Saint Petersburg State University

***Markova Anna Vyacheslavovna***

**Final qualifying work**

«AML/CFT compliance: regulation in the European Union and the Russian Federation»

Level of education: master degree

Field 40.04.01 "Jurisprudence"

Main educational program

"VM.5848.2021 Transnational legal practice"

Scientific adviser:

Associate Professor of the Department of Labor and Social Law

Sychenko Elena Vyacheslavovna

Scientific consultant

Rogachevsky Anton Lvovich

Reviewer:

Korobova Polina Igorevna

Saint Petersburg

2023

TABLE OF CONTENTS

[INTRODUCTION 3](#_Toc133157339)

[CHAPTER 1. THE CONCEPT OF MONEY LAUNDERING 6](#_Toc133157340)

[1.1 The concept of money laundering and terrorism financing 6](#_Toc133157341)

[1.2 The role of international bodies as standard setters in the field of anti-money laundering 11](#_Toc133157342)

[CHAPTER 2. SPECIFICS OF AML/CFT REGULATION IN THE EUROPEAN UNION AND THE RUSSIAN FEDERATION 15](#_Toc133157343)

[2.1 AML/CFT regulation in the European Union 15](#_Toc133157344)

[2.2 AML/CFT regulation in the Russian Federation 28](#_Toc133157345)

[CHAPTER 3. BUILDING AN EFFECTIVE AML COMPLIANCE PROGRAM TO MEET AML COMPLIANCE REQUIREMENTS: KEY FEATURES 39](#_Toc133157346)

[CONCLUSION 58](#_Toc133157347)

[LIST OF REFERENCES 60](#_Toc133157348)

# INTRODUCTION

In the current reality, crimes in the economic sphere that pose a threat to national security are a significant concern. Among them is money laundering, which is now becoming transnational in nature. Its scale is only growing from year to year, which undoubtedly affects not only the economy of a state but also the world economy. Such acts are illegal and cause enormous damage both to individuals, organizations, and the states.

The lack of control over the movement of funds on international markets enables criminal elements to launder with impunity money derived from illicit activities at both national and international levels. The United Nations Office on Drugs and Crime (UNODC) conducted a study to determine the magnitude of illicit funds generated by drug trafficking and organized crimes and to investigate to what extent these funds are laundered. The published on October 25, 2011, report estimates that in 2009, criminal proceeds amounted to 3.6% of global GDP, with 2.7% (or USD 1.6 trillion) being laundered[[1]](#footnote-1).

This falls within the widely quoted estimate by the International Monetary Fund, which stated in 1998 that the aggregate size of money laundering in the world could be somewhere between two and five percent (**or between 800 billion and 2 trillion US dollars)** of the world’s gross domestic product[[2]](#footnote-2).

«Due to the illegal nature of the transactions, precise statistics are not available, and it is therefore impossible to produce a definitive estimate of the amount of money that is globally laundered every year»[[3]](#footnote-3). The Financial Action Task Force (FATF) therefore does not publish any further data on this. Therefore, the above estimates should be treated with caution.

The problem of combatting money laundering is urgent since the number of such crimes is significant and is causing considerable damage to economic growth. The relevance is based on the fact that at the present stage, the fight against money laundering is one of the main concerns of almost all countries in the world. That is why it is the task of states to elaborate and adopt a whole range of measures to combat money laundering. What is more, in order to comply with anti-money laundering (AML) requirements in the private sector, it is obligatory for businesses to implement effective compliance programs, which may include various aspects to be considered. Therefore, it is also important to pay attention to meeting such criteria not to be liable for non-compliance and not to bear heavy fines and other consequences as a punishment for violations of AML compliance measures.

In this connection, the aim of this work is to observe the concept of money laundering and key elements of the AML compliance program and to conduct a comparative legal analysis of the approaches to the AML/CFT regulation in the Russian Federation and the European Union.

To achieve this goal, it seems necessary to set the following objectives: define money laundering and terrorism financing, analyse, and compare the approaches to the AML/CFT regulation in the Russian Federation and the European Union, and observe elements of effective AML compliance program.

Since the topic of AML is extensive, the present paper is be limited to the following aspects. In the first chapter attention is paid to the concept of money laundering and terrorism financing, and the role of key organizations as bodies dedicated to set international standards in combatting money laundering. The second chapter examines AML/CFT regulation in the European Union and the Russian Federation respectively, with the highlight on the latest amendments in the legislation of these jurisdictions. Since EU AML legislation is aimed to set the same standards for all the Member States, it is reasonable to also review the AML/CFT regime in one of the countries of the European Union. The third chapter is dedicated to key features of an effective AML compliance program which are to be implemented by regulated businesses in order to comply with AML requirements. Particular attention will be paid to KYC and KYB procedures as these fall within the professional interest of the author of the paper.

The topic of anti-money laundering is rather developed. The topic is dealt with, in particular, in scientific papers by A.V. Kuchumov, E.V.Pecheritsa, P. Dare, S. Thornhill, A. Bastrykin, Pisarenko A.P, David Schreuders, Nosh Van Der Voort, and others. The normative base of the study consists of international instruments, such as UN Conventions, FATF Recommendations, and others, laws and regulations of the Russian Federation and the Netherlands, as well as Directives and other legal acts of the European Union.

# CHAPTER 1. THE CONCEPT OF MONEY LAUNDERING

## **The concept of money laundering and terrorism financing**

Money laundering is one of the transnational crimes that has become very widespread in the world at the turn of the 20th and 21st centuries. This type of criminal activity is multifaceted and therefore very dangerous, as it not only has a criminal law basis but also affects the normal functioning of the economy, leading to corruption, unstable financial institutions, market distortions, loss of government revenue, and other gross consequences. Moreover, this type of criminal activity often generates an even more dangerous crime for society - terrorism - as terrorist acts are financed with dirty money. This type of criminal activity is transnational and has a structurally complex crime element, which makes it difficult to qualify.

Money laundering is described as the process by which proceeds from criminal activity are disguised to conceal their illicit origin. More precisely, according to the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention), it may encompass three distinct, alternative actus reas: (i) «the conversion or transfer, knowing that such property is the proceeds of crime (ii) the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime; and (iii) the acquisition, possession or use of property, knowing, at the time of the receipt, that such property is the proceeds of crime»[[4]](#footnote-4). The United Nations Convention against Transnational Organized Crime (Palermo Convention) of 2000 and the United Nations Convention Against Corruption of 2003 collectively extended the derivative offences to money laundering offences. In this way, all three conventions have laid the foundation for the modern global anti-money laundering system[[5]](#footnote-5).

Money laundering takes a variety of forms. Criminally derived property can be laundered by using an almost infinite number of methods involving all financial services and products. To enable the complete cycle to be illustrated, whatever its form or complexity, the laundering process has been described as taking place in three stages, which are the following[[6]](#footnote-6):

a) placement: the placement of funds generated from crime into the financial system, either directly or indirectly. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location. «By using an account with a low risk, the money launderer avoids being detected by authorities»[[7]](#footnote-7).

b) layering: the process of separating illicit proceeds from their source by creating complex 'layers' of financial transactions designed to disguise the audit trail and provide anonymity. The funds might be channeled through the purchase and sale of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance. Such actions lower the chance that law enforcement detects and follows the money flow.

c) integration: the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system and appear to be legitimately earned or acquired funds.

However, it is not even necessary for criminals to use all three stages of the model in order to legitimize criminal property. Whilst the three-stage model of money laundering outlined above is a convenient way of describing the activity, it is rare for a single bank or its money laundering reporting officer to see or be able to identify all three stages related to a single case.

As technology advances, financial crime is becoming more sophisticated, and the stages are becoming more complex as criminals find new methods to prevent the detection of their activities. Regulators and institutions are finding it increasingly difficult to detect or prevent laundered money from entering financial systems[[8]](#footnote-8).

Terrorist financing involves the solicitation, collection, or provision of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both legal and illicit sources. More precisely, according to the International Convention for the Suppression of the Financing of Terrorism, a person commits terrorism financing «if that person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out»[[9]](#footnote-9) an offense within the scope of the Convention.

The primary goal of individuals or entities involved in the financing of terrorism is therefore not necessarily to conceal the sources of the money but to conceal both the financing and the nature of the financed activity.

The facilitation of the financing of prospective acts of terrorism is a different process to that of laundering the proceeds of crimes that have already occurred and, in many cases, funds used to finance terrorism will have been legally acquired or donated. In other words, money laundering is the process of making dirty money appear clean, whereas terrorist financing often involves clean money being used for criminal purposes.

However, these two crimes have several common features. Thus, «the source of laundered funds has to be disguised, just like the source and destination of money used to support terrorism; both the crimes will generally require the assistance of the financial sector; many terrorist groups derive money from criminal organizations; and many of the techniques used to disguise the destination of terrorist funds are identical to those used to launder the proceeds of crime»[[10]](#footnote-10).

