and who must be any of the financial institutions identified in Article 3 (among them, credit institutions or PIs, including branches of foreign ones) or act as an agent on a local or foreign PI or EMI.

4.3 The New Fourth AMLD and PSD 2 Rules

In this context, now we are facing the new Fourth AML EU Directive and PSD 2 rules. About the relationship between home and host supervisory authorities, the new Fourth AML Directive provides clear provisions on AML supervision where cross-border cases are concerned, whereas the Third AML EU Directive did not explicitly cover.

The host country's supervisory authority has jurisdiction over the branches and agents located in its own territory for AML supervision; these branches must comply with local money laundering legislation.

The host country can now demand that the PI or the e-money institution, operating multiple branches or agents in its own territory, designate a CCP, responsible for ensuring that the institution complies with AML and terrorist financing laws. This CCP must provide any documents or data upon request of the competent supervision authority or any other support.

According to Recital (50) of the new Fourth AML Directive, where Member States require issuers of electronic money and payment service providers which are established in their territory in forms other than a branch and the head office of which is situated in another Member State, to appoint a CCP in their territory, they should be able to require that such a CCP, acting on behalf of the appointing institution, ensure the establishments' compliance with AML/CFT rules. They should also ensure that that requirement is proportionate and does not go beyond what is necessary to achieve the aim of compliance with AML/CFT rules, including by facilitating the respective supervision.

According to Recital (38b) of the new Fourth AML Directive, where an obliged entity operates establishments in another Member State, including through a network of agents, the competent authority of the home Member State should be responsible for supervising the obliged entity's application of group-wide AML/CFT policies and procedures. This could involve on-site visits in establishments based in another Member State. The competent authority of the home Member State should cooperate closely with the competent authority of the host Member State and should inform the latter of any issues that could affect their assessment of the establishment's compliance with the host AML/CFT rules.

According to Article 45, para. 9, of the new Fourth AML Directive, Member States may require electronic money issuers as defined in point (3) of Article 2 of Directive 2009/110/EC and payment service providers as defined in point (9) of Article 4 of Directive 2007/64/EC established on their territory in forms other than a branch, and whose head office is situated in another Member State, to appoint a CCP in their territory to ensure, on behalf of the appointing institution, compliance with AML/CFT rules and to facilitate supervision by competent authorities, including by providing competent authorities with documents and information on request.

According to Article 45, para. 10, of the new Fourth AML Directive, the European Supervisory Authorities (ESAs) shall develop draft regulatory technical standards on the criteria for determining the circumstances when the appointment of a CCP pursuant to paragraph 9 is appropriate, and what the functions of the CCPs should be. The ESAs shall submit the draft regulatory technical standards to the Commission by 26 June 2017. According to Article 45, para. 11, power is delegated to the Commission to adopt the regulatory technical standards referred to in paragraph 9 in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010.

According to Article 48, para. 4, of the new Fourth AML Directive Member States shall ensure that competent authorities of the Member State in which the obliged entity operates establishments supervise that these establishments respect the national provisions of that Member State pertaining to this Directive. In the case of the establishments referred to in

Article 45(9), such supervision may include the taking of appropriate and proportionate measures to address serious failings that require immediate remedies. These measures shall be temporary and be terminated when the failings identified are addressed, including, with the assistance of or in cooperation with the home country's competent authorities.

According to Article 48, para. 5, of the new Fourth AML Directive, Member States shall ensure that the competent authorities of the Member State in which the obliged entity operates establishments shall cooperate with the competent authorities of the Member State in which the obliged entity has its head office, to ensure effective supervision.

Also according new PDS 2, Member States may decide to require that PIs operating on their territory under the right of establishment, and whose head office is situated in another Member State, appoint a CCP in their territory, in order to facilitate the supervision of networks of agents. The EBA will develop draft regulatory standards setting out the criteria to determine when the appointment of a CCP is appropriate and what its functions should be.

In this sense, Article 26a, para. 5, 6, and 7, of new PSD 2, regarding supervision of PIs exercising the right of establishment and freedom to provide services, Member States may require PIs operating on their territory through agents under the right of establishment, and whose head office is situated in another Member State, to appoint a CCP in their territory to ensure adequate communication and information reporting on compliance with new rules, without prejudice to any AML provisions and to facilitate supervision by home and host competent authorities, including by providing competent authorities with documents and information on request. EBA shall develop draft regulatory technical standards setting out criteria for determining the circumstances when the appointment of a CCP is appropriate, and what the functions of CCPs should be. EBA shall submit these draft regulatory technical standards to the Commission within one year of the date of entry into force of this Directive.[8] Power is delegated to the Commission to adopt the regulatory technical standards referred to in paragraph 6 in accordance with the procedure laid down in Articles 10 to 14 of Regulation (EU) No 1093/2010.

Then, the set-up of such a contact point can be requested for the purpose of ensuring compliance with the money laundering and antiterrorist financing rules under AML EU Directive,[9] while the Member States option under PSD2 can only be invoked for the purpose of adequate communication and information by the PI on compliance with the rules under PSD2.

4.4 Some Problems Arising from the Application of the New Rules in EU Member States

From this new system of rules derive various problems related to the supervision of the money services agents.

Now a first issue concerns how and whether PSD 2 could be implemented in some uniform way so as to allow Home Supervisors to delegate AML/CFT inspections of PS agents work to Host Supervisors. A second, but not secondary, issue concerns which jurisdiction's (home or host) AML/CFT law should apply when such delegated inspections took place.

When will enter a regime the opportunity to request payment service providers as defined by Directive 2007/64/EC established on their territory in forms other than a branch, and whose head office is situated in another Member State, to appoint a CCP in their territory to ensure on behalf of the appointing institution compliance with AML/CFT rules and to facilitate supervision by competent authorities, we will run the serious risk of an asymmetric supervision of agents. It seems at least they should be co-ordinates the activities of the CCP, imposed for the two different purposes that we have explained above.

Paradoxically, the application, as well appropriate, of the principle of proportionality[10] could lead—as unintended consequence—to expectations of national "administrative" regimes any different.[11] To avoid this practice, the ruling task assigned to the EBA will be crucial.[12]

In my opinion, we would need—just to avoid reduced competition between the laws of the Member States in the implementation of the new EU Directives—as fast as possible harmonisation of procedures for the supervision of PIs operating by agents.

In the European Banking Union and the EU single financial market,[13] a common approach to the regulation of cross-border PS agents within Europe at present, to counter the risk of violation domestic law and distortion of competition within a local market because of uncontrolled AML/CFT measures by using a huge network of agents, appears at this point no longer be postponed.

We need a "standardised" and uniform approach, so as to consider the justified interests of the PS industry to get predictable regulatory conditions, also to get to the configuration of a common European legal framework among EU Member States, that is, the "Europeanisation" of the fight against crime and money laundering within the area of freedom, security, and justice.[14]

Notes

1. About the EU Third AMLD see, among others, M. Pellegrini (2005), "Anti-Money Laundering Legislation in the light of the Proposal of the Third EC Directive" *European Business Law Review*, Vol. 5, p. 1181; E. Katz (2007), "Implementation of the Third Money Laundering Directive. An Overview" *Law and Financial Markets Review*, Vol. 1, No. 3; V. Mitsillegas and B. Gilmore (2007), "The EU Legislative Framework against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards" *International and Comparative Law Quarterly*, Vol. 56 (1), p. 119; S. Buisman (2011), "The Influence of the European Legislator on the National Criminal Law of Member States: It is All in the Combination Chosen", *Utrecht Law Review*, Vol. 7, No. 3; S. Costa (2013), *Implementing the New Anti-Money Laundering Directive in Europe: Legal and Enforcement Issues—The Italian Case* (Milan: Paolo Baffi Center on International Markets, Money and Regulation) No. 2008-13; E. Herlin-Karnell (2014), "Constructing Europe's Area of Freedom, Security and Justice Through the Framework of 'Regulation': A Cascade of Market Based Challenges in the EU's Fight Against Financial Crime" *German Law Journal*, p. 49.
2. See A. Proctor (2005), "Supporting a risk-based anti-money laundering approach through enforcement action" *Journal of Financial Regulation and Compliance*, Vol. 13, No. 1, p. 10; S. Ross and M. Hannan (2007), "Money Laundering Regulation and risk-based decision making" *Journal of Money Laundering Control*, Vol. 10, No. 1, p. 106.
3. See, in this respect, ESA's Joint Committee Sub-Committee on Anti Money Laundering, Supervisory Cooperation Protocol between "Home Supervisor" and "Host Supervisor(s) of Agents and Branches of Payment Institutions in Host Member State", July 2012; Joint Committee of the European Banking Authority (EBA), European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA), Report on the application of AML/CTF obligations to, and the AML/CTF supervision of e-money issuers, agents and distributors in Europe, December 2012.
4. See Kokert, J. and Held, M. (2014) "Payment Services Directive II: Risks and serious consequences for users and banks", BaFin section for IT infrastructure of banks, June 2014; Valcke, Peggy and Vandezande, Niels and Van de Velde, Nathan, The Evolution of Third Party Payment Providers and Cryptocurrencies Under the EU's Upcoming PSD2 and AMLD4 (23 September 2015). SWIFT Institute Working Paper No. 2015-001.
5. See A. Janczuk-Gorywoda (2010) "The Single Payments Area in Europe" *Columbia Journal of European Law*, Vol. 16, No. 2, 321.
6. About illegal cash brought to an alternative remittance provider for the placement outside of the banking system (e.g., "money-transfers" agents), G. Ardizzi, C. Petraglia, M. Piacenza, F. Schneider and G. Turati (2013), *Money Laundering as a Financial Sector Crime—A New Approach to*

Measurement, with an Application to Italy CESifo Working Paper Series No. 4127, p. 6, observe that "since bank money is essential to transform capital into profitable investments in the global formal economy, it is reasonable to assume that a relevant share of illegal funds placed outside the banking system will be subsequently deposited in cash on a bank account".

7. About Italian AML law see P. Fratangelo, Prevention and Countering of Money Laundering and Terrorism Financing, in D. Siclari (ed.), Italian Banking and Financial Law. I. Supervisory Authorities and Supervision, Palgrave Macmillan, 2015, p. 105; I. Borrello, Financial Intelligence Unit (FIU), in D. Siclari (ed.), Italian Banking and Financial Law. I. Supervisory Authorities and Supervision, Palgrave Macmillan, 2015, p. 261.
8. Those draft regulatory technical standards shall, in particular, take account of: (a) the total volume and value of transactions carried out by the payment institution in host Member States; (b) the type of payment services provided; and (c) the total number of agents established in the host Member State.
9. For example, in Italy the legislative decree implementing EU AML Directive (European Delegation Law 2015) requires now, as a criterion for the exercise of legislative delegation, the obligation to establish a CCP (art. 14, para. 2, letter. C, no. 3), giving the Bank of Italy to adopt an enforcement regime.
10. About the principle of proportionality see recently the proceedings of the EBA Workshop "The application of the principle of proportionality in the context of Institutional and Regulatory Reforms", London, 3 July 2015.
11. For example, in Belgium by Circular of the National Bank No. 11 of 22 October 2014, the Bank introduced an obligation for financial institutions established in Belgium to annually fill in an electronic questionnaire on AML/CFT. Payment institutions and EMIs, including branches and central contact points in Belgium of payment institutions and EMIs authorised in other Member States of the European Economic Area, fall within the scope of this Circular and must therefore normally complete the full questionnaire annually. However, in accordance with the principle of proportionality, the Bank has decided to ease its requirements regarding the periodic information which must be provided on the arrangements put in place by the institutions to meet the legal obligations regarding AML/CFT, taking into account the specific characteristics or the scale of the establishment in Belgium of the payment institution or EMI concerned. Are therefore exempted from the obligation to complete the full questionnaire attached to Circular NBB_2014_11 of 22 October 2014: PIs and EMIs governed by Belgian law which, by virtue of Articles 48 or 105 of the Law of 21 December 2009, are exempted from application of the provisions of this law; "Central contact points" in Belgium of European payment institutions which have established in Belgium a network of fewer than 100 agents or distributors, and which have executed in Belgium over the past year, through their agent network, less than 100,000 payment transactions on behalf of their clients; "Central contact points" in Belgium

of European EMIs, which have established in Belgium a network of fewer than 100 agents or distributors, and which have distributed, over the past year and through their network of distributors in Belgium, electronic money amounting to less than EUR 5,000,000, and which have executed, through their agent network in Belgium, less than 100,000 payment transactions on behalf of their clients (see Banque Nationale de Belgique, Circular No. 12, Brussels, 22 October 2014).