It is also important to mention such crimes as financing of proliferation (or proliferation of weapons of mass destruction). These acts should be understood as the transfer and export of nuclear, chemical, or biological weapons, their means of delivery, and related materials. «The interconnection is based on the fact that proliferation might be a means for supporting the undertaking of terrorist activities. Its disruption is therefore essential for the prevention of terrorist acts. Moreover, the practical undertaking of proliferation financing often uses the same channels as terrorist financing. Measures to be applied in order to disrupt proliferation financing would therefore often be similar to the measures applied to counter terrorist financing»[[11]](#footnote-11). Since financing proliferation is considered an integral part of terrorism financing, in further research financing proliferation should be presumed when mentioning terrorism financing.

In October 2022 European Union Agency for Criminal Justice Cooperation (Eurojust) published a report on money laundering, providing an overview of the legal and practical issues to be expected and possible solutions[[12]](#footnote-12). The most relevant challenge in the anti-money laundering sphere is accurate qualification. Thus, money laundering is often not considered a stand-alone offence, but is imputed in addition to some other offences, which are called predicate offences. Predicate offence means a component of a more serious crime. For example, kidnapping, narcotics trafficking, and other relevant crimes may be considered a predicate offence to money laundering. Such predicate offences enable offenders to accumulate the funds to be laundered. Due to the lack of harmonization in identifying it properly, proceedings become more complicated. Moreover, in some jurisdictions, money laundering may be identified as tax fraud, which makes the investigations more difficult to prosecute and for judicial cooperation. As a consequence, such cases are not easy to investigate, and even more difficult to prove the fault of offenders for committing money laundering.

As the report states, a lack of cooperation between the states leads to complication in prosecutions. Since the report is made by Eurojust, it reviewed mainly the AML situation in the EU. Thus, cases of money laundering are manageable within the EU, however, when cooperation is required outside of the Union, it becomes difficult to investigate such cases and sometimes authorities discontinue the pursuit of such cooperation[[13]](#footnote-13).

Also, the usage of cryptocurrencies has become a problem in recent years, which makes it difficult to keep track of the assets held by those under investigation. It is essential to know the activity and mechanisms used to monetize or convert cryptocurrency into legal tender.

Notwithstanding the above, the importance of identification of ultimate beneficial owners (UBOs) cannot be ignored. As was mentioned above, criminals are always trying to find new ways to launder money and to hide all the financial trails, and therefore the use of shell companies or letterbox companies, identification of extraneous elements in the companies’ structures, or act under different names complicates the process of finding true beneficiaries of business under investigation.

The listed above examples of issues in money laundering only several key challenges that the repost specified, but they are the ones indicating how money laundering is evolving, how it is important to focus on such a problem, and how many complex issues are still to be resolved in the future.

## **The role of international bodies as standard setters in the field of anti-money laundering**

For a long time, the international community has recognized the need for cooperation at the international level in the fight against organized crime, including money laundering. As such, many international organizations have contributed to the development of standards and legislation, good practices for regulated (or obliged) entities in the area of money laundering and terrorism financing. They are also taking the lead in identifying trends and emerging threats in this area. As the range of financial products is growing incredibly fast these days, this provides almost unlimited opportunities for criminals to launder illicit funds. Thus, the role of international bodies as standard setters is significant since it is highly important to implement the recommended measures into national legislation and policies of regulated entities in order to prevent money laundering.

In the context of the United Nations’ efforts to prevent and combat terrorism, the United Nations Office on Drugs and Crime (UNODC) has an expanded program of work for technical assistance to counter-terrorism. This is based on mandates recommended by the UN Commission on Crime Prevention and Criminal Justice and approved by the UN General Assembly. These mandates include the provision of assistance and advisory services to countries to combat terrorism. Consequently, UNODC's operational activities focus on strengthening the legal regime against terrorism.

As a part of the UNODC, The United Nations Global Programme against Money Laundering (GPML)[[14]](#footnote-14) assists member states to set up legislation against money laundering in full compliance with international legal instruments, develop and maintain strategies to combat money laundering, encourage AML policy development, raise public awareness about money laundering, and act as a coordinator of joint AML initiatives by the UN with other international organizations.

Notwithstanding the importance and influence of the UN Conventions relating to anti-money laundering (AML) mentioned in paragraph 1.1 above, the efforts of the Financial Action Task Force (FATF) have been most important in strengthening the international AML regime. For more than thirty years, the Financial Action Task Force, a specialized international organization, has been working effectively to combat money laundering and the financing of terrorism. It is the most important and influential of the international bodies in AML and CFT. The FATF was established in 1989 at the G7 meeting in Paris with the participation of the European Commission[[15]](#footnote-15). The creation of the FATF was a response to the increased volume of laundered money around the world.

In April 1990 the FATF issued a report containing a set of Forty Recommendations, which were intended to provide a comprehensive plan of action needed to fight against money laundering.

Shortly after the attacks on the US on September 9, 2001, the FATF placed action to combat terrorism and terrorist financing on an equal footing with preventing money laundering, which therefore led to the comprehensive revision of the FATF standards. In October 2004 the FATF published additional IX Special Recommendations, further strengthening the agreed international standards for combating money laundering and terrorist financing.

In February 2012, the FATF completed a thorough review of its standards and published the revised FATF Recommendations[[16]](#footnote-16). This revision is intended to strengthen global safeguards and further protect the integrity of the financial system by providing governments with stronger tools to act against financial crime. They have been expanded to deal with new threats such as the financing of proliferation of weapons of mass destruction, and to be clearer on transparency and tougher on corruption. The IX Special Recommendations on terrorist financing have been fully integrated with the measures against money laundering.

The FATF currently consists of 37 Member states and 2 regional organizations, representing most major financial centers in all parts of the globe, which are the European Commission and the Gulf Co-operation Council[[17]](#footnote-17). All FATF members, including members of FATF-style regional bodies, undertake to implement the FATF anti-money laundering and counter-terrorism Recommendations as part of their membership obligations. With that said, over 200 jurisdictions have undertaken obligations to implement the FATF Recommendations into their national legislation, and in some cases implementing effective risk-based policies against money laundering, terrorism financing, and financing of proliferation of weapons of mass destruction[[18]](#footnote-18). However, such implementation cannot be mandatory, and all members will approach their obligations in different ways, and under different timetables.

Special attention should be paid to the International Monetary Fund (IMF) as an international body whose aim is to fight against money laundering. Since its main goal is to promote economic stability, the IMF provides technical assistance to many countries to enable AML/CFT frameworks to be developed. What is more, IMF completes the assessment of member countries’ compliance with international standards, such as FATF 40+9 Recommendations[[19]](#footnote-19). Thus, unlike the FATF, the IMF does not intend to set international anti-money laundering standards. Instead, it has a significant role in evaluating the compliance of the member states with such standards[[20]](#footnote-20).

The World Bank is also one of the main international bodies which combats money laundering. Its Financial Integrity Program provides countries with tools for increasing transparency and for going after the “dirty money” to reinforce the strength, safety, and integrity of the financial system[[21]](#footnote-21). Working on the international level with FATF, UN, G20, many regional organizations, national AML/CFT-relevant authorities, and civil societies, the Financial Integrity unit has achieved significant results in implementing the standards aimed to combat money laundering in national legislation and policies of the regulated entities.

The role of the EU institutions, such as the European Commission, the Council, and the European Parliament, has been highly important in setting off and promoting AML/CFT improvement through member states by issuing AML Directives, which are required to be implemented into the national legislation of EU member states. By such implementation, the FATF Recommendations are implemented across the Union, harmonizing the legislation of all the member states in this field. However, such implementation may take a long time and therefore may be regarded as a disadvantage of such a process[[22]](#footnote-22). More precisely EU AML Directives will be discussed in Chapter 2 below.

The Wolfsberg Group is an association of thirteen global banks that aims to develop frameworks and guidance for the management of financial crime risks[[23]](#footnote-23). Notwithstanding that, this institution has no official status, and its standards are not binding even on its own members, its statements of good practice have received international recognition throughout the financial sector[[24]](#footnote-24). Starting from 2000, alongside Transparency International (which is a civil society with national chapters that played an important role in promoting anti-corruption conventions and in monitoring their application in practice)[[25]](#footnote-25), the Wolfsberg Group has published a significant number of documents, whether in the form of Principles, Guidance, Frequently Asked Questions or Statements. The main goal of that institution, among others, is to promote engagement between private and public sectors in the field of combatting illicit financial activity, which is highly important.

Having considered the concepts of money laundering, terrorist financing, the list of the main international instruments regulating this area, and the key international organizations involved in combating money laundering, it can be concluded that the problem is complex. Although combating money laundering is a global priority and that many resources are focused on preventing instability in the international financial system, criminals still manage to find loopholes to carry out their criminal intentions. In addition, advances in technology also have a major impact. Therefore, certain threats to the international financial system appear constantly, and all countries have to participate in their prevention.

# CHAPTER 2. SPECIFICS OF AML/CFT REGULATION IN THE EUROPEAN UNION AND THE RUSSIAN FEDERATION

## **2.1 AML/CFT regulation in the European Union**

Combating money laundering and terrorist financing is a key priority for the European Union since it contributes to global security, the integrity of the financial system, and sustainable growth. Accordingly, the EU creates laws, such as the EU Anti-Money Laundering Directives (AMLD), to prevent the misuse of the financial market to commit these crimes. Such AMLDs are considered primary sources of anti-money laundering regulation in the EU.

The EU periodically publishes amended versions of Anti-Money Laundering Directives for its member states, which are required to implement them as part of their domestic legislation.

The first AML Directive was agreed on 10 June 1991 and it was as much a rhetorical tool as a policy directive, enjoining Member States to take the problem of AML seriously. Although Member States had responsibilities under such instrument, a solely national approach, «without taking account of international coordination and cooperation, would have very limited effects»[[26]](#footnote-26). The FATF Recommendations, which entered into force earlier, were a basis for the directive. Thus, the directive imposed certain obligations on Member States on elements of the private sector deemed best placed to act as ‘gatekeepers’ for the financial system. Member States were required to legislate to ensure that such regulated entities undertook consistent Customer Due Diligence (CDD) and Know Your Customer (KYC) procedures at onboarding, as well as on later stages in certain intervals, and kept records of the relationship up to five years after it had ended. What is more, such financial organizations were required to monitor the operations of such clients, identify suspicious activities, and inform national authorities.

Notwithstanding that the directive was a positive first step to identify and mitigate a problem of anti-money laundering that had been largely ignored as a major policy issue in Europe until the late 1980s, it was obvious that it needed further review.

The second EU AML Directive was agreed on in December 2001[[27]](#footnote-27), and its primary aim was to fill the gaps in the first directive identified over the previous decade. For instance, it was amended that suspicious reporting needed to be reported to a dedicated national Financial Intelligence Unit (FIU); from that second directive, the term financial institution was extended and included not only banks, as it was before. Thus, financial institutions also included Money Service Bureaus (MSBs), known collectively as “Non-Banking Financial Institutions” (NBFIs), as well as designated non-financial business and professions (DNFBPs), which could be involved in financial transactions.

The third AML Directive[[28]](#footnote-28), which was adopted in 2005, was primarily dedicated to combat against terrorism. As the FATF revised its Recommendations considering new responsibilities as the international standard setter for Countering the Financing of Terrorism (СFT) as well as AML, creating nine Special Recommendations on terrorist financing. These new Recommendations shaped the relevant CFT content and history of 3AMLD, including due diligence measures to ensure obligated entities were not providing services to designated terrorists or terrorist groups.

In addition to terrorism, the 3AMLD extended AML to other sectors, such as casinos and external accountants. Also, a risk-based approach was introduced, which allowed the application of CDD measures to vary based on the risk profile of the client, its product, and other factors. Thus, depending on the client, it could be required to undergo Simplified Due Diligence (SDD) or Enhanced Due Diligence (EDD) approaches.

With the need to motivate the regulated entities, the 3AMLD also introduced effective, proportionate, and dissuasive penalties and sanctions for AML/CFT violation[[29]](#footnote-29). Nevertheless, the 3AMLD has referred issues of liability for breaches of AML/CFT standards to Member States.

For a long time, the issue of AML/CFT was not dealt with at the EU level. This is usually attributed to the fact that the consequences of the 2007-2008 Global Financial Crisis, and other issues were being dealt with. However, the moment for amending AML legislation came in 2015 when the EU initiated a new wave of AML/CFT activity, leading to the relatively rapid creation and implementation of three other AML Directives.

In addition to the perception that AML has been dormant for too long, a number of other factors have catalyzed this process. Such factors were a growing recognition of the pace of money laundering sophistication and typologies and the need for specific financial measures to counter the growing threat.

Rapid advances in technology have given added impetus. Not only has it become easier for criminals to move money quickly with faster payment technologies, but there are also opportunities for financial institutions and DNFBPs to use their own data and increasingly available external data streams to combat financial crime using new types of regulatory technology.

The next fourth AML Directive was adopted in 2015 and provided a more detailed guidance on taking a risk-based approach (RBA) in the implementation of CDD. It also extended the scope of AML obligations, including new regulated entities, that were not included in this list previously, such as gambling organizations. What is more, cash transactions of more than 10,000 euros became subject to AML regulation[[30]](#footnote-30), even though it was categorized by the Member States as a challenge to implement it in practice.

The other important point that the 4AMLD covered is the requirement to disclose the ultimate beneficial owners (UBOs) of the company. It was made in order to put a new emphasis on creating more transparency around structures launderers could use to hide the proceeds of bribery, corruption, and tax evasion. Thus, «Member States shall ensure that the companies registered in their territory hold adequate, accurate and current information about UBOs»[[31]](#footnote-31). Such information should be published in the central or public register of the Member State, and it should be ensured that information in the registered named above is accurate and current.

Moreover, the 4AMLD continued to impose EDD measures on politically exposed persons (PEPs), while expanding the scope of the term to include not only foreign nationals but domestic politically linked individuals as well.

The fifth AMLD came just over a year later, on July 9, 2018, and was shaped by countering terrorism financing concerns, as Europe had faced several Islamic terrorist attacks. One important element of the directive was aimed at reducing the financial capacity that perpetrators used to commit terrorist attacks.

In line with the desire to expand the obligations of previous directives, 5AMLD also expanded the range of obligated entities to include art traders, estate agents, services similar to auditors, external accountants, and tax advisors.

Moreover, providers engaged in exchange services between virtual currencies and fiat currencies were also included, making a step forward in regulating crypto assets on the European level in terms of the AML. Therefore, AML/CFT measures, such as CDD, suspicious activity reports (SARs), record keeping, and appropriate controls became a necessity for such types of businesses. Thus, the 5AMLD brought more transparency and trustworthiness to the industry that probably needed it the most. Under the directive, virtual currencies are «a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically»[[32]](#footnote-32).

Since the anonymity of virtual currencies may be used potentially for criminal purposes, it was decided that, in order to combat such anonymity, «national Financial Intelligence Units (FIUs) should be able to obtain information allowing them to associate virtual currency addresses to the identity of the owner of virtual currency»[[33]](#footnote-33). Moreover, under the respective directive regulated crypto businesses should register with the applicable national authority, these are, for instance, the Financial Market Authority (FMA) in Austria and the Swiss Financial Market Supervisory Authority (FINMA) in Switzerland[[34]](#footnote-34).

What is more, the 5AMLD established a new approach that should be applied when interaction with high-risk third countries takes place. It means that regulated entities should conduct EDD to protect the company from the dangers that come with the vulnerability of such regulations. It should be complied with in order to stop money laundering-related funds from entering the financial market of the European Union, and therefore the Member States should be cautious and limit their engagement with high-risk regions. Such additional measures that should be taken if the transaction includes such a high-risk third country counterparty, are: «obtaining additional information on the customer and its UBOs, their source of funds and source of wealth, information on intended nature of the business relationship, approval of senior management for establishing or continuing the business relationship, conducting enhanced monitoring of the business relationship»[[35]](#footnote-35).

Moreover, the directive added further detail to its transparency agenda by requiring national UBO registries to become available to the general public, without the need to prove the legitimate interest, as it was stipulated previously. However, despite the focus on achieving transparency in the EU, on 22 November 2022, the European Court of Justice (ECJ) published its judgment[[36]](#footnote-36), which was particularly significant in the context of AML. It was decided that open public access to the beneficial owner registers of EU member states companies is no longer valid since it is in contravention of articles 7 and 8 of the Charter of Fundamental Rights of the European Union[[37]](#footnote-37) (the Charter).

The court upheld the claim related to joined cases of Sovim SA and WM, who is not named publicly. The latter plaintiff claimed that because of his position, he had to travel frequently to countries with unstable political regimes and high crime rates. According to WM, because of this, the disclosure of personal data poses a significant risk of him being kidnapped or even murdered.

The 4AMLD established that public registers could publish information on UBOs to the ones, who could demonstrate legitimate interest, such as corruption, tax crimes, and fraud[[38]](#footnote-38). It was later amended by the 5AMLD, and since that date, Member States were required to make the beneficial owner registers fully accessible to the general public without the need to demonstrate a legitimate interest in order to more effectively prevent the use of the financial system for the purpose of money laundering and terrorist financing. In accordance with this provision, data on the UBO included «at least the name, the month and year of birth and the country of residence and nationality of the beneficial owner as well as the nature and extent of the beneficial interest held»[[39]](#footnote-39), with the addition that Member States may provide additional information enabling the identification of the beneficial owner.