12. See S. Cappiello (2015), *The Interplay between the EBA and the Banking Union*, Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS 2015/77.
13. See, in this regard, Moloney S (2014) "European Banking Union: Assessing its risks and resilience" *Common Market Law Review*, 51, 1609 ss.; E. Ferran (2014) *European Banking Union and the EU Single Financial Market: More Differentiated Integration, or Disintegration?*, University of Cambridge Faculty of Law Research Paper nr. 24; C. Brescia Morra (2014) *From the Single Supervisory Mechanism to the Banking Union*, Working Paper LUISS Guido Carli.
14. About the "Europeanisation" of the fight against crime and the role of the EU in fighting crime within the area of freedom, security and justice, the impact of EU policies in the Member States, the progressive convergence of Member States' criminal law systems, the emergence of mutual recognition as an alternative to harmonisation, and the incremental development of the ECJ's jurisdiction see C. Eckes and T. Konstadinides (eds.), *Crime within the Area of Freedom, Security and Justice. A European Public Order*, Cambridge University Press, 2011.

CHAPTER 5

Risk Assessment

Pierluigi Tonnara

Abstract This essay focuses on risk assessment, a new strategy of risk-based regulation provided by the Fourth Directive on anti-money laundering (AML)/counter terrorism financing (CFT). This strategy is structured on three levels: the supranational/ European Union (EU) level, the national level, and the obliged entities' level. These levels are linked to and fed by each other in a dynamic way, even though a supremacy role is attributed, to some extent, to the European Commission.

5.1 Introduction

The European Union (EU) and the Member States need to identify, understand, manage, and mitigate the risks of money laundering and terrorist financing they face.

Risks are variable in nature and the combination of several variables makes risks increasing or decreasing. In other terms, certain situations present a greater risk of money laundering and terrorist financing, while others might have a less significant impact. It is, therefore, necessary for EU and Member States to underpin a risk-based approach (RBA). Indeed, each measure needs to be assessed also according to a cost-effective approach, since overreaction may waste resources and lead to a lower performance of the whole regulatory framework.[1]

In this regard, the full and clear knowledge by EU and Member States is necessary to allow them adopting appropriate and proportionate measures to face the risks and avoiding an overreaction. Indeed, economies

D. Siclari (ed.), *The New Anti-Money Laundering Law*,
DOI 10.1007/978-3-319-29099-7_5

and crimes change their features so quickly that all institutions struggle to stay ahead. Thus, the need for updated, precise, and accurate information should be at the top of regulators' list.

The Fourth Directive on money laundering and terrorist financing tries to do so also by entailing a new strategy: the risk assessment. Such strategy should embrace the supranational level (Article 6), the national level (Article 7), and the obliged entities' level (Article 8). These levels are linked to and fed by each other in a dynamic way, even though a supremacy role is attributed, to some extent, to the European Commission.

5.2 The Reasons for an RBA

Risk-based regulation has been becoming more and more widespread across the world and in different areas such as environment, food, legal service, and finance.[2] Risk-based regulation is a set of strategies in the hand of regulators to target public resources at those sites and activities that present threats to regulators' ability to achieve their objectives.[3] By embracing such approach, regulators would tend to focus on the highest risks and they would be encouraged to pull back resources from lower risks. This tendency, however, is not always followed strictly, since lower risks may have some capacity to produce both significant harms and political contention, and consequently regulators may be demanded to face lower risks too.[4]

With specific regard to anti-money laundering (AML), after the Financial Action Task Force (FATF) issued its Revised Forty Recommendation in 2003, concepts of risk assessment and risk management became two key elements in the definition of the AML regulation.[5]

In this regard, last FAFT's Recommendations re-points out that countries should apply an RBA to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. The use of such approach should lead to an efficient allocation of resources across the AML and countering the financing of terrorism (CFT) regime.[6] More specifically, FAFT's Recommendations suggest that countries need to: (a) identify higher risks to adequately address them; and (b) allow simplified measures when addressing lower risks. Further, FAFT's Recommendations point out that countries should have: (a) national AML/CFT policies, informed by the risks identified to be periodically revised; and (b) a coordination mechanism for such policies. This coordination mechanism should concern also the supranational/international level, so that policies and activities to combat money laundering and terrorist financing become more effective.

Against the above background, risk assessment can be regarded as one new strategy of risk-based regulation. Indeed, risk assessment is functional to the use of evidence-based decision-making in order to target the risks of money laundering and terrorist financing. Risk assessment is, therefore, seen as a way to increase effectiveness of AML with the necessary degree of flexibility to allow adaptation to the different situations and actors. In this regard, the IV Directive structures the risk assessment on three levels: EU, national, and obliged entities. However, these levels should not be seen as separate monads, since the Fourth Directive provides for, inter alia, a circular flow of information: top-down (from the Commission to Member States and, finally, the obliged entities) and bottom-up (from the obliged entities to the Member States and, finally, to the Commission). Actually, only a circular flow of information may create a full and clear knowledge of the risk to be faced at and within the EU.

5.3 Risk Assessment at EU Level

The Fourth Directive acknowledges that the importance of a supranational approach to risk identification has been encouraged at international level. In this regard, the Directive indicates the Commission as the best placed authority to review cross-border threats that could affect the internal market and to coordinate the assessment of risks relating to cross-border activities. In order to do so, Member States are required to share the outcomes of their risk assessments with each other and with the EU Institutions, namely the Commission, the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA) (jointly referred as European Supervisory Authorities, ESAs).

The flow of information and the findings of the risk assessment at the EU level have to be gathered in a report by the Commission. Such a report is to be prepared by 26 June 2017 and it is to be updated at least every two years, since only updated information may constitute the basis for a real evidence-based decision-making.

More specifically, the said report must cover at least the following issues: (a) the areas of the internal market which are characterised by the highest risks, (b) the risks characterising each relevant sector, and (c) the most widespread means used by criminals to launder their illicit activities.

Moreover, with the aim to fruitfully use the flow of information and the different expertise, the Commission has to take into account: (a) the opinions issued by the ESAs (the Joint Committee has to issue its first opinion by 26 December 2016 and renovate it every two years), (b) the Member States' experts in the areas of AML/CFT, (c) representatives from Financial Intelligence Units (FIUs), and (d) other Union level bodies (where appropriate).

Moreover, the report is to be submitted to the European Parliament and to the Council every two years, or more frequently if appropriate, with the aim to clarify: both (a) the findings resulting from the regular risks assessments, and (b) the actions taken following these findings.

Finally, it seems that the Commission is not only entitled to coordinate risk assessments at and within EU but it is also entitled to "guide" Member States' risk assessment policies. Indeed, Member States are obliged to base their risk assessments on the Commission's findings. Moreover, the Commission is entitled to make recommendations to Member States with a comply-or-explain mechanism: if Member States decide not to apply any of the recommendations in their national AML/CFT regimes, they must notify the Commission and provide a justification for such a decision.

5.4 Risk Assessment at National Level

The Fourth Directive requires Member States to take all necessary steps to identify, assess, understand, and mitigate the risks of money laundering and terrorist financing.

More specifically, Member States are required to: (a) designate an authority or establish a coordinating mechanism to address money laundering and financing of terrorism risks (Member States have to notify their designated authority to the Commission, to the ESAs, and to the other Member States); and (b) carry out risk assessments periodically so to keep the relevant information updated.

As already pointed out, the Directive structures the different levels of risks assessments at and within EU as linked to and fed by each other with a guiding role of the Commission. Accordingly, Member States, in carrying out their risk assessments, must make use of the findings of the report by the Commission.

In carrying out the risk assessment, each Member State has to: (a) identify any areas where obliged entities are to apply enhanced measures and, where appropriate, specifying the measures to be taken; and (b) make appropriate information available promptly to obliged entities to facilitate the carrying out of their own money laundering and terrorist financing risk assessments.

According to the Directive, the scope of risk assessment at national level is to: (a) allocate and prioritise the resources to combat money laundering and terrorist financing; and (b) ensure that appropriate rules are drawn up for each sector or area, in accordance with the risks of money laundering and terrorist financing.

Finally, always with the aim to make information available to all institution involved in combating money laundering and the financing of terrorism, each Member State is required to share the findings of its risk assessment with the Commission, the ESAs, and the other Member States.

5.5 Risk Assessment at Obliged Entities' Level

The strategy on AML/CFT will be harmless, if entities involved in business relations are not called to play a significant role. This is why the Fourth Directive does not only calls such entities to carry out their own risk assessments to identify and assess the risks of money laundering and terrorist financing; the Fourth Directive also requires obliged entities to adopt proportionate measures (policies, controls, and procedures) to mitigate and manage effectively the risks of money laundering and terrorist financing at all levels, including EU and national levels. In other words, while Commission and Member States are mainly called to study the problems, obliged entities are called to study and to act accordingly.

For the sake of clarity, according to Article 2, obliged entities are: (a) credit institutions; (b) financial institutions; (c) auditors, external accountants, tax advisors, notaries, and other independent legal professionals, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning some particular activities;[7] (d) trust; (e) estate agents; (f) other persons trading in goods to the extent that payments are made or received in cash in an amount of EUR 10,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked; and (g) providers of gambling services.

In this regard, Member States have to ensure that obliged entities take the appropriate steps and, more specifically, that such steps are proportionate to the obliged entities' nature and size. For instance, a Member State may decide that individual documented risk assessments are not required where the specific risks of the sector are clear and understood.

Risk assessments by obliged entities have to take into account risk factors including those relating to their customers, countries or geographic areas, products, services, transactions, or delivery channels. For reasons already explained, obliged entities' risk assessments are to be kept updated and made promptly available to the competent authorities.

Based on the findings of risk assessments, obliged entities have to adopt their steps on AML/CFT. The Fourth Directive gives general indications on such steps. More specifically, obliged entities' policies are to aim for: (a) the development of internal policies, controls, and procedures, including model risk management practices, customer due diligence, reporting, record keeping, internal control, compliance management including, where appropriate with regard to the size and nature of the business, the appointment of a compliance officer at management level, and employee screening; and (b) where appropriate with regard to the size and nature of the business, an independent audit function to test the internal policies, controls, and procedures referred to in point (a).