Based on the court decision, giving access to the personal data of the ultimate beneficial owners constitutes a serious interference with the fundamental rights to respect for private life and to the protection of personal data enshrined in Articles 7 and 8 of the Charter, such as respect for private and family life and protection of personal data.

The possibility of access to the personal data of the UBOs by an unlimited number of persons may lead to the fact that such information may be freely accessed by the persons who seek to find out about the material and financial situation of UBOs[[40]](#footnote-40). Furthermore, such data may not be only accessed, but also retained and disseminated and that, in the event of such successive processing, it becomes increasingly difficult for those data subjects to defend themselves effectively against abuse.

Thus, in the event that a Member State continues to publish such data and the UBO requests to classify such information about itself, it will be able to invoke the EU Court of Justice judgment in a national court, and probably receive compensation for the country's failure to follow the judges’ opinion.

Even though that decision recognizes the legitimate interest in accessing beneficial ownership information, it was criticized by journalists, anti-corruption, and transparency organizations[[41]](#footnote-41). Such a decision of ECJ further restricts the already limited access to public interest information on businesses, complicates the access to the data on UBOs for the purposes of anti-money laundering and has already led to the immediate closure of the registers in some countries, such as Luxembourg, and the Netherlands. What is more, it is not yet clear whether the AMLD can be further amended to allow public access in situations outside of a legitimate interest.

The Covid-19 pandemic put enormous pressure on financial services, leading to a review of EU anti-money laundering regulations in late 2020, which resulted in the adoption of the sixth EU anti-money laundering directive (6AMLD). The pandemic has intensified the drive to digitize financial services. «While digitization is generally seen as a benefit, at the same time it gives cybercriminals the opportunity to evolve and expand their methods of financial crime»[[42]](#footnote-42). The 6AMLD was launched quickly enough to address these growing threats.

Thus, the latest directive on AML/CFT in the EU brought a series of amendments to the European legislation in order to strengthen the financial system of the European Union from being used for money laundering and terrorism financing.

The major amendment that was stipulated by the 6AMLD is the severe criminalization of money laundering. The directive extended the list of predicate offences, among which are kidnapping, smuggling, fraud, and others, including to that list cybercrimes and environmental crimes[[43]](#footnote-43). Also, the money laundering term expended also to the laundering of property as well as the acquisition, concealment, and distribution of all physical and virtual assets stemming from illegal activities.

What is more, 6AMLD established that not only individuals should be liable when committing money laundering, but also legal entities should bear the consequences of participation in such a criminal activity. Sanctions for legal entities under the directive are fines (which may be criminal or non-criminal), placing under judicial supervision, a judicial winding-up order, temporary or permanent closure of establishments, and others[[44]](#footnote-44). These new rules apply also if the regulated entity failed to implement effective AML policies, therefore making senior management accountable for any resulting money laundering. Also, 6AMLD makes liable everyone associated with the crime. For instance, individuals who cooperated in hiding assets or who knew about money laundering keeping silence can now face punishment. For serious violations, prison sentences are set at a minimum of four years.

It is important to mention that the «6AMLD is unarguably the toughest measure that the EU has ever put forward to deter money laundering and makes the potential consequences for not only committing the crime – but also helping or even allowing it to happen – potentially disastrous for individuals and businesses alike»[[45]](#footnote-45). Therefore, it is essential that not only Member States should implement new provisions into national legislation, but they should also ensure that the regulated entities comply with them, making such businesses review their AML policies and compliance programs as a whole.

Generally, Member states had some time for implementation of such directives in their national legislation. As was stipulated, the 6AMLD should have been integrated by December 3, 2020. However, such a deadline may be not reached by some countries. For instance, Cyprus enacted the previous directive (5AMLD) on February 18, 2021, when the deadline was a year before that, and the following failure resulted in Cyprus receiving a letter of formal notice by the European Commission[[46]](#footnote-46).

It is important to note that, based on the previous major changes in EU AML legislation, the focus on the AML itself in the EU is a key priority. Thus, it is expected, that the regulation of AML will only evolve in the future.

For instance, the European Commission proposed to establish a new agency, Anti-Money Laundering Authority (AMLA)[[47]](#footnote-47), which main aim will be supervision in the EU and enhance cooperation among financial intelligence units. As it comes from the proposal, it will be the central authority coordinating national authorities to ensure the private sector correctly and consistently applies EU rules. However, AMLA is not responsible for monitoring and tackling money laundering in the EU, as it remains one of the national authorities’ prerogatives. Nonetheless, AMLA is monitoring and supporting the correct application of EU regulations and directives across the continent. AMLA will also be empowered to supervise and impose penalties on financial institutions whose national supervisor is unable or unwilling to take remedial action[[48]](#footnote-48). However, it is not yet clear when it will be created and accordingly become fully operational.

In order to have a closer look at the national legislation of EU counties, the Netherlands could be suggested as one of the examples of efficient AML regulation implementation. The Netherlands is an attractive location for businesses these days, and it is a leader in technology and innovation and has a competitive business climate. Notwithstanding the above, legal entities that wish to enter the market of this country must be aware of the AML/CFT regulations, which are considered rather strict. For instance, when 5AMLD was implemented by the Netherlands, their version was so rigid that it put the country’s crypto sector in crisis.

On August 24, 2022, the FATF published a Mutual Evaluation Report dedicated to the Netherlands’ compliance with the FATF standards[[49]](#footnote-49). Overall, the report considered the Netherlands’ compliance positively. For instance, the Netherlands is well aware of the risks it faces and has developed robust risk-based policies and strategies to address them. What is more, there is strong cooperation between the Dutch financial intelligence unit (FIU-NL) and law enforcement agencies, as well as with their international partners. In the Netherlands terrorist financing, primarily involving the funding of foreign terrorist fighters, is also successfully detected, investigated, and prosecuted. However, the FATF recommends to the Dutch authorities to pay more attention «to prevent legal persons from being used for criminal purposes, strengthen risk-based supervision, and ensure sanctions for money laundering and terrorist financing offences are proportionate and dissuasive»[[50]](#footnote-50). Based on the report, the Netherlands was considered as compliant with 10, largely compliant with 28, and partially compliant with 2 of the FATF Recommendations[[51]](#footnote-51).

The main legislative instrument in the AML field in the Netherlands is the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft). Since the Netherlands is one of the members of FATF, it should be noted that its legislation is mainly influenced by the FATF Recommendations. Moreover, the national legislation is based on the AML/CFT Directives of the EU, therefore most provisions of the Dutch legislation do not essentially differ from the EU directives. Thus, the obligation of the regulated entities to perform CDD, KYC, KYB, transaction monitoring, record keeping, suspicion transactions reporting, adverse media, and sanctions screening, in accordance with the risk-based approach, do not vary significantly.

Under the current Dutch legislation, the regulated businesses are banks, businesses providing crypto services, exchanges, insurances, electronic money institutions, and some other businesses[[52]](#footnote-52). It should also be mentioned that not only legal entities should be obliged to comply with the AML requirement, but also civil-law notaries, lawyers, and tax advisors are required to conduct such activities[[53]](#footnote-53). These organizations are constantly receiving and transferring money and other valuables in their activities. They must therefore keep a close eye on customer transactions and operations in order to prevent illegal schemes.

There are several regulators in the Netherlands. The main one is The Authority for the Financial Markets, known as the Autoriteit Financiële Markten (AFM), which supervises the whole financial market sector. It may conduct inspections of the Netherlands’ financial institutions, and issue warnings, file reports, and impose fines to enforce regulations, if necessary[[54]](#footnote-54). The other key regulator is De Nederlandsche Bank (DNB), which operates alongside the AFM, often sharing information with each other to mitigate risks of money laundering in the Netherlands. Among other things, the DNB monitors the financial health of the country’s financial institutions. What is more, The Financial Intelligence Unit (FIU) of the Netherlands is the central institution, to which regulated entities should report suspicious transactions. According to the general rule laid down by the Wwft, occasional transactions of at least 15,000 euros should be the basis of additional investigation of the customer[[55]](#footnote-55).

Under the Ditch Criminal Code (Wetboek van Strafrecht) there are several types of money laundering, which are «money laundering with intent (Article 420bis), habitual money laundering (Article 420ter), culpable money laundering (without intent) (Article 420quater), and "simple" money laundering, which is money laundering that solely consists of acquiring or possessing an object that derives directly from an offence committed by oneself (Article 420bis.1 and Article 420quater.1)»[[56]](#footnote-56). As for the financing of terrorism, it is considered an umbrella term for various illegal acts. Unlike the money laundering, the main challenge of terrorism financing is the purpose for which the money is used, rather than the origin of the funds/assets.