Finally, the Fourth Directive boosts for an international cooperation amongst Member States on controls over obliged entities which operate establishments in another Member State. In this regard, it should be structured a double check on AML/CFT policies (i.e. sort of both "home Member State control" and "host Member State control"). More specifically, the home Member State should be: (a) responsible for supervising the obliged entity's application of group-wide AML/CFT policies and procedures, and (b) allowed carrying out inspections also in the establishments located in the host Member State. The host Member State should be: (a) responsible for enforcing the establishment's compliance with AML/CFT rules, (b) allowed carrying out inspections and offsite monitoring, and (c) entitled to appropriate and proportionate measures to address serious infringements of those requirements.

Finally, the competent authority of the home Member State should cooperate closely with the competent authority of the host Member State and should inform the latter of any issues that could affect their assessment of the establishment's compliance with the host AML/CFT rules.

5.6 Third Countries Jurisdictions

All efforts by EU Institutions, Member States, and obliged entities might be softened or even annulled by those third countries which have deficiencies in their national AML/CFT regimes. Actually, the changing nature of money laundering and terrorist financing threats, which is made easier by a continuous evolution of technology and of the means in criminals' hands, requires quickly adapting the legal framework as regards high-risk third countries. By doing so, important steps can be done to address efficiently existing risks and prevent new ones from arising.

In this regard, the Fourth Directive demands the Commission to identify the high-risk third countries to protect the proper functioning of the internal market. The Commission should take into account information from international organisations and standard setters in the field of AML/CFT, such as FATF public statements, mutual evaluation or detailed assessment reports or published follow-up reports, and adapt its assessments to the changes therein.

More specifically, high-risk countries will be identified on the basis of the following possible deficiencies: (a) legal and institutional AML/CFT framework, (b) powers and procedures in the hands of third countries' institution to combat money laundering and the financing of terrorism, and (c) the effectiveness of the AML/CFT in addressing the relevant risks.

After high-risk third countries are identified, the Commission is entitled, within one month, to adopt acts restricting the free movement of capital to or such third countries involving direct investment—including in real estate—establishment, the provision of financial services or the admission of securities to capital markets.

5.7 Relations with Data Protection and Statistics

Just a brief overview has to be given about the relations amongst risk assessments, data protection, and statistics.

In this regard, the Fourth Directive provides that personal data have to be processed only for the purposes of the prevention of money laundering and terrorist financing. Other purposes, such as commercial purposes, are prohibited. The processing of data for the purposes of AML/CFT is expressly classified as a matter of public interest under the meaning of the Directive on data protection (95/46/EC).

Moreover, as accurate statistics are crucial for a proper risk assessment, the IV Directive sets out some requirements to make statistics comprehensive. More specifically, statistics have to include:

(a) data measuring the size and importance of the different sectors which fall within the scope of the Directive, including the number of entities and persons and the economic importance of each sector;

(b) data measuring the reporting, investigation, and judicial phases of the national AML/CFT regime, including the number of suspicious transaction reports made to the FIU, the follow-up given to those reports and, on an annual basis, the number of cases investigated, the number of persons prosecuted, the number of persons convicted for money laundering or terrorist financing offences, the types of predicate offences, where such information is available, and the value in euro of property that has been frozen, seized, or confiscated;
(c) if available, data identifying the number and percentage of reports resulting in further investigation, together with the annual report to obliged entities detailing the usefulness and follow-up of the reports they presented;
(d) data regarding the number of cross-border requests for information that were made, received, refused, and partially or fully answered by the FIU.

5.8 Brief Conclusive Comments

The introduction of a new strategy of risk-based regulation, such as the risk assessments under the Fourth Directive, is to be welcomed.

The risk assessments strategy reminds to a well-known way to organise power and competencies within the EU. Indeed, such a strategy requires different institutions, some at EU level and others at national level, to exercise their competences to reach one single and unitary scope. In other terms, each involved institution or obliged entity is called to play its part in a single music score, what has been referred as "concerto regolamentare europeo" (European regulatory concert).[8] In another perspective, risk assessments strategy can be regarded as a set of "mixed administrative proceedings".[9] More specifically: (a) the circular flow of information amongst the institutions to prepare risk assessments reports; (b) the Commission's power to recommend Member States the adoption of measures according to a "comply-or-explain" mechanism; and (c) the policies to be adopted by the obliged entities following the activities carried out by the Commission and the Member States, seem to create "hybrid administrative proceedings".

In this regard, it can be stressed out that a guiding role in risk assessments strategy has been attributed to the Commission. However, works at EU level requires the continuous and real involvement of both Member States and obliged entities.

Moreover, a crucial role is to be played by obliged entities. Actually, only obliged entities are directly involved in business transactions: it should not, therefore, sound surprising that the Fourth Directive demands them to keep the findings of risks assessments and to convert such findings in sounding policies.

Finally, it should be also underlined that an excessive flow of information can lead to a malfunctioning of risk assessments strategy. In this regard, involved institutions have to put all efforts for a sounding implementation of the principle of proportionality so to orientate the gathering and the analysis of information towards what is really relevant for AML/CFT.

In conclusion, risk assessments may significantly boost AML/CFT policies. However, flows of information are useful only when policies really take place. In this regard, recent experiences teach that a lot is yet to be done.

Notes

1. Barone, R. & Masciandaro, D. (2008) "Worldwide Anti-Money Laundering Regulation: Estimating Cost and Benefits", *Global Business & Economic Review*, 243–264.
2. Black, J. (2005) "The emergence of risk-based regulation and the new public management in the United Kingdom", *Public Law*, Autumn, pp. 512–549; Hampton, P. (2004) *Reducing Administrative Burdens: Effective Inspection and Enforcement*, London: HM Treasury Department; Hutter, B. (2005) *The Attractions of Risk Based Regulations: Accounting for the Emergence of Risk Ideas in Regulations*, London: Centre for Analysis of Risk and Regulation (CARR) Discussion Paper DP 33, London School of Economics and Political Science (LSE).
3. Black, J. & Baldwin, R. (2010) "Really Responsive Risk-Based Regulation", *Law & Policy*, April, Vol. 32, pp. 181–213.
4. Black, J. & Baldwin, R. (2012) "When risk-based regulation aims low: Approaches and challenges", *Regulation & Governance*, Vol. 6, pp. 2–22.
5. Dalla Pellegrina, L. & Masciandro, D. (2009) "The Risk-Based Approach in the New European Anti-Money Laundering Legislation: A law and Economics View", *Review of Law & Economics*, Vol. 5, pp. 931–952; Ross, S. & Hannan, M. (2007), "Money Laundering Regulation and Risk-Based Decision Making", *Journal of Money Laundering Control*, pp. 106–115.
6. FAFT (2012) *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, Financial Action Task Force, Paris.
7. These activities are: (a) buying and selling of real property or business entities; (b) managing of client money, securities or other assets; (c) opening or man-

agement of bank, savings or securities accounts; (d) organisation of contributions necessary for the creation, operation or management of companies; and (e) creation, operation or management of trusts, companies, foundations, or similar structures.

8. Cassese, S. (2012) *Istituzioni di diritto amministrativo*, Torino: Giuffrè Editore, p. 126.
9. Della Cananea, G. (2004) "The European Union's Mixed Administrative Proceedings", *Law and Contemporary Problems*, Winter, pp. 197–218.

CHAPTER 6

Tax Crimes Inclusion in "Criminal Activity" Definition

Andrea Zaccagna

Abstract The new European Union (EU) Directive 2015/849 includes tax offences in the range of predicate offences that qualify criminal activity, such as to constitute the basis of money laundering, in line with the revised FATF Recommendations. The Directive IV provides that each Member State identify tax offences constituting "criminal activity". The tax crimes inclusion in the definition of criminal activity is undoubtedly an important innovation of Directive IV, especially considering that the most part of money laundered arise from tax crimes activities.

The year 2014 was a record year for hidden and laundering money operations in Italy with thousands of illegal criminal activities. The annual Financial Police Report estimates that during last year in Italy the total amount of Euros involved in laundering money activity was approximately 2.8 billion euro. The main category of predicate offences from which money laundered arise are related to tax crimes: almost 1.1 billion of euros on a total amount of 2.8 billion comes from tax evasion. They are money evaded from the State balance, saved and hidden by those who do not pay taxes. Despite the law enforcement of Financial Police, the illegal business continues to grow. It is easy to understand how this situation affects severely the economy of the States, already weakened by European sovereign debt crisis that has been taking place in the European Union (EU) since the end of 2009. It is on the basis of these considerations that EU Member States have felt the need to combat money laundering with any tools. Already in its

D. Siclari (ed.), *The New Anti-Money Laundering Law*,
DOI 10.1007/978-3-319-29099-7_6

12 February 2012 Recommendations, FATF-GAFI included expressly tax crimes in the category of "predicate offences" in order to extend the application field of Anti Laundering Law. The third FATF's Recommendations states that: "Countries should criminalise money laundering on the basis of the Vienna Convention and the Palermo Convention. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences."[1]

In particular, in the section "Interpretative note to recommendation 3 (Money laundering offence)", FATF ruled that:

1. Countries should criminalise money laundering on the basis of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and the United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention).
2. Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences; or to a threshold linked either to a category of serious offences; or to the penalty of imprisonment applicable to the predicate offence (threshold approach); or to a list of predicate offences; or a combination of these approaches.
3. Where countries apply a threshold approach, predicate offences should, at a minimum, comprise all offences that fall within the category of serious offences under their national law, or should include offences that are punishable by a maximum penalty of more than one year's imprisonment, or, for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences that are punished by a minimum penalty of more than six months imprisonment.
4. Whichever approach is adopted, each country should, at a minimum, include a range of offences within each of the designated categories of offences. The offence of money laundering should extend to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime. When proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence.
5. Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in

that country, and which would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence, had it occurred domestically.

6. Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.
7. Countries should ensure that: (a) The intent and knowledge required to prove the offence of money laundering may be inferred from objective factual circumstances. (b) Effective, proportionate, and dissuasive criminal sanctions should apply to natural persons convicted of money laundering. (c) Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil, or administrative proceedings with respect to legal persons in countries in which more than one form of liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be effective, proportionate, and dissuasive. (d) There should be appropriate ancillary offences to the offence of money laundering, including participation in, association with, or conspiracy to commit, attempt, aiding and abetting, facilitating, and counselling the commission, unless this is not permitted by fundamental principles of domestic law.

The 2012 April Paper from the European Commission proposed to examine if the current approach of use of "all serious offences" could be sufficient to include also tax crimes or if they should be included in the specific category of "serious offences" according to art. 3, n. 5 or if it would be better to give a more precise definition of tax crimes.

The solution chosen by Directive IV is the second one such as the inclusion of tax crimes in a specific category of "serious offences" to art. 3, n. 4 letter f. The new EU Directive 2015/849 of the so-called fourth Money Laundering Directive, dated 20 May 2015 includes tax offences in the range of predicate offences that qualify criminal activity, such as to constitute the basis of money laundering.

Not all the tax crimes are included in this category but only such tax crimes that in the national legislations are punished with a maximum fine of over one year of prison and a minimum of over six months of prison.

The 11th whereas of Directive IV highlights that "tax crimes" relating to direct and indirect taxes are included in the in the broad definition of "criminal activity", in line with the revised FATF Recommendations. Given that different tax offences may be designated in each Member State as constituting "criminal activity", national law definitions of tax crimes may diverge. While no harmonisation of the definitions of tax crimes in Member States' national law is sought, Member States should allow, to the greatest extent possible under their national law, the exchange of information or the provision of assistance between EU Financial Intelligence Units (FIUs).

The article 3, number 4 of the Directive gives the definition of criminal activity, such as any kind of criminal involvement in the commission of the following serious crimes:

1. acts set out in articles 1–4 of Framework Decision 2002/475/JHA;
2. any of the offences referred in Article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;
3. the activities of criminal organisations as defined in Article 1 of Council Joint Action 98/733/JHA;[2]
4. fraud affecting the Union's financial interests, where it is at least serious, as defined in Article 1(1) and Article 2(1) of the Convention on the protection of the European Communities' financial interests;[3]
5. corruption;
6. all offences, including tax crimes relating to direct taxes and indirect taxes and as defined in the national law of the Member States, which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards Member States that have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months.

The tax crimes inclusion in the definition of criminal activity is undoubtedly an important innovation of Fourth Directive, especially considering that the most part of money laundered arise from tax crimes activities.

Of course, for such tax crimes, it is essential to verify the moment in which the offence occurs and the presence of eventual punishment thresholds under which there is no punishment.

Tax crimes are set by Legislative Decree n°74/2000 which splits them into two main categories:

1. Tax crimes related to tax returns;
2. Tax crimes related to accounting records and tax payments.

The first category includes the following offences:

- Art. 2—Fraudulent tax return by the use of invoices or other documents for non-existent transactions. This article shall punish anyone, in order to evade income tax or value-added tax, making use of invoices or other documents for non-existent transactions and indicates in the annual tax return relating to these tax items, false liabilities. The fraud is realised with no minimum threshold.
- Art. 3—Fraudulent tax return by the use of other devices: it shall punish with imprisonment from one year and six months to six years anyone, in order to evade income tax or value-added tax, on the basis of a false representation in the compulsory accounting and making use of fraudulent means such as to hinder the investigation. It indicates in one of the annual statements relating to such taxes active elements for an amount less than the actual or false liabilities, when jointly:
  1. the unpaid tax is higher, with reference to single out any of the taxes, of 75,000 euro;
  2. the total amount of the assets taken from taxation, also by indicating false liabilities, and more than 5 % of the total amount of the assets mentioned in the statement, or, in any case, and more than 1.5 million euro.
- Art. 4—Misrepresented tax return, when someone, in order to evade taxes, reports in his annual tax return, false assets and liabilities. This crime is realised only if the tax evaded is more than Euro 10,329,138 and at the same time the total amount of activities and liabilities is more than 10 % of the total amount of activities indicated in the tax return or more than Euro 206,582,760.
- Art. 5—Annual tax return omission: in order to be punished, the total amount of tax evaded shall be higher than 7,746,853 euro.

In any case, the above-mentioned offences are not punishable if just attempted.

The second category of tax crimes is related to accounting records and tax payments.

- The art. 8 of the legislative Decree punishes with imprisonment from one year and six months to six years anyone who, in order to permit any other evasion of income tax or value-added tax, issues invoices or other documents for non-existent transactions.
- The art. 10 (Hidden or destruction of accounting records) punishes anyone who, in order to evade taxes, acts with the purpose to not allow the reconstruction of incomes or business cash flow.
- The art. 10—bis (Omitted payment of withholdings) punishes anyone who, within the term for submitting tax return, does not pay withholdings for an amount exceeding 50,000 euro.
- The art. 10—ter (Omitted VAT payment) punishes anyone who, within the term for the payment of the first advance payment, does not pay an amount of VAT exceeding 50,000 euro.
- The art. 10—quater (Undue tax compensation) punishes anyone who does not pay taxes using in compensation undue or not existing tax credits for an amount exceeding 50,000 euro.
- The art. 11 (Fraudulent subtraction to tax payments) punishes anyone who, in order to not pay taxes, simulates the selling or carrying out of fraudulent acts on own or others' properties with the scope to make inefficient the collection of taxes. The fraudulent subtraction is realised only if the total amount of taxes evaded is exceeding 5,164,569 euro.

The problem of tax crimes as predicate offences for money laundering is currently debated. The Italian doctrine[4] is not unanimous in considering tax crimes as predicate offences for money laundering because tax evasion does not generate new income but results in a tax savings on an income produced by another activity. In accordance with such opinion is the thesis that the concept of origin indicates a motion from a location so the object of laundering money could be only an increase of income, considered as illegal flow of income coming from outside and held by recycler.[5]

According to this opinion, a relevant part of tax crimes should not be included in the category of predicate offences for money laundering. For example, the selling of goods is not declared in balance sheet with related misrepresented tax return (see art. 4 Dlgs. 74/2000): the flow of income is generated by economical activity and not by tax evasion that determines a saving and not a new income.[6]

Despite this trend, the current position of Italian criminal jurisdiction is to consider tax crimes as predicate offences of money laundering, in accordance with the above-mentioned FATF's Recommendations and the 23 April 2012 Bank of Italy UIF's Communication that consider tax evasion and money laundering strictly linked.

Moreover, it is important to notice that for criminal law, laundering money definition (art. 648 *bis* Italian Criminal Code) is wider than tax definition provided by Legislative Decree 231/2007; thus, tax crimes should be undoubtedly considered predicate offence for laundering money.

The Italian legal system has been recently updated with the introduction of the article 648 *ter*, 1st coma, so-called Self money laundering.[7] Self money laundering consists in hide and use of proceeds arising from self-crimes and it is particularly frequent in tax offences such as tax evasion.

The Directive IV lays the foundation for an effective and enhanced implementation of a system to combat money laundering, also to give greater clarity and force the rules of the Member States.

From 26 June this year and in two years, the EU countries are obliged to put in place provisions to comply with Directive IV. In particular, they will have to include in its national legislation the definition of criminal activity by broadening the range of predicate offences with the inclusion of tax crimes, related to direct and indirect taxes, punishable by a custodial sentence or other measure of equivalent maximum of more than one year or, in the case of legal system that have a minimum threshold for offences, those offences, again by way of detention or equivalent measure, the minimum duration of six months.

Unfortunately, this new Directive does not still lead to full harmonisation at Community level of the scope of criminal activities, such as the assumption of laundering money: it would be better to take this opportunity to define exactly what is meant by tax offence in the individual countries of the European Community, regardless of the legislation of a criminal tax in force in each State and the type of punishment that the rules further provide in the case of commission of a tax offence.

In any case, it is however a huge step forward in the fight against international money laundering because by now many countries have already included in their legislation the tax crimes and the new offence of self-laundering whose predicate offence may well be the tax offence.

Since the entry into force of the Directive, even the appearance that the source of funds may result from tax offences will trigger the obligation for the broker reporting of suspicious activity.

Therefore, the tax compliance of law which enters now essential requirement of verification of customers without any doubt first generated from the non-express reference to these offences among those who could qualify criminal activity.

It is worth remembering that among the European countries that have already incorporated the crime of self-laundering, there are—as well as Italy—also France, Spain, the UK, Germany, Belgium, and Portugal.

Moreover, the new Directive and the new legislation contained in it is quoted and echoed last directive on the exchange of information between tax authorities will come into effect the same timing predicting that intermediaries adopt European anti-money laundering standards for the identification of the owner actual and then communicate automatically to the countries with whom such persons are residents.

The entry into force of the new joint European standards raises crucial information assets of European states contributing to the international fight against tax evasion.

The European Parliament resolution of 25 October 2011 on organised crime in the EU, while not binding, has contributed a lot to the introduction of self-laundering crime in Italian legal system. Through its resolution, European Parliament has requested expressly to Member States to introduce a legal tool to counteract the laundering of illegal money done directly by the crime's author. Currently only Italy, Belgium, Greece, Portugal, and UK have introduced a specific law on self-laundering money while it is not present in France, Germany, Austria, and Denmark.

With reference to Italian legal system, the article 3 of Law n. 186/2014 has introduced the new article 648—*ter* of Italian Criminal Code (i.e. Codice Penale) so-called self-laundering, as well as an amendment to Art. 25-octies of Legislative Decree 231/01, which will now also consider this new offence (entered into force on 01/01/2015).

The self-laundering is the activity of occultation of the proceeds of crimes committed by the author of the principal crime. It is seen above all as a result of specific offences, such as tax evasion, corruption, and the appropriation of company assets.

It is interesting to notice that the Article. 648-ter, paragraph 1, of the Criminal Code, unlike what happens, for example, for recycling, specifically lists the conduct subject to prosecution.

These are related to three behaviours: use, substitution, or transfer activities in economic, financial, entrepreneurial, or speculative money, of goods or other benefits from the predicate crime.

The object of reutilization must be in fact related to revenues resulting from the commission of the predicate offence and it must actually hinder the identification of the criminal origin.

From the foregoing emerges, as anticipated above, the difference between the structure of the offence in question and that of recycling.

The legislature, in fact, for the new offence introduced a listing, peremptory, pipelines punishable.

While recycling, not only is the conduct of using (but only those of substitution or transfer) of proceeds not provided, but there is also a general clause given by the formula: "or carries out other transactions in their" (clause obviously refers money, goods, and other benefits).

This then allows, for the purposes of money laundering, to use among the prohibited conducts, any recycling conducts while this is not possible in the new offence of self-laundering.

With the term "use", it may be concluded that the legislature intended to affect the use of money, goods, or other economic benefit from the predicate offence and specific to a particular aim.

However, it is still too early to assess the impact of the new legislation on the Italian legal system and on the fight against criminality. The coming months will be a useful test in assessing the true effectiveness of the EU reforms (Fig. 6.1).

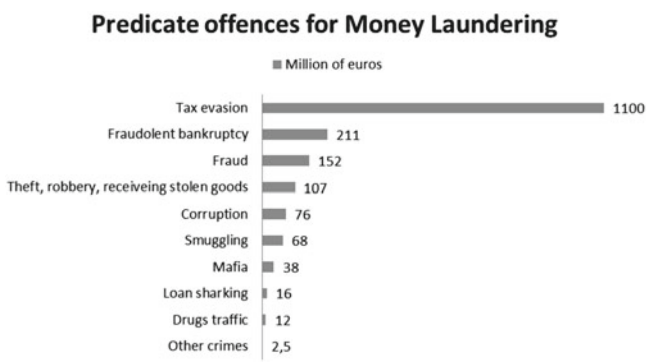

Fig. 6.1 Data from Corriere della Sera 9 August 2015

Notes

1. FATF Recommendation 3rd pag. 14.
2. Joint Action 98/733/JHA of 21 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on EU, on making it a criminal offence to participate in a criminal organisation in the Member States of the EU (OJ L 351, 29.12.1998, p. 1).
3. OJ C 316, 27.11.1995, p. 49.
4. Zanchetti, *Il riciclaggio di denaro proveniente da reato*, Milano, 1997, 398 ss. Manes, *Riciclaggio* in A.A.V.V. *Diritto Penale, Lineamenti di parte speciale*, Bologna, 2009 pag. 722; Flora, *Sulla configurabilità del riciclaggio di proventi da frode fiscale*, in Foro Ambrosiano 1999, pag. 411.
5. Luigi Domenico Cerqua, Il delitto di riciclaggio dei proventi illeciti, in Il riciclaggio del denaro. Il fenomeno, il reato, le norme di contrasto a cura di CAPPA-CERQUA, Mlano 2012, pag. 78.
6. Studio Antiriciclaggio n. 261-2013/B, Reati fiscali e normativa antiriciclaggio: i confini dell'obbligo di segnalazione a carico dei notai by Consiglio Nazionale Del Notariato.
7. Introduced by art. 3 Law 186/2014 published on 17 December 2014 with the related change of art. 25 *octies* Legislative Decree n° 231/2001.