Criminal offences in the Netherlands may be contributed to both individuals and legal entities. Thus, the maximum imprisonment for both the money laundering and terrorism financing for individuals established is 8 years, following the potential fine up to the fifth category[[57]](#footnote-57), which is 90,000 euros. Individuals may be also removed from the profession, and they could be denied some of the civil rights, like running for public office for committing money laundering.

As for the legal entities, it should be proved that the offence is attributable to such a legal entity. It depends on the criminal offence committed by the employees of the legal entity, and whether the offence took place in the field of activity of the legal entity. The relevant circumstances are as follows: «whether the offence was committed by the employee, it was made beneficial for such entity, whether the offence was allowed to be committed by the legal entity, and other relevant circumstances»[[58]](#footnote-58). Under the Dutch Criminal Code, the potential maximum of fine to the legal entities may rise to 900,000 euros. However, if this amount will not be considered appropriate, a fine of 10% of annual turnover may be imposed on the legal entity which committed money laundering. It should be noted that the Netherlands has not implemented 6AMLD into their own legislation, therefore amendments relating to the criminal liability of legal entities are expected to be faced in the future.

As for the administrative liability for non-compliance with AML legislation of the Netherlands, Article 31 of the Wwft indicates, that fines of 10,000 euros may be imposed on the regulated entities. In case of repeated offences in the period of 5 years, the maximum fine imposed could rise to 10,000,000 euros[[59]](#footnote-59). However, if this amount will not be considered appropriate, an administrative fine of 20% of annual turnover may be imposed on the legal entity for non-compliance with AML legislation.

For instance, on 18 January 2023 DNB, which is the Netherlands’ central bank, imposed €3,325,000 administrative fine on Coinbase Europe Limited (Coinbase)[[60]](#footnote-60). Under the 5AMLD, which was implemented in the legislation of the Netherlands with the publishing of the Wwft, crypto businesses are required to register with DNB[[61]](#footnote-61). However, for a period of almost 2 years, Coinbase did not obtain such registration. Due to the absence of registration, Coinbase could not report unusual transactions to FIU-Netherlands during the non-compliance period and until 22 September 2022, when the registration finally took place. Therefore, «a large number of unusual transactions may have gone unnoticed by the investigative authorities during this period»[[62]](#footnote-62).

Even though it may seem that AML legislation is over-regulated, there are still a lot of gaps in law to review and decide on. As fraud techniques continue to evolve, notably the recent creation of so-called deep fakes, regulators will have to incorporate additional layers of security in the nearest future to filter out identity fraudsters and enhance due diligence. The emergence of new threats, such as the use of artificial intelligence, may occur. Although regulators have not yet identified it as potentially dangerous, artificial intelligence and similar technologies are likely to be included in future reviews. That said, artificial intelligence could be used to identify fraudulent transactions, suspicious activity, and false positives more accurately.

So, for any business operating in the EU, it remains vital to stay aware and ahead of the requirements that might be placed upon them by new AMLDs or new regulatory instruments. It is also essential for the senior management of the regulated entities to be sure that their businesses are ready for such changes and are able to react without undue delay.

## **2.2 AML/CFT regulation in the Russian Federation**

«Counter-terrorism, corruption, as well as prevention of shadow entrepreneurship, the basis of which, in particular, consists of legalization (laundering) of proceeds of crime, play an important role in the system of comprehensive measures to ensure the national security of the Russian Federation»[[63]](#footnote-63). All these negative phenomena are global threats to the development of the country.

In the early 2000s, the Russian Federation had no effective legal and institutional framework for combating money laundering and terrorist financing[[64]](#footnote-64). However, in recent years, Russia has made a confident breakthrough in the legal regulation of the aforementioned relations. Currently, the main law that stipulates AML/CFT standards is Federal Law “On Combating Money Laundering and the Financing of Terrorism” N 115-FZ dated 7 August 2001 (hereinafter, 115-FZ), which entered into force on February 1, 2002.

Article 5 of 115-FZ specifies, which entities, as well as some types of sole entrepreneurs, should be considered as regulated entities. Such are, for instance, credit institutions, professional participants in the securities market, insurance companies, telecommunications operators, organizations, and individual entrepreneurs that provide intermediary services for real estate purchase and sale transactions (estate agents)[[65]](#footnote-65). The same approach is followed in the EU, as has been established in the case of the Netherlands. As these institutions and individuals are faced with financial transactions, it is necessary for them to detect suspicious transactions in time, as well as to carry out risk assessments of their clients.

There are several regulators in Russia, which supervise the compliance with the AML/CFT requirements of the regulated entities. The main authority in this sphere is the Federal Financial Monitoring Service, or Rosfinmonitoring, which conducts financial intelligence investigations, monitors transactions of regulated entities, cooperates with international authorities, and has many more obligations. It is considered as the financial intelligence unit of the Russian Federation. The other key authorities that are obliged to monitor compliance with AML legislation in the Russian Federation are the Central Bank of Russia, which regulates the activities of credit institutions and non-credit financial institutions, reducing the level of money laundering and terrorism financing in the financial sector.

As specified in clause 1 of article 6 of the 115-FZ, a transaction should be subject to mandatory control if the amount of such transactions equals or exceeds 1 million rubles, or the equivalent of this amount in foreign currency[[66]](#footnote-66).

The criminal liability for individuals is specified in articles 174 (the legalization (laundering) of funds and other property acquired by other persons illegally) and 174.1 (the legalization (laundering) of monetary funds or other property acquired by a person as a result of an offence committed by him) of the Criminal Code of the Russian Federation. As both articles establish the same penalties for the commitment of such crimes, a fine for an ordinary corpus delicti is up to 120,000 rubles or in the amount of the wages or other income of the convicted person for a period of up to one year, and if there are qualifying elements of the crime, the punishment can be up to seven years imprisonment and a fine of 1 million rubles or in the amount of the wages or other income of the convicted person for a period of up to five years[[67]](#footnote-67). As for the financing of terrorism, it is punishable by imprisonment for five to fifteen years with a fine of up to five hundred thousand rubles or in an amount of the wages or other income of the convicted person for a period of up to three years or without such a fine[[68]](#footnote-68).

One of the latest cases of money laundering in Russia is the following. On April 27, 2023, a criminal case has been launched against Elena Blinovskaya. She is suspected of committing crimes, such as tax evasion on a particularly large scale, legalization (laundering) of money on a particularly large scale, or other property acquired by a person as a result of a crime. «According to investigators, Blinovskaya, providing information services through the Internet, using a "split" business scheme, understated the income received and failed to pay value-added tax and personal income tax for the period 2019-2021 for a total amount of over 918 million rubles»[[69]](#footnote-69). In addition, in order to give the appearance of lawful possession, use, and disposal of the funds received, she legalized them by carrying out financial transactions. Since the investigation has only started, the development of this case is expected. Due to the large sum of funds, the penalty for Blinovskaya might be rather decent.

Since the Criminal Code of the Russian Federation stipulates that criminal liability may be imposed only for individuals, legal entities are only subject to administrative liability in the event of a violation of the AML legislation of the Russian Federation.

The Code of the Russian Federation on Administrative Offences contains several articles, which impose liability for non-compliance with AML legislation. The key article is 15.27, which specifies certain corpus delicti. Under this article, for instance, if the financial institution fails to develop internal control rules and (or) appoint special officers responsible for implementing internal control rules, such an institution should bear a warning or an administrative fine for officials in the amount of ten thousand to twenty thousand rubles; for legal entities in the amount of one hundred thousand to two hundred thousand rubles[[70]](#footnote-70). For other cases of non-compliance, officials could be disqualified, and legal entities’ activity could be suspended for a period of 90 days. Under article 15.27.1, which stands for the financing of terrorism and proliferation of weapons of mass destruction, a maximum fine of 60 million rubles could be imposed on legal entities[[71]](#footnote-71).

On September 1, 2022, came into effect article 15.27.3 (engaging in transactions or financial operations with criminally obtained assets for the benefit of a legal entity) of the Code of the Russian Federation on Administrative Offenses[[72]](#footnote-72). The scope of such a crime is to give lawful status to the possession, use, and disposal of the money or other property in question. Only legal entities could be punished in accordance with that article since the responsibility for individuals for such an offence is stipulated by the Criminal Code of the Russian Federation. Transactions with criminally obtained property will be punishable by a fine of up to three times the amount of money or property that is the subject of the administrative offence, or administrative suspension of activities for up to 30 days. In addition to any of these main penalties, confiscation of the object of the offence - illegally obtained money or other property - may be imposed[[73]](#footnote-73).

Attorneys and notaries may be subject to disciplinary liability, in accordance with the codes of professional ethics for attorneys and notaries respectively, which could even include suspension of the respective status.

Comparing the penalties for being non-compliant with the AML legislation in the Netherlands and Russia, certain conclusions could be made. Although the term of imprisonment under the Russian law for offences is rather high, especially regarding the financing of terrorism, attention must also be paid to fines, both in administrative and criminal proceedings, as they are significantly lower than under the Dutch law. The imposition of a fine on a person or organization should be a preventive measure against breaking the law and should be an incentive not to commit such offences.