CHAPTER 7

The Effects of New Rules on Gambling

Elena Giacone

Abstract The European Union (EU) Fourth Directive introduces an important innovation that applies not only to casinos, already affected by the previous Directive, but also to the providers of gambling services, including those online. What follows is a comparative analysis vis-a-vis the previous Directive, providing a focus on the main changes and relevant implementation issues.

7.1 The Limits of the Third Anti-Money Laundering Directive

Directive 2005/60/EC of the European Parliament and of the Council (hereinafter "Third AML Directive"), adopted on 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, constitutes one of the most powerful legal instruments to ensure an effective framework to safeguard the soundness, integrity, and stability of credit and financial institutions and confidence in the financial system as a whole, against the risk of money laundering and terrorist financing.

The Third AML Directive reflects to a considerable degree the Recommendations on international standards adopted in February 2012 by the Financial Action Task Force (FATF); however, since the same Directive follows a minimum harmonization approach, the legal framework was completed by rules adopted at the national level.

D. Siclari (ed.), *The New Anti-Money Laundering Law*,
DOI 10.1007/978-3-319-29099-7_7

As far as the (betting and) gambling sector is concerned, it should be noted how the Directive's approach was generic and lacking as regards both definitions and regulatory requirements to be applied to this matter. In fact, the Third Directive, in Article 2, merely envisages the application of anti-money laundering (AML) measures to "casinos" only, by resorting to a formulation which does not seem free from flaws, and, though being a "minimum standard" and surely not an upper limit to the national law-makers' power to extend its scope to activities other than those performed in casinos, has so far given rise to an application across Europe that might best be defined as "patchy".

In actual fact, the 14th Recital extends the application of the Directive "also to those activities of the institutions and persons covered hereunder which are performed on the Internet". Nevertheless, by making reference only to casinos, it is to be understood that its application can be extended only to the so-called *online* casinos, and not also to other types of *online* gambling.

As regards the obligation of customer due diligence referred to in Article 10(1) and (2), concerning a requirement that all casino customers be identified and their identity verified if they purchase or exchange gambling chips with a value of EUR 2000 or more, the customer due diligence requirements shall be deemed in any event satisfied if casinos register, identify, and verify the identity of their customers immediately on or before entry, regardless of the amount of gambling chips purchased and adopt appropriate procedures to reconnect their identification data to the purchase or exchange of gambling chips that each customer makes with a value of EUR 2000 or more.

These provisions are recognized as overly permissive and generic since there was no setting of minimum requirements for the factors that are to be taken into account in the different situations, and possible exemptions provided were not justified on the basis of risk.

It was just this lack of regulatory guidance which made it necessary to complete the framework of AML legislation through national implementing measures adopted by Member States which could somehow fill the gaps in the Directive.

In Italy, for instance, the Third Directive was transposed by Law No 29 of 25 January 2006 (so-called Community Law 2005), which delegated the Government to adopt one or more legislative decrees in order to implement the principles and provisions contained therein as an organic whole.

Subsequently, the delegation was implemented by Legislative Decree No 231 of 21 November 2007 that, through its 68 articles, divided into five titles and a technical annex, set out to become the single standard reference in the field of prevention of the use of the financial system for the purpose of laundering the proceeds of criminal activity and terrorist financing.

It is important to emphasize that, in the betting and gaming sector, Legislative Decree No 231 of 2007, namely Article 14, extended the customer due diligence requirements to all gaming (gambling services) distributed on the internet and not only online casinos, and subsequently to all betting and gaming collected through a physical network (collection points) with the sole exception of *Gioco del Lotto* (Italian lottery), instant and deferred lotteries (scratch cards) and sports-based pools, in view of their low risk for money laundering purposes.

It was Italy's experience in this field which allowed to highlight a number of peculiarities of the gambling sector which are such as to make it necessary, as implemented by the Commission thereafter, to adopt a customization of approaches and obligations for gambling operators.

The Commission itself, in its Report to the European Parliament and the Council on the application of the Third AML Directive, stated that

> the Directive also covers activities "performed on the Internet" (recital 14), thus also covering on-line casinos. Consultations have indicated general support in favour of a broader definition of gambling in the Directive, but with the precise scope to be determined on a risk-based basis at national level. Consideration could be given to capturing gambling activities which pose higher AML/CFT risks, while avoiding the imposition of an excessive burden on lower risk activities. The Commission services are planning to adopt an action plan on on-line gambling in 2012, and it will therefore be appropriate to ensure a consistent approach between any initiatives proposed to tackle money laundering in this sector and the revisions to the Third AML Directive.

After the application of the Third Directive, the Commission has initiated work to update and enhance the existing international standards in order to further strengthen the EU's defences against the evolving threats related to money laundering and terrorist financing to ensure the soundness, integrity, and stability of credit and financial institutions, trying to provide a constant proportionate response. On 7 February 2013, the Commission presented a package composed of two elements:

- a 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 (AML Directive);
- a proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds (AML Regulation).

The Directive and the Regulation were adopted simultaneously, but whereas the Directive gives the Member States a period of two years to transpose it into national law, the Regulation is instead directly applicable in all Member States 20 days after its publication in the Official Gazette.

7.2 From the Commission's Proposal for a Directive to the IV AML Directive

With the approval and adoption by the European Parliament of the revised Fourth AML Directive, major changes were introduced also in respect to the gambling sector.

The European legislators have taken into account the specificities of this business, extending the scope of the new Directive to all gambling services.

The long introduction to the text indicates the reasons which prompted the Community legislature to a new intervention in the gambling sector given that, in particular, the use of gambling services for laundering of proceeds of criminal activity is becoming increasingly widespread, and, more generally, the EU legislation in this matter is today excessively complex, stratified, and poorly harmonized.

Indeed, it should be pointed out that gambling services fall within the scope of Article 56 of the Treaty on the Functioning of the European Union (TFEU) and are governed by the rules and regulations on the provision of services. This term encompasses a wide range of service activities to which individuals may have direct access by electronic means, such as:

- online sports betting;
- casino games;
- media games;
- promotional games;
- gambling services operated by and for the benefit of recognized charities and non-profit making organizations;
- lotteries.

Within the context of online games, the preparation and provision of hardware and software technological platforms that allow players to make bets at a distance, via the Internet or other telecommunication network, are used to:

– to offer consumers services of gambling;
– to allow consumers to bet or gamble against other consumers (e.g. betting exchanges or poker online);
– as a distribution technique (e.g. to purchase lottery tickets).

The Fourth Directive proposal was introduced to:

– STRENGTHEN the Internal Market by reducing complexity across borders;
– SAFEGUARD the interests of society from criminality and terrorist acts;
– SAFEGUARD the economic prosperity of the EU.

These objectives also involve the public gaming sector for the continued and increasing importance and attention devoted to it by both national governments and entrepreneurs. The former are working constantly to ensure greater legality and control, also in order to preserve the tax revenues derived from them; the latter consider the differences in regulatory legislation in the various countries as opportunities to increase the supply with the consequent increase of business volumes and revenue opportunities.

The achievement of these objectives can only be ensured through greater consistency with the EU and international approaches and, accordingly, greater consistency between national rules and regulations that will require a certain degree of flexibility in their implementation.

Internationally, the vulnerabilities of the system for the prevention of money laundering in the gaming sector were highlighted, in a 2009 report,[1] by the FATF, regarded as a reference on a global scale in the field of standards against money laundering and terrorist financing.

Moreover, at Community level, the Green Paper on online gambling in the Internal Market[2] was published in March 2011,[3] followed by the Communication from the Commission of 23 October 2012.[4]

The IV Directive builds on the above studies and intends to implement the Recommendations adopted by the FATF and, in some respects, goes further in that it extends the FATF requirements and provides additional safeguards in the gambling sector as well.

The text adopted in plenary session confirms the extension of the scope of the new Directive to all public gambling services, allowing appropriate supervision that the Member State will decide to apply to them, for transactions amounting to EUR 2000 or more.

The Commission itself in making an impact assessment[5] of the previous Directive, has analysed inter alia the negative economic impacts and instability of the financial market as possible consequences of money laundering and terrorist financing, and has come to the conclusion that one of the viable options to improve the situation is the introduction of a requirement for Member States to carry out a risk assessment at the national level and take measures to mitigate risks.

This has led to the application of a risk-based approach to fight in a more targeted way the risks related to money laundering and terrorist financing. The importance of a supranational approach to risk assessment has been recognized internationally since such approach constitutes an application of the broader principle of proportionality and aims to maximize the effectiveness of company controls (safeguards), rationalize the use of resources, and reduce the burden on recipients.

Moreover, in proven low-risk circumstances, Member States are allowed to exempt certain gambling services from some or all of the requirements laid down, in strictly limited and justified circumstances, with the exception of casinos which will not in any way benefit from exemptions. Such exemptions in any event will be subject to a specific risk assessment.

These conclusions were reached after the Committee on Economic and Monetary Affairs and the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament had approved the Joint Legislative Resolution to the then Proposal for a Directive.[6]

Of the numerous proposed amendments concerning gambling to the Proposal for a Directive, only four were adopted.[7]

The common denominator of the various proposals for legislative changes was the principle of safeguarding and maintaining public order that the use of the gambling sector for the purpose of laundering the proceeds of criminal activity could undermine and therefore create major problems, regardless of the types of games concerned. However, emphasis was also placed on the importance of their specificities and their particular vulnerability to money laundering techniques. For this reason, it was deemed necessary, during amendment debate, to envisage appropriate and specific arrangements for each of three categories: casinos, providers of gambling services and online gambling, as well as providers of other gambling services.

Nevertheless, some of the amending proposals approved focused attention on the need to distinguish between gambling services with a high risk of being used for money laundering purposes and those for which such a risk is extremely low. To this end, Member States should be allowed to evaluate the need for further tests and research to understand the nature and extent of risks in the different areas of gambling, which should, obviously, be treated differently. An example is that of casinos that should ensure that customer due diligence, if it is taken at the point of entry to the premises, can be linked to the transactions conducted on those premises.

It must in fact be considered, as was done by those who proposed this last legislative amendment, that, although there are risks in some gambling activities, in the absence of thorough testing, the inclusion of the entire gambling sector can be inefficient and disproportionate. The FATF itself has stressed that any legislation should be based on risk and that some activities are regarded as lower risk based on national risk assessments.

In this regard, we can say that in the case of supply of gambling services with high payouts, there is a greater risk that they could be used for money laundering; this is particularly true in the case where the gambling services have high event frequency, their success does not depend solely on chance, and it is possible to place very high stakes in a short time. This is the reason for the introduction of an obligation for all providers of gambling services to conduct customer due diligence, on a regular basis or even enhanced, for single transactions (bets and winnings) of EUR 2000 or more, and in any case when the average payout percentage exceeds 90 %. Here, then, for State gambling operators with low average payout percentages and in any case not exceeding 55 %, an obligation has been envisaged to conduct customer due diligence for the winnings of EUR 2000 or more; moreover, casinos must ensure that customer due diligence, carried out at the point of entry to the premises, can be linked to the transactions conducted on those premises.