Notwithstanding the decent fines, which may be imposed on organizations, violation of the AML requirements specified by 115-FZ by organizations conducting transactions with funds or other assets and acting based on a license, could lead to the revocation (annulation) of such a license[[74]](#footnote-74).

An example of non-compliance with AML/CFT requirements in Russia can be seen in the revocation of the license of Joint Stock Company Conservative Commercial Bank (CCB). On 11 February 2022, the Central Bank of the Russian Federation ruled by Order No. OD-283[[75]](#footnote-75) that CCB violated federal laws governing banking activities and Bank of Russia regulations, and also committed violations of anti-money laundering and counter-terrorist financing legislation.

CCB specialized in providing e-commerce services as a settlement bank for the WebMoney transfer system[[76]](#footnote-76). CCB did not investigate the economic substance of customer transactions, and the sources of funds were not transparent[[77]](#footnote-77). It was found that the credit institution's activities were characterized by increased risks of involvement in servicing shadow gambling businesses and illegal financial market participants.

Despite the revocation of the license, on the same day, $30.7 million was withdrawn from the bank to a Cypriot company, Northforce Limited, which subsequently led to criminal proceedings under Article 172 (“Illegal banking activities carried out on a particularly large scale”) of the Russian Criminal Code[[78]](#footnote-78). Following that, the General Prosecutor's Office of the Russian Federation filed a lawsuit to seize ten billion rubles from the owners of CCB Andrei Trubitsyn and his wife as a result of laundering illicit proceeds[[79]](#footnote-79).

As to the recent innovations in AML regulation in Russia, from July 1, 2022, the “Know Your Customer” platform (the KYC platform) went live in Russia[[80]](#footnote-80), which aims to reduce the burden on bona fide entrepreneurs and save the resources of financial institutions, which could focus on preventing suspicious transactions. It is a centralized platform of the Bank of Russia, to which all banks within the country are already connected. This platform will categorize legal entities and individual entrepreneurs according to risk levels. Legislative changes related to the appearance of the KYC platform are reflected in clauses 7.6-7.8 of 115-FZ.

The Central Bank will send information on risk levels to banks. However, it should be noted that the information from this platform is supporting, and financial institutions may not use this platform and take risks into account independently in accordance with their internal control rules.

According to the innovations, legal entities and individual entrepreneurs will be assigned a status - green, yellow, or red (accordingly, low, medium, or high) - depending on the degree of risk. If clients are in the green group, transactions between them should be unhindered. If both the bank and the regulator give the client a "red" rating, the bank must immediately impose a ban on almost all its operations. The bank must warn the client that it has been assigned a high-risk rating and explain the measures that are being taken against it. If the customer does not agree with the decision to be placed in the red group, this decision can be appealed. If the decision is not appealed, the company or individual entrepreneur will be forcibly removed from the registers of legal entities and individual entrepreneurs at the request of the Central Bank[[81]](#footnote-81).

On 17 December 2019, the FATF published Mutual Evaluation Report dedicated to AML/CFT compliance in the Russian Federation[[82]](#footnote-82). The report showed that Russia is compliant with 7, largely compliant with 28, and partially compliant with 5 FATF Recommendations[[83]](#footnote-83), which does not differ much from the result, which was obtained by the Netherlands. Even though Russia has developed its legislation in order to comply with the FATF standards, has strengthened its understanding of risks of money laundering and terrorism financing, and has delivered concrete results in its activity in developing AML compliance within its territory since the previous assessment conducted in 2008, there were still identified some of the key issues that Russia faces.

Russia has made a step forward in understanding its weak point, such as commitment to crimes within its territory, such as corruption, abuse of power, fraud in the financial sector, and being both the transit and destination point of narcotics trafficking. A large proportion of criminal proceeds generated in Russia are laundered abroad, which makes the pursuit of proceeds of crime to other countries an important focus. However, the FATF discovered that Russia still needs to improve «its ability to freeze, without delay, assets linked to terrorism, financing of terrorism and proliferation of weapons of mass destruction, and ensure that this freezing obligation extends to all natural and legal persons»[[84]](#footnote-84).

It is essential to understand that «the high-risk group includes the most frequently used ML methods and tools, such as the use of front/ shell companies, the use of non-resident legal persons and arrangements, trade-based ML through fictitious economic activity abroad, people affiliated with public officials, the misuse of electronic payments and virtual currencies, and cash operations»[[85]](#footnote-85). It is notable that, most of the identified methods and tools involve moving funds out of Russia illicitly to further launder those funds abroad. Therefore, Russian authorities should focus on the investigation and prosecution of complex money laundering cases, especially concerning money being laundered abroad.

Regarding the financial sector, Russia has enhanced the supervision of the banking sector and has now reduced the risk that financial institutions may be owned or controlled by criminals. However, sanctions against banks that do not comply with anti-money laundering and counter-financing of terrorism requirements seem not effective and dissuasive.

Therefore, even though the improvement in the legislation and compliance with anti-money laundering itself has been obtained, there are still more challenges that should be resolved by the Russian authorities.

However, notwithstanding the positive assessment of compliance with the FATF Recommendations, in March and June 2022, the FATF published statements on the Russian Federation, limiting its role and influence within the organization. «The Russian Federation can no longer hold any leadership or advisory roles or take part in decision-making on standard-setting, FATF peer review processes, governance and membership matters. The Russian Federation can also no longer provide assessors, reviewers or other experts for FATF peer-review processes»[[86]](#footnote-86).

Moreover, on February 24, 2023, the FATF published a landmark statement concerning the Russian Federation. It was stated that «the Russian Federation’s actions unacceptably run counter to the FATF core principles aiming to promote security, safety, and the integrity of the global financial system. They also represent a gross violation of the commitment to international cooperation and mutual respect upon which FATF Members have agreed to implement and support the FATF Standards»[[87]](#footnote-87). Due to that reason, the FATF suspended the membership of the Russian Federation in the organization. Notwithstanding that decision, Russia remains accountable for its obligation to implement the FATF Standards and must continue to meet its financial obligations.

It is important to note that in the suspension statement, the FATF does not state that it automatically places the Russian Federation on the blacklist. Jurisdictions, that are on the blacklist of the FATF, do not cooperate with this organization and fail to implement its recommendations on money laundering and terrorist financing. Currently, 3 countries are considered high-risk jurisdictions, which are Democratic People’s Republic of Korea, Iran, and Myanmar[[88]](#footnote-88).

What is more, the FATF did not also move the Russian Federation to the “grey list”, which specifies jurisdictions under increased monitoring. Generally, placing jurisdiction under increased monitoring means that it undertook to promptly resolve the identified strategic deficiencies within an agreed timeframe. As for now, such countries are, for instance, Gibraltar, Panama, South Africa, Turkey, and some others[[89]](#footnote-89).

By these statements, the FATF warns other countries that «all jurisdictions should be alert to possible emerging risks from the circumvention of measures taken in order to protect the international financial system and take the necessary measures to mitigate these risks»[[90]](#footnote-90).

Since the publishment of these statements, some countries have implemented additional measures in assessing funds and clients themselves, which come from the Russian Federation, such as completing enhanced due diligence procedures in relation to the clients during the onboarding, accounts freezing or even closing. As the latest example, one of the largest banks in the UAE, Emirates NBD, started transferring the assets of Russians to separate accounts where all payments on securities belonging to them will be transferred[[91]](#footnote-91). Russian citizens, which are not residents of the EU, the European Economic Area, or Switzerland will not be able to withdraw funds from such accounts.

Seeking to mitigate the risks of Russian involvement in the financial systems of the countries, some assess with more scrutiny the clients with a Russian background. For instance, the Bank of Cyprus started to close the accounts to Russian tax residents, to the ones who have income from a sanctioned business in Russia, as well as F-type residence permit holders, i.e. those who obtained it in connection with the purchase of real estate in the country[[92]](#footnote-92). In addition, account closure notices are sent to Russians who are in Cyprus on a tourist visa.

The issue described above has been present for a certain period in different countries. However, it might be only the beginning, since the process of account closures is likely to start in many countries, as even "friendly" Russian states not only try to avoid secondary sanctions, which may be imposed on them but also apply their risk assessment procedures on the customers with Russian passports.

Under the review of the AML legislation in different jurisdictions, such as the European Union as a whole, with reference to the Netherlands’ AML/CFT regime, and regulation in the Russian Federation, it is possible to make certain conclusions.

Even though it may seem that AML legislation in both the EU and Russia is over-regulated, there are still more loopholes, that should be further reviewed. With the constant improvement in technology, criminals will always have the opportunity to find new ways to commit financial crimes. The advancement and adoption of artificial intelligence, deep fake technology, cryptocurrencies, and many other innovations make the fight against money laundering and terrorist financing much more comprehensive. It is therefore essential that the financial sectors of states are prepared to counter the commission of such crimes and to preserve the integrity of the financial system. Thus, more amendments to the AML legislation are expected in order to fight new challenges that may occur in this field.