The amendment concerning the above was based on the fact that the Commission's proposal did not distinguish the gambling offers with a higher risk of money laundering from those with a lower risk, and this was in stark contrast to the risk-based approach that is the basis of the proposal, and now of the Directive.

The emphasis, in fact, should have been placed on those games that, owing to their high payout percentages and other characteristics included in the amendment, are of interest for those who intend to launder money. This shall not apply to the State gambling operators with low payout percentages.

On 5 June 2015, the Fourth Directive was published in the *Official Journal of the European Union*.

7.3 Public Games and the Innovations of the Fourth AML Directive

After numerous interventions in the field of gambling, both at Community level and at international level, it was considered necessary, as fully detailed in the previous paragraph, with respect to the revision of the Third AML Directive, to also extend the scope of gambling since the removal of barriers in the internal market, on the one hand, facilitated the creation and the development of legitimate activities in the EU, on the other hand, offered and still offers a number of occasions to criminal activities to infiltrate in order to carry out laundering and try to conceal or disguise their true nature, source, or ownership of property so as to convert the latter into seemingly legitimate proceeds. What's more, factual elements indicate that the application of the Third Directive limited to only physical and *online* casinos has exposed other areas of gambling to exploitation by criminals.

According to the report approved by the Financial Security Committee (FSC) in July 2014, entitled "National analysis of the risks of money laundering and terrorist financing" (National Risk Assessment, NRA), the gaming industry has often represented a huge financing resource to organized crime to invest proceeds in purchasing casinos and registering the latter in a straw man's name. The aim is either to draw substantial profits from alteration of game rules to limit gambler's chance of winning and from adoption of tricks to reduce the amount of tax withdrawals, or to redeploy illegal capital into the economic system by shielding that illegal capital behind the apparent winning and by realizing operational schemes which might also conceal abusive lending and usury.

In regard to the above, the Court of Justice[8] has confirmed that the provision of games of chance or gambling is an economic activity of a special nature, where restrictions may be justified for reasons of overriding general interest such as consumer protection, fraud prevention, the fight against money laundering, and the preservation of public order and health; any restrictions imposed thereto need to comply with those provided for by the TFEU, such that they must be proportionate to the objectives pursued and must not be discriminatory.

The European Parliament in its Resolution of 10 September 2013[9] entitled "Online gambling in the internal market" points to the fact that online gambling is a non-cash-based environment and that—given the dependency on third party financial service providers—additional safeguards against money laundering are needed. To this end, a close cooperation between national gambling authorities, national police and national enforcement authorities in preventing criminal activity should be implemented.

Those are the principles and reasons which prompted the Member States and the expert group to urge the Commission to accept the proposal to extend the provisions of the Third AML Directive for including all forms of gambling and ensuring that any transaction suspected of being potentially connected to money laundering or other criminal activity is reported in accordance with the provisions of the then Third Directive.

The aim of the Fourth Directive, in fact, was to reinforce obligations with regard to customer due diligence, by improving the accessibility and intelligibility of legal framework in order to have adequate controls and procedures permitting a better customer knowledge and understanding of the nature of the activities carried out by the customer himself.

The same proposal already extended the scope of the obligations with regard to customer due diligence to all those persons supplying goods or providing services against cash payment of financial transactions larger than EUR 7,500—rather than EUR 15,000 as in the past (although in the version finally approved the threshold is still EUR 15,000, except for occasional transactions carried out by persons and settled in cash amounting to a maximum threshold of EUR 10,000)—as well as to public gaming operators carrying out financial transactions larger than EUR 2,000, whether the transaction is carried out in a single operation or in several operations which appear to be linked.

It remains, therefore, the requirement to carry out the customer due diligence, in any case, regardless of the threshold, exemption or derogation in all cases of suspected money laundering or terrorist financing as well as in case of doubts about data obtained during a previous identification of the customer.

Following the final approval of the text by the Commission and the European Council, it can be observed how the European legislators have achieved the aim and have taken into account the specificities of this business—the gambling services—thus allowing appropriate supervision that the Member State will decide to apply to public gaming services for transactions amounting to or higher than EUR 2,000, but without any exemption for casinos. The text adopted in plenary session confirmed the extension of the scope of the new AML Directive to all public gambling.

If compared to the previous text, the Fourth Directive still provides for "providers of gambling services" in Article 2(1) among the obliged entities to which the Directive shall apply, but in paragraph 2 it is moreover provided for a possible exemption of low-risk providers from obligations on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services, with the exception of casinos. Decisions about exemptions shall also take into consideration the degree of vulnerability of the applicable transactions, including with respect to the payment methods used. Any decision shall be notified to the Commission, together with a justification based on the specific risk assessment. The Commission shall communicate that decision to the other Member States.

For this reason, Recital 21 states that the use of an exemption by a Member State should be considered only in strictly limited and justified circumstances, and where the risks of money laundering or terrorist financing are low.

Casinos have always been the most used place by organized crime to launder money through the mechanism of purchase of gambling chips in large quantities in order to play, but then only using a small quantity of the same or even not using them at all.

The purpose of these transactions is to convert gambling chips into money and simultaneously be issued by the casino a document certifying the winning; but, organized crime even prefer to acquire direct control of a casino by declaring black money as income from gambling business.

It is clear from the above that there is a high risk of money laundering for casinos and consequently it is also clear the reason why it is impossible to exempt them from the application of the new AML Directive.

The new Directive also considers another sector of special interest that is, the *online gambling*, then, not only the "online casinos" as provided for by the Third Directive, but the whole industry of *online* games including poker, bingo, betting exchange, which are available both on the computer and on smart phones and tablets. The most attractive factor of *online* game is definitely its profitability; the latter is proven by an increase in the number of legitimate online sites which have a jurisdictional license to conduct their activities as well as of unauthorized sites far more numerous than to the first ones.

The focus on *online gambling* is due to the intrinsic risk that *online* gaming platforms may become an instrument for money laundering. This risky scenario applies mainly to *online gambling*:

(a) as it generates a large number of transactions and cash flows;
(b) as it is not a physical product, thus making cash flow and the transition from real to virtual money less traceable. UIF[10] reminds that the so-called virtual currency,[11] more and more common, is a digital representation of value that is accepted—on a voluntary basis—as a means of payment to purchase goods and services. It can be transferred, stored, or traded electronically. Virtual currency is issued neither by a central bank nor by a public authority, it does not constitute legal tender, or is similar to electronic money. There are different types of virtual currencies. In today's world, there are over 500 types: the most common is "Bitcoin";[12]
(c) moreover, in many jurisdictions, the winnings are not taxed (excluding Italy).

The elements described above make *online* game websites very attractive for money laundering purposes; there may exist two scenarios at this end:

- to bet on *online gambling* websites using the money to be laundered, which is then "cleaned". As these transactions often take place offshore, tougher local regulations do not allow to increase the chance of identifying the transactions themselves;
- or to use the games in a "player-to-player" mode, thus allowing the transfer at will of the money to be laundered through fictitious play challenges. The "tax free" nature of the winnings is a further advantage on many websites.

It is also necessary to consider that most websites, either authorized or not, allow players to make deposits and withdrawals of money even through unauthorized banks. This circumstance, along with the various available methods of deposit/withdrawal, leads to a scenario where money laundering becomes anything but a remote possibility.

Those who are willing to use *online gambling* for illicit purposes have three weapons at their disposal: anonymity, settlement procedure (through anonymous communication systems on the internet—VPN, proxy servers, TOR) and ancillary services or the so-called *mixer* or similar services which allow players to buy virtual currency anonymously or to disguise the origin of their capital.

Conversely, among the physical network gambling forms, VLT machines and fixed odds[13] betting have very significant vulnerabilities—significant specific risk and very significant vulnerability—because they can be used for the purpose of laundering operations.

Reports of anomalies related to the use of VLT machines are increasing. Most of the reports relate to the existence of recurring winners at the same provider points: the frequency of winnings in hands of the same entities might be a signal of the existence of a secret market of winning tickets. Within such a market, the recyclers would buy tickets from the actual winners against a larger compensation. Other cases concern a possible distorted use of VLT machines: after the insertion of banknotes, they may deliver winning tickets even in the absence of an effective wagering of a stake, thereby facilitating the laundering of funds of suspicious origin.

The sector of sports betting agencies is also of special interest to the organized crime involved in money laundering. Buying the winning tickets represents the traditional means to launder money. In this case, the lucky winner attracted by the offering of an amount larger than the winning, is induced to deliver the winning ticket to the organized crime that, in turn, obtains legal income. However, it may even be the case that the organization decides to bet large amounts (through multiple operations) on all possible outcomes of a sporting event so as to secure a substantial payout, although being an amount lower than the wagering of a stake.

From a subjective standpoint, the inclusion of providers of gambling services (for transactions amounting to or exceeding EUR 2,000) among the obliged entities to which the new Directive shall apply is a significant innovation since the Third Directive, in Article 2, provided for the application of the same directive only to "casinos", intended as the physical place reserved to gambling.

With respect to the meaning of "providers of gambling services", the Fourth Directive, in Article 3(14), establishes that *'gambling services' means a service which involves wagering a stake with monetary value in games of chance, including those with an element of skill such as lotteries,… and betting transactions that are provided at a physical location, or* online and those games in which the random element is prevalent (e.g. poker games). Actually, the nature of poker games and skill games is generally quite controversial because, although the Directive expressly qualifies both as gambling, it is the player's skill that prevails on risk most of the times. The player may at any time withdraw, change the combination of cards in his possession, and/or destabilize his opponents with moves such as *bluff* or *all in*. Lotto (the so-called *lottery*) and betting pools are excluded from the list referred to in Article 3(14) of the new Directive since they are of low risk for AML purposes.

Another aim of the new Directive is to affect again the obligations of customer due diligence since it has been deemed necessary to increase clarity and transparency of its rules, in order to have adequate controls and procedures to enable a better understanding of the customer and the nature of the activities he carries out. In this regard, Article 11(d) extends the above obligation to providers of gambling services at the time winnings are realized, when wagering of a stake is placed, or in both cases when a transaction amounting to or larger than EUR 2,000 takes place, whether the transaction is carried out in a single operation or in several operations which appear to be linked.

Following a comparison with the previous Third Directive, Article 10, paragraph 1, and despite a similar content, it is to be noted that the current framework is broader and more general because it refers to different types of gambling and not only to casinos.

And just because of the limited range of the Third Directive, and following what was regulated by the second paragraph of the above mentioned Article, *casinos subject to State supervision shall be deemed in any event to have satisfied the customer due diligence requirements if they register, identify, and verify the identity of their customers immediately on or before entry, regardless of the amount of gambling chips purchased.*

Continuing to analyse the various innovations, it is certainly to be highlighted the one included in Article 47, paragraph 1, concerning the obligation for Member States to provide that also "providers of gambling services be regulated" and, paragraph 2, concerning the obligation *to ensure that the persons who hold a management function in the entities referred to in paragraph 1, or are the beneficial owners of such entities, are fit and proper persons.*

The new Directive introduces new measures in order to ensure effective transparency of beneficial ownership. There is a need, even among providers of gambling services, to identify any natural person who exercises ownership or control over a legal entity, and although a specified percentage shareholding or ownership interest does not automatically result in identifying the beneficial owner, it should be one evidential factor among others to be taken into account. In fact, the need for accurate and current information on the beneficial owner is a key factor for the tracing of criminals who might otherwise conceal their identity behind a corporate structure.

In this regard, it should be emphasized that organized crime is gaining substantial gaming market share whose revenues (including the legal ones) are growing exponentially. There are many varied and creative criminal ways to become part of the "game". Infiltration of casinos' management companies and betting spots, which lend themselves in a "legal" way to be "laundries" for laundering of black money.

The phenomenon is more widespread in the field of *online* gambling, considering that the number of *online* casinos is so high that local authorities find it extremely difficult to control, not to say monitor, their activities. Just to realize the extent of the phenomenon, in the year 2014, there were approximately 104 international jurisdictions governing a total of 2734 gambling websites on the Internet for at least one type of betting, and it is estimated that there are at least 25,000 gambling websites around the world which are not regulated.

Last but not the least, is the provision in Article 48, paragraph 3, stating that *in the case of credit institutions, financial institutions, and providers of gambling services, competent authorities shall have enhanced supervisory powers.*

This latter provision is a big innovation as to the gambling sector and is closely associated with the risk-based approach, which characterizes the entire Directive and that meets the need for Member States to identify, understand, and mitigate the risks of money laundering and terrorist financing.

Certainly, the emphasis posed on a risk-based approach calls on Member States for increased orientation on the factors to be taken into account when applying the customer due diligence, as either simplified or enhanced obligation, and the approach to supervision performed on a risk-sensitive basis.

7.4 A Few Reflections

In light of the above, it may be surely asserted that the new AML Directive definitely enhanced the EU protection against money laundering and terrorist financing by allowing greater solidity, integrity, and stability of the financial system.

As a matter of fact, and considering the constant evolution of the risks of money laundering and terrorist financing, it is essential that the EU as a whole be able to react in a robust but flexible way.

As to gambling services, the review process carried out by the Commission and concluded with the approval of the Fourth Directive has tried to overcome the concerns highlighted by the different parties involved in the application of the previous Directive, by introducing more robust rules able to address the risks and make the EU legislature a leader with respect to international standards.

It should, however, be considered that if, on the one hand, the introduction of more targeted and risk-sensitive rules should ensure greater effectiveness, on the other hand, this type of approach—which involves the nature of the relationship, the constant control, and the detection of suspicious transactions—is hardly applicable to the game sector because it assumes a player's familiarity not comparable to the one credit institutions and/or financial institutions have in general. Moreover, to avoid this inconvenience, the new Directive does not provide for specific instructions, easily accessible and usable by the operators to assess their degree of "risk" in the field of gambling. In addition, the number of available data relating to the game is rather less than the number of available data of credit institutions and/or financial institutions; for example, it seems difficult to request game operators to supply their customers with a questionnaire containing information relevant to their employment, family, and/or economic status.

In this regard, it would have been appropriate that the Directive had established not only criteria for complying with customer due diligence but also suitable instruments such as the obligation for supervisory authorities to make access to the information systems of those authorities issuing data and documents (e.g. identity card and tax identification number) available to operators.

On the contrary, in the *online* gaming industry, it may be suitable that the Directive be applied only to those games potentially high-risky with respect to laundering as those ensuring an average return on winnings higher than 80%, thus excluding, as it is the case in Italy, betting pools, Lotto, and lotteries (the latter listed as gambling in Article 3(14) of the Directive).

With exclusive reference to *online* games where there is the physical presence of the player and the payment can be made only with traceable instruments, it is to be pointed out that in the case of payments made by credit card or prepaid card, the gaming operator is not able to know if the card holder is actually the player or if the card is stolen or cloned. Therefore, it would be advisable that indicators of anomaly (the so-called *Key Indicators*) be arranged by the competent authorities in consultation with the operators themselves and implemented as appropriate by each subject according to their specific operations.

A further critical issue can be observed in the field of exchange of information to which the Fourth Directive dedicates special provisions which confirm and reinforce the main tools available to the EU Financial Intelligence Unit (the 'EU FIUs Platform').[14] As to the gaming sector, it would be appropriate that information be exchanged not only between the various FIUs of the Member States or between them and other third countries but also between FIUs and gaming operators with the aim of improving the analysis of anomalous behaviours in order to prevent fraud for the sake of players and public interests.

A definitely relevant aspect of the new Directive is certainly the introduction of the principle that allows Member States to exempt low-risk gambling operators. Nevertheless, it will be necessary that national legislators address the most significant aspects because, although it is true that low-risk individual types of game/sectors should not be subject to obligations relating to money laundering, it is also undeniable that the customer due diligence requirements should not be the only pivot on which the fight against laundering of proceeds from illegal activities can rest. As suggested by the Commission, it would be appropriate to carry out a monitoring of the entire supply chain, also through the incentive to the use of payment instruments which are alternative to cash money for all kinds of game, even land games.

Lastly, the impact that the new Directive will have on costs should not be neglected. Certainly, the implications will be very different depending on the positions of the various stakeholders.

The most important cost factors are those connected to compliance with the legislation on money laundering and related to the initial one-off costs relating to the introduction of new systems, training, consulting, and so on. In particular, for the gambling sector that has not been considered within the scope of the money laundering rules so far, but that will have to apply these rules in the future. In fact, in some Member States only "traditional" casinos have so far fallen within the scope of national standards.

In any case, despite the observations above, the implementation of the Fourth AML Directive across all gambling sectors will ensure to achieve greater compliance with the system at Community level, and therefore internationally, to combat money laundering and to maintain a level playing field within the EU.

From now on, the most important task will be up to Member States that will have to make an extra effort to ensure that the Directive be implemented with rules that can be easily applied and interpreted, but most of all enacted as part of a greater uniformity and harmonization between the different interests of operators acting at Community level.

Notes

1. Faft Report—"Money Laundering and the Terrorism Financing in the Securities Sector", October 2009. Cf.: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20end%20tf%20in%20the%20securities%20sector.pdf
2. Cf.: http://eur.-tex.europa.eu/legal-content/EN/TXT/PDF/?url=CELEX:52012DC0596&from=EN
3. Green Paper of the European Commission of 24 March 2011 on online gambling in the Internal Market [COM (2011) 128 final—Not published in the Official Journal] whose purpose was to launch an extensive public consultation on all relevant public policy challenges and possible Internal Market issues resulting from the rapid development of both licit and unauthorized online gambling offers directed at citizens located in the EU.
4. Cf.: http://ec.europa.eu/internal_market/services/docs/gambling/comm_121023_onlinegambling_it.pdf
5. Available at: http//ec.europa.eu/internal_market/company/financial-crime/index_en.htm
6. "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", Strasbourg, 5 February 2013—COM/2013/045 final—2013/0025 (COD).
7. Amendment 128, by Jean-Paul Gauzès and Sophie Auconie (EPP); Amendment 129, by Graham Watson, Bill Newton Dunn and Nils Torvalds Party (ALDE); Amendment 130, by Markus Ferber, Manfred Weber and Frank Engel (EPP); Amendment 131, by Peter Simon (S&D).
8. In this regard, see Case C 275/92 Schindler, paragraphs 57–60; Case C 124/97 Läärä and Others, paragraphs 32 and 33; Case C-67/98 Zenatti, paragraphs 30 and 31; Case C-243/01 Gambelli and Others, paragraph 67; Case C-42/07Liga Portuguesa, paragraph 56; Joined Cases C 316/07, C 358/07 to C 360/07, C 409/07 and C 410/07, Markus Stoß and Others, paragraph 74; Case C 212/08, Zeturf Ltd, paragraph 38; Case C-72/10 Florida, paragraph 71; Case C 176/11 Hit Larix, paragraph 15; Joined Cases C 186/11 and C 209/11 Stanleybet and others, point 44.
9. P7_TA(2013)0348—"Online gambling in the internal market"—European Parliament resolution of 10 September 2013 on online gambling in the internal market (2012/2322(INI)).
10. FIU for Italy—Bank of Italy Eurosystem—document title "Anomalous use of virtual currencies", available at https://uif.bancaditalia.it/
11. The nature and the characteristics of current virtual currencies are described analytically in the following documents available online:
    EBA Opinion on 'virtual currencies' of 4 July 2014: (http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf); FATF Report, Virtual Currencies, published in

June 2014: (http://www.fatf-gafi.org/media/fatf/documents/reports/Virtualcurrency-key-definitions-and-potential-aml-cft-risks.pdf); ECB—Virtual Currency Schemes of October 2012: (http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf)

12. Bitcoin is an electronic money invented in 2009 by an anonymous known by the pseudonym Satoshi Nakamoto, implementing his idea presented on the Internet in late 2008. Conventionally, the term *Bitcoin*, capitalized, refers to the technology and network and the term *bitcoin*, lowercase, refers to the unit of account. Unlike most traditional currencies, Bitcoin does not use a central repository: it uses a database allocated among network nodes that keep track of the transactions, and uses encryption to manage the functional aspects such as generating new currency and the assignment of ownership of bitcoin. The Bitcoin network allows the possession and transfer of anonymous coins; information needed to use bitcoins can be stored on one or more personal computers in the form of digital "portfolio", or kept at third parties that perform functions similar to a bank. In any case, bitcoin can be transferred over the Internet to anyone with a "bitcoin address". The peer-to-peer system of Bitcoin network and the lack of a central repository make it impossible for any authority, governmental or not, to block the network, seize bitcoin to the legitimate owners or devalue it by creating new currency.
13. The fixed odds betting on sporting and non-sporting events depends upon the type of sport or event on which you bet. With reference to football matches, for example, the ability to wager varies greatly from the classical "1 × 2" to the correct score of a match, the outcome for the first half, the number of goals above or below a pre-set number and many other types of results. Bets may be "single" that is, relating to a single event, or "multiple" when a bet is placed on a combination of events; in the latter case, the share of the winning is equal to the product of the individual odds offered for the outcomes indicated for each event. The wagering of a stake is placed at sports agencies, sports shops, and corners. The minimum cost of a fixed odds betting is EUR 1.00 and the minimum amount to be bet is EUR 3.00. Bets originating a winning larger than EUR 10,000 are not placeable. Parimutuel betting differs from fixed odds betting in that it is a betting system in which all bets of a particular type are placed together in a pool which represents the payoff. Accepted wagers are as follows:
    - single: the prediction of the bettor indicates the occurrence of more predictable outcomes of the same event;
    - plural: the prediction of the bettor indicates the occurrence of more predictable outcomes of an event;
    - multiple: the prediction of the bettor indicates the occurrence of one or more predictable outcomes of several events.

The amount of the payout is the multiplication between the quota and the single wager.

14. The Directive formally recognizes the FIU Platform of the EU (EU FIUs' Platform), active since 2006 as an informal group used to exchange views and facilitate cooperation among the FIUs of the Member States. A specific legal basis recognizes the important role played by the Platform for the development of common policies and clarifies its mandate. This mandate will be pursued through the development of advice for the implementation of the provisions applicable to FIUs and to the reporting agents, and coordination for the development of international cooperation.

Bibliography

Ahmad Naheem, M. (2015). Trade based money laundering: Towards a working definition for the banking sector. *Journal of Money Laundering Control, 18*(4), 513.

Alldridge, P. (2003). *Money laundering law*. Oxford: Hart Publishing.

Ardizzi, G., Petraglia, C., Piacenza, M., Schneider, F., & Turati, G. (2013), *Money laundering as a financial sector crime—A new approach to measurement, with an application to Italy*. CESifo working paper series no. 4127. Center for Economic Studies, Munich.