The fact that all the general principles and standards are of the responsibility of the FATF, and all of the EU countries and the Russian Federation are members of this organization, which have the basis of FATF Recommendations to be implemented in the national systems of the countries. On the EU level are issued AML Directives, which should be further incorporated in the legislation of the Member States. Therefore, AML Directives also include general provisions, that should be later detailed by the Member States. Due to the same foundation, the general principles in AML regulation (which are risk assessment, reporting suspicious transactions, customer due diligence, and others) in countries of EU and Russia are the same. The differences in the approaches of the reviewed jurisdictions are only in detail, like criminal liability for legal entities, the penalties for non-compliance with the AML requirements, amount of transaction which requires detecting, and other particulars. There are in fact some novelties, such as new AML authority and landmark decision on UBO registries in the EU, a new centralized KYC platform for banks in Russia, and others.

However, the results of the implementation of norms, and building AML systems in different jurisdictions may vary significantly. Even though, as was stated by the FATF Mutual Evaluations, the Netherlands and Russia are almost on the same level of compliance with the FATF Recommendations, it may be not enough to build an effective compliance model due to the various challenges and risks that these jurisdictions may face.

As for now, the Members States of the European Union and other jurisdictions must apply additional measures in order to mitigate risks, that are referred to Russia due to the suspension of its membership in the FATF in order to prevent the international financial system from such jurisdiction.

With that said, the international financial system faces various challenges, which come from innovations in technology, political situation in different jurisdictions, and other important factors, on an ongoing basis. Therefore, enhancement of the AML/CFT regulation are likely to be expected.

# CHAPTER 3. BUILDING AN EFFECTIVE AML COMPLIANCE PROGRAM TO MEET AML COMPLIANCE REQUIREMENTS: KEY FEATURES

Since money laundering is a complex challenge that is faced by the whole world, it is essential that not only public institutions should be involved in its combatting. The private sector should take its part in complying with Anti-Money Laundering (AML) standards and regulations, which should be implemented by the regulated entities. Such private institutions and businesses are primarily the ones who are involved in money laundering schemes since illicit funds are placed in them. Therefore, it is highly important for regulated businesses to be aware and to participate in anti-money laundering activities.

AML is a series of measures and procedures carried out by financial institutions and other regulated entities to prevent financial crimes. AML compliance is mandatory for regulated entities under AML/CFT regulations. The scope of regulated entities varies across jurisdictions. Usually, these include financial and credit institutions, insurance companies, e-money and payment institutions, gambling service providers, and other regulated entities. All the efforts of these businesses to enforce the regulations they are obliged to comply with constitute the AML compliance program of these businesses.

An AML compliance program is a set of policies, practices, measures, procedures, and controls related to the prevention and reporting of money laundering and terrorist financing. An AML compliance program should ensure that an institution is able to detect suspicious activities associated with money laundering, including tax evasion, fraud, and terrorist financing, and report them to the appropriate authorities. An AML compliance program should focus not only on the effectiveness of internal systems and controls developed to detect money laundering but on the risk posed by the activities of customers and clients with which an institution does business.

An AML program should be built on a strong foundation of regulatory understanding and overseen by personnel who are experienced and knowledgeable enough to create a climate of compliance at every level of the organization.

Companies that fail to meet compliance obligations are subject to large fines. According to the Finbold’s Bank Fines 2020 report[[93]](#footnote-93), authorities around the world issued $14.21 billion in AML fines, with three large US banks, Goldman Sachs, Wells Fargo, and JP Morgan Chase accounting for over half of that total.

As an example, in April 2021, ABN AMRO Bank N.V. (ABN AMRO) announced a settlement offer from the Dutch Public Prosecution Service (DPPS)[[94]](#footnote-94). Before that, DPPS investigated ABN AMRO's non-compliance with its obligations under the Dutch Anti-Money Laundering and Counter-Terrorist Financing Act. Based on this investigation, it was discovered that ABN AMRO had certain failures in AML processes, such as the client acceptance, transaction monitoring, and client exit processes (the “Client Life Cycle” processes) in the period between 2014 and 2020. As part of this settlement, ABN AMRO agreed to pay a fine of 300 million euros and 180 million euros as disgorgement, which reflects how serious such failures in compliance were.

AML compliance programs include various complex processes that vary depending on the specifics of the company. If the program works well, companies can grow their business in a safe environment without fearing consequences from legal authorities[[95]](#footnote-95). What is more, they’ll be well protected from financial criminals and more attractive to customers thanks to a stronger reputation. The following features described below are based on FATF Recommendations.

***AML Policies and internal controls***

To defend the market from criminal enterprises, corrupt public officials, and terrorists, governments came up with a countermeasure, which is defensive regulatory AML and Know Your Customer (KYC) policy that should be adopted by all financial businesses. «Internal policies may vary depending on the type and size of a particular financial institution and the scope and nature of its operation need to be in place»[[96]](#footnote-96).

Anti-money laundering policy is a combination of measures used by a financial institution to stop the reintroduction of the proceeds of illegal activities. The implementation of such rules is mandatory and overseen by regulatory authorities. The AML policy may include definitions of money laundering and terrorism financing, reasons why the policy is necessary, commitment to the company KYC appropriately, commitment to regular audits, and other important information. The measures that could be stated in the AML compliance program are described further.

AML policy is often a combination of the FATF Recommendations and locally introduced laws. The location of a business determines its regulatory authority that oversees the implementation of the appropriate controls and issues fines for non-compliance.

An AML compliance program should focus on the internal controls and systems the institution uses to detect and report financial crime. The program should involve a regular review of those controls in order to measure their effectiveness in meeting compliance standards. Internal controls should be focused on mitigating risks discovered in a money laundering risk assessment. Organization should ensure to implement a comprehensive, compliant internal controls program built around the company’s unique risk profile.

Internal controls extend to an institution’s employees, who should be aware of their own roles and responsibilities within the system, how to conduct due diligence on business interests, and how to navigate policies and procedures which ensure compliance on an ongoing basis.

***Appointment of the AML Compliance Officer***

AML compliance programs should appoint a designated principal AML compliance officer who is responsible for overseeing the general implementation of AML policy within their institution[[97]](#footnote-97). AML Compliance Officers should have sufficient experience and authority within their institution to ensure they can perform their duties effectively. Those duties include communicating with authorities and auditors, briefing senior management, and making AML policy recommendations based on audits and reports. The practical duties of AML Compliance Officers include also ensuring compliance with current AML regulations, and other relevant legislation; keeping and maintaining records of high-risk customers and reporting suspicious activities to the authorities; overseeing and implementing an ongoing AML training program for other employees.

An AML Compliance Officer’s primary professional focus falls on the internal systems and controls that their institution puts in place to help detect, monitor, and report money laundering activities to the authorities. Their job is to ensure that their institution is not exposed to criminal risk and does not inadvertently facilitate financial crime.

In any context, an AML Compliance Officer’s expertise should extend beyond regulatory procedure, to the details and methodologies of the financial crimes they are charged with detecting and reporting.

***AML Training for employees***

Training and education of all relevant employees within a financial institution have a critical role in the successful implementation of any risk-based approach to managing potential money laundering risks. Usually, employees are the first ones who deal with all suspicious activities and their decision-making is crucial in situations of high risk. Therefore, companies should provide ongoing training for those who have AML-specific responsibilities and deal with transactions and accounting. This will keep such employees aware of the relevant legal obligations when dealing with high-risk customers. «All relevant employees must be aware of and understand the legal and regulatory environment in which they operate, including relevant money laundering prevention provisions, as well as the financial institution's own measures to give effect to their risk-based approach»[[98]](#footnote-98).

***Risk-based approach***

Companies need to evaluate risks related to their customers, products, services, and location. Employees, agents, and third-party vendors should be the subject of scrutiny as well. Specifically, companies need to distinguish high-risk customers and update risk profiles regularly. Thus, risk management is an ongoing process that is kept under regular review.

Adopting a risk-based approach implies the adoption of a risk-management process for dealing with money laundering and terrorist financing. This process encompasses recognizing the existence of the risks, undertaking an assessment of the risks, and developing strategies for managing and mitigating the identified risks.

A risk-based approach can therefore be summarized as covering the following areas:

«*risk identification* *and assessment*, which are identifying the money laundering risks facing an institution (including related legal, regulatory, and reputational risks), given its customer, product, and services profile and having regard to available information, and assessing the potential scale and impact of the risks; *risk mitigation*, or identifying and applying effective measures to mitigate the material risks emerging from the assessment; *risk monitoring* - putting in place management information systems and keeping up to date with changes to the risk profile through changes to the business or to the threats; and *documentation*, which stands for documenting the risk assessment and strategy and having policies and procedures that cover the above and achieve effective accountability, from the board and senior management down» [[99]](#footnote-99).