Barone, R., & Masciandaro, D. (2008). Worldwide anti-money laundering regulation: Estimating cost and benefits. *Global Business & Economic Review, 10*(3), 243–264.

Basel Committee on Banking Supervision. (2014). *Sound management of risks related to money laundering and financing of terrorism*. Basel: Basel Committee on Banking Supervision.

Bergstrom, M., Svedberg Helgesson, K., & Morth, U. (2011). A new role for for-profit actors? The case of anti-money laundering and risk management. *Journal of Common Market Studies, 49*(5), 1043.

Black, J. (2005) The emergence of risk-based regulation and the new public management in the United Kingdom. *Public Law*, Autumn, 512–549.

Black, J., & Baldwin, R. (2010). Really responsive risk-based regulation. *Law & Policy, 32*, 181.

Black, J., & Baldwin, R. (2012). When risk-based regulation aims low: Approaches and challenges. *Regulation & Governance, 6*, 2.

Booth, R., Farrell, S., Bastable, G., & Yeo, N. (2011). *Money laundering law and regulation. A practical guide*. Oxford: Oxford University Press.

D. Siclari (ed.), *The New Anti-Money Laundering Law*,
DOI 10.1007/978-3-319-29099-7

Borrello, I. (2015). Financial intelligence unit (FIU). In D. Siclari (Ed.), *Italian banking and financial law. I. Supervisory authorities and supervision* (p. 261). New York: Palgrave Macmillan.

Bowles, R., Faure, M., & Garoupa, N. (2005). Forfeiture of illegal gain: An economic perspective. *Oxford Journal of Legal Studies, 25*(2), 275.

Brooks, G. (2012). Online gambling and money laundering: "Views from the inside". *Journal of Money Laundering Control, 15*(3), 304.

Brown, R., & Gillespie, S. (2015). Overseas financial investigation of organised crime: Examining the barriers to effective implementation. *Journal of Money Laundering Control, 18*(3), 371.

Buisman, S. (2011). The influence of the European legislator on the National Criminal Law of member states: It is all in the combination chosen. *Utrecht Law Review, 7*(3), 137–155 .

Cappiello, S. (2015). *The interplay between the EBA and the Banking Union*. Robert Schuman Centre for Advanced studies research paper no. RSCAS 2015/77. Center for Economic Studies, Munich.

Costa, S. (2013). *Implementing the new anti-money laundering directive in Europe: Legal and enforcement issues—The Italian case*. Milan: Paolo Baffi Center on International Markets, Money and Regulation No. 2008-13.

Costanzo, P. (2013). The risk-based approach to anti-money laundering and counter-terrorist financing in international and EU standards: What it is, what it entails. In B. Unger & D. van der Linde (Eds.), *Research handbook on money laundering* (p. 352). Cheltenham: Edward Elgar.

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

de Koker, L. (2014). The FATF's customer identification framework: Fit for purpose? *Journal of Money Laundering Control, 17*(3), 281.

Della Cananea, G. (2004). The European Union's mixed administrative proceedings. *Law and Contemporary Problems, 68*, 197.

Demetriades, G. (2015). "Is the person who he claims to be?" Old fashion due diligence may give the correct answer! *Journal of Money Laundering Control, 19*, 1.

Dion, M. (2015). Is money laundering an ethical issue? *Journal of Money Laundering Control,* vol. 68 *18*(4), 425.

Dostov, V., & Shust, P. (2014). Customer loyalty programs: Money laundering and terrorism financing risks. *Journal of Money Laundering Control, 17*(4), 385.

Doukas, D., & Anderson, J. (2008). The dice is loaded: Commercial gambling and the European Court of Justice. *Oxford Yearbook of European Law, 27*, 237.

Eckes, C., & Konstadinides, T. (Eds.). (2011). *Crime within the area of freedom, security and justice. A European public order*. Cambridge: Cambridge University Press.

FAFT. (2012). *International standards on combating money laundering and the financing of terrorism & proliferation*. Paris: Financial Action Task Force.

Ferran, E. (2014). *European Banking Union and the EU Single Financial Market: More differentiated integration, or disintegration?* University of Cambridge Faculty of law research paper no. 24. Center for Economic Studies, Munich.

Fisher, J. (2010). The anti-money laundering disclosure regime and the collection of tax in the UK. *British Tax Review, 55*, 1.

Fisher, J. (2013). The global financial crisis: The case for a stronger criminal response. *Law and Financial Markets Review*, 159–166.

Fisher, J. (2015). Economic crime and the global financial crisis. *Law and Financial Markets Review*, 276–289.

Fratangelo, P. (2014). International anti-money laundering policies and the protection of financial integrity. In R. Miccù & D. Siclari (Eds.), *Advanced law for economics. Selected essays*. Turin: Giappichelli.

Fratangelo, P. (2015). Prevention and countering of money laundering and terrorism financing. In D. Siclari (Ed.), *Italian banking and financial law: Supervisory authorities and supervision* (p. 105). New York: Palgrave.

Gilmour, N., & Ridley, N. (2015). Everyday vulnerabilities—Money laundering through cash intensive businesses. *Journal of Money Laundering Control, 18*(3), 293.

Gnutzmann, H., McCarthy, K. J., & Unger, B. (2010). Dancing with the devil: Country size and the incentive to tolerate money laundering. *International Review of Law and Economics, 30*(3), 244.

Hampton, P. (2004). *Reducing administrative burdens: Effective inspection and enforcement*. London: HM Treasury Department.

Handoll, J. (2007). *Capital payments and money laundering in the European Union*. Oxford: Oxford University Press.

Herlin-Karnell, E. (2011). The EU's anti-money laundering agenda: Built on risks? In C. Eckes & T. Konstadinides (Eds.), *Crime within the area of freedom, security and justice. A European public order* (p. 76). Cambridge: Cambridge University Press.

Herlin-Karnell, E. (2014). Constructing Europe's area of freedom, security and justice through the framework of 'regulation': A cascade of market based challenges in the EU's fight against financial crime. *German Law Journal*, 49–74.

Hutter, B. (2005). *The attractions of risk based regulations: Accounting for the emergence of risk ideas in regulations*. London: Centre for Analysis of Risk and Regulation (CARR). Discussion paper DP 33, London School of Economics and Political Science (LSE).

Ioannides, E. (2014). *Fundamental principles of EU law against money laundering*. Burlington: Ashgate.

Janczuk-Gorywoda, A. (2010). The single payments area in Europe. *Columbia Journal of European Law, 16*(2), 321.

Kaburakis, A., Rodenberg, R., & Odds, M. (2011). Gambling, law, and strategy in the European Union. *Business Law International, 13*(1), 63.

Katz, E. (2007). Implementation of the third money laundering directive. An overview. *Law and Financial Markets Review, 1*(3), 207–211.

Kokert, J., & Held, M. (2014). *Payment services Directive II: Risks and serious consequences for users and banks.* BaFin Section for IT infrastructure of banks, June 2014. Center for Economic Studies, Munich.

Komárek, J. (2008). Legal professional privilege and the EU's fight against money laundering. *Civil Justice Quarterly,* 13–22.

Lavorgna, A. (2015). Organised crime goes online: Realities and challenges. *Journal of Money Laundering Control, 18*(2), 153.

Masciandaro, D. (1999). Money laundering: The economics of regulation. *European Journal of Law and Economics, 3*, 225.

Masciandaro, D. (2005). False and reluctant friends? National money laundering regulation, international compliance and non-cooperative countries. *European Journal of Law and Economics, 20*, 17.

Masciandaro, D., & Volpicella, A. (2014). *Economics and politics in designing supervision: The case of the FIUs against money laundering*. Baffi Center research paper no. 2014-156.

Masciandaro, D., Takatz, E., & Unger, B. (2007). *Black finance. The economics of money laundering*. Cheltenham: Edward Elgar.

Mendes, C., & Oliveira, J. (2013). Money laundering and corrupt officials: A dynamic model. *Journal of Money Laundering Control, 16*(1), 55.

Mitsillegas, V., & Gilmore, B. (2007). The EU legislative framework against money laundering and terrorist finance: A critical analysis in the light of evolving global standards. *International and Comparative Law Quarterly, 56*(1), 119.

Moloney, S. (2014). European Banking Union: Assessing its risks and resilience. *Common Market Law Review, 51*, 1609.

Mugarura, N. (2014). Customer due diligence (CDD) mandate and the propensity of its application as a global AML paradigm. *Journal of Money Laundering Control, 17*(1), 76.

Pellegrini, M. (2005). Anti-money laundering legislation in the light of the proposal of the third EC directive. *European Business Law Review, 5*, 1181.

Proctor, A. (2005). Supporting a risk-based anti-money laundering approach through enforcement action. *Journal of Financial Regulation and Compliance, 13*(1), 10.

Ross, S., & Hannan, M. (2007). Money laundering regulation and risk-based decision making. *Journal of Money Laundering Control, 10*(1), 106.

Ruce, P. J. (2011). Anti-money laundering: The challenges of know your customer legislation for private bankers and the hidden benefits for relationship management ('The bright side of knowing your customer'). *Banking Law Journal, 128*(6), 548.

Simser, J. (2013). Money laundering: Emerging threats and trends. *Journal of Money Laundering Control, 16*(1), 41.

Soudijn Melvin, R. J. (2014). A critical approach to trade-based money laundering. *Journal of Money Laundering Control, 17*(2), 230.

Sterling, S. (2015). Identifying money laundering: Analyzing suspect financial conduct against the speed, cost, and security of legitimate transactions. *Journal of Money Laundering Control, 18*(3), 266.

Tofangsaz, H. (2015). Rethinking terrorist financing; where does all this lead? *Journal of Money Laundering Control, 18*(1), 112.

Tsingou, E. (2014). Money laundering. In D. Mügge (Ed.), *Europe and the governance of global finance* (p. 153). Oxford: Oxford University Press.

Unger, B. (2007). *The scale and impact of money laundering*. Cheltenham: Edward Elgar.

Unger, B., & van Waarden, F. (2013). How to dodge drowning in data? Rule-and risk-based anti-money laundering policies compared. In B. Unger & D. van der Linde (Eds.), *Research handbook on money laundering* (p. 405). Cheltenham: Edward Elgar.

Usman Kemal, M. (2014). Anti-money laundering regulations and its effectiveness. *Journal of Money Laundering Control, 17*(4), 416.

Valcke, P., Vandezande, N., & Van de Velde N. (2015). *The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4*. SWIFT Institute Working paper no. 2015-001.

van den Broek, M. (2011). The EU's preventive AML/CFT policy: Asymmetrical harmonization. *Journal of Money Laundering Control, 14*(2), 170.

Vlaemminck, P., & De Wael, P. (2003). The European Union regulatory approach of online gambling and its impact on the global gaming industry. *Gaming Law Review, 7*(3), 177.

Walker, J. (1999). How big is global money laundering? *Journal of Money Laundering Control, 3*(1), 25.

Walker, J., & Unger, B. (2009). Measuring global money laundering: The Walker Gravity Model. *Review of Law and Economics, 5*(2), 821.

Williams Clifford, C. (2013). A burning desire: The need for anti-money laundering regulations in carbon emissions trading schemes to combat emerging criminal typologies. *Journal of Money Laundering Control, 16*(4), 298.

Yeoh, P. (2014). Enhancing effectiveness of anti-money laundering laws through whistleblowing. *Journal of Money Laundering Control, 17*(3), 327.