It is considered that AML/CFT risk-based strategy and assessment must be individually tailored to a particular organization. However, there are several general issues that need to be taken into consideration. In identifying its money laundering risk and in establishing the nature of these systems and controls, an organization should consider a range of factors. Such factors may include, for instance, its customers, products and activity profiles, distribution channels, complexity and volume of its transactions, processes, and systems[[100]](#footnote-100).

***Customer Due Diligence (CDD)***

Customer Due Diligence (CDD) refers to the act of collecting identifying information to verify a customer’s identity and more accurately assess the level of criminal risk they present. At a basic level, CDD requires firms to collect a customer’s name and address, information about the business in which they are involved, and how they will use their account. In order to ensure that customers are being honest, companies should then verify that information with reference to official documents such as driving licenses, passports, utility bills, and incorporation documents.

CDD is a foundation of the Know Your Customer (KYC) process, which requires companies to understand who their customers are, their financial behavior, and what kind of money laundering or terrorism financing risk they present. All FATF member states must implement CDD requirements as part of their domestic AML/CFT legislation – as set out in Recommendation 10 of the FATF’s 40 Recommendations[[101]](#footnote-101).

CDD is required during the onboarding of new customers (i.e. set of legal procedures which businesses must conduct before working with a new customer), occasional transactions, money laundering suspicion, unreliable documentation, and ongoing monitoring[[102]](#footnote-102).

The CDD procedure has several steps to complete. Firstly, the customer should be verified. Then, businesses should choose between regular, enhanced, and simplified due diligence based on what they know about a customer. The last step is ongoing monitoring - due diligence needs to be continuous as there’s always a chance that a customer’s profile changes over time. For instance, they can be included in a PEP list, initiate a high-risk transaction, or their ID is no longer valid. Since CDD is the foundation of the KYC process, the step of verifying the customer is described further.

In circumstances posing a low money laundering risk, some regulators allow conducting a simplified check, known as Simplified Due Diligence (SDD). It is not always required for every consumer to go through the full verification process. SDD is a good solution for low-risk customers, such as well-known public enterprises and individuals with reliable sources of funds[[103]](#footnote-103). SDD doesn’t skip over any of the essential CDD steps, but it does allow businesses to reduce the time and extent of the verification process.

On the other hand, Enhanced Due Diligence (EDD) may be required for persons or situations that present a greater risk. It may be applied to customers «connected to high-risk countries, politically exposed persons (PERs), for a correspondent banking and similar relationship»[[104]](#footnote-104). The Interpretive Note to Recommendation 10 FATF also lists several circumstances, which may also include application of the EDD measures, which are, for instance: «a business relationship conducted in unusual circumstances – e.g., unexplained geographic distance between the firm and customer; non-resident customers, or those subject to economic sanctions; legal persons or arrangements that are personal asset-holding vehicles; companies that have nominee shareholders or shares in bearer form»[[105]](#footnote-105).

EDD measures generally involve a more intensive level of CDD scrutiny, including requirements to obtain additional customer identification materials, establish the source of funds or wealth, and apply closer scrutiny to the nature of the business relationship or purpose of a transaction[[106]](#footnote-106).

***Know Your Customer (KYC)***

AML obligations include the Know Your Customer (KYC) process, which enables firms to identify their customers and understand their financial behavior. Given the proximity of the terms KYC and AML, however, and the fact that they are often used interchangeably, it can be difficult to understand how they differ in a regulatory context.  AML is an umbrella term for the range of measures, controls, and processes that firms must put in place to achieve regulatory compliance. By contrast, KYC is a part of AML and refers specifically to how firms establish and verify their customers’ identities and monitor their financial behavior.

KYC also gets confused with CDD. The main difference between these two concepts is that CDD applies to all regulations, while the meaning of KYC can slightly differ from jurisdiction to jurisdiction.

The term KYC describes the measures and controls that businesses must put in place to verify the identities of their customers and clients before and during a business relationship. The term can also reference the range of regulated bank practices that are used to verify clients’ identities.

Most banking institutions, credit companies, insurance agencies, crypto businesses, and gambling platforms that offer their services constantly require customers to provide personal information as part of the KYC process. That information is used to establish their identities, inform compliance risk assessments, and ensure that those customers are not involved in financial crimes such as corruption, bribery, money laundering, and terrorism financing.

However, KYC can be also useful for businesses that aren’t subject to AML regulations, such as marketplaces and carsharing platforms. It can help filter out suspicious individuals as well as risky suppliers and platforms.

As the global cost of money laundering rises, KYC policies evolve to better detect criminal methodologies and prevent illegal transactions. Accordingly, effective KYC protects both financial service providers from costly compliance penalties, criminal liability, and reputational damage, and the individual customers that might otherwise be harmed by financial crime.

Under Anti-Money Laundering obligations, businesses must also ensure that customers are trusted individuals (not fraudsters or under sanctions). This can be done by сhecking global sanctions lists, watchlists, blocklists, or adverse media.

Generally, the KYC process involves the collection and verification of a range of identifying information from customers including name, address, and date of birth. It may also include ongoing transaction monitoring and a range of customer screening measures, including politically exposed person (PEP) screening, sanctions screening, and adverse media screening.

The KYC process should take place during onboarding to ensure that customers are being truthful about who they are. The identity verification process should involve an assessment of a customer’s personal information.

KYC should also take place throughout the business relationship in order to establish that a customer’s risk profile continues to match the firm’s previous assessment of them. This includes checking that documents haven’t expired and detecting suspicious transactions.

Proper KYC verification should include several steps, which include:

**Identification**, which is requesting that the customer provides their personal data. For instance, in the Netherlands the documents and data shall at least include[[107]](#footnote-107):

a. for natural persons, not being beneficial owners (i) the surname, first names, date of birth, address, and place of residence or place of business of the client as well as of the person acting on behalf of a such natural person, or a copy of the document containing a personal identification number and based on which the verification of identity took place; (ii) the nature, number and date and place of issue of the document by means of which the identity has been verified;

b. for natural persons, being beneficial owners (i) the identity, including at least the surname and first names of the beneficial owner; and (ii) the data and documents gathered based on the reasonable measures taken to verify the identity of the beneficial owner.

In Russia, this list includes surname, first name, and patronymic (if applicable), nationality, date of birth, identity document details, details of documents confirming the right of a foreign citizen or stateless person to reside in the Russian Federation, address of residence (registration) or place of stay, taxpayer identification number (if available)[[108]](#footnote-108).

**Verification** is aimed to check that the customer is who they say they are. This includes determining that the customer’s documents are authentic and current. This step may include AML screening to check whether the customer is absent in adverse media, sanctions lists, PEP lists, etc.

**Address verification** checks whether the customer actually resides in their selected country by checking utility bills, bank statements, or other proof of address documents. This includes checking whether the customer comes from high-risk countries or countries under increased monitoring.

**Liveness check**, which stands for the verification that the customer is a real and living person. This can be done through facial biometrics authentication, which may include fingerprints, voice, and face, and comparing it to a pre-existing database[[109]](#footnote-109). For instance, the German regulator Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), which is considered one of the strictest regulators, suggests several methods for verifying a person’s identity, with video identification being a distinctive feature of the regulator. Thus, the main requirements for video identification are as follows: specially trained employees to conduct such procedure, video identification must be conducted in real-time and without interruptions; end-to-end encrypted channels for video chat must be applied to ensure safety and privacy; the need for high-quality images for the employee to check the provided ID document and its optical security features[[110]](#footnote-110).

**The final step is risk assessment, which** determines the risk category of the customer based on the results of the above checks. Depending on the calculated risk level, businesses adjust their approach to the customer’s verification. The results of a risk assessment should help a financial institution determine a customer’s risk profile, and make predictions about their future financial behavior. Businesses may also use a customer’s established risk profile to consistently monitor their account activity, and better detect transactions that seem unusual or suspicious. Accordingly, a higher risk score will necessitate additional checks, such as ongoing transaction monitoring and a range of customer screening measures, including politically exposed person (PEP) screening, sanctions screening, and adverse media screening, while lower-risk customers may receive the minimal necessary scrutiny.

***Know Your Business (KYB)***

Know Your Business is a related concept to KYC. The difference from KYC lies in the purpose and intentionality of the process, which is focused on **[identifying](https://www.electronicid.eu/en/blog/post/identity-verification/en%22%20%5Ct%20%22_blank)companies and suppliers.**

Fraud and money laundering are growing threats to the B2B (Business-to-Business) industry. In 2021, «98% of B2B retailers, manufacturers, and marketplaces had experienced financial losses due to successful fraud attacks»[[111]](#footnote-111). Therefore, most **B2B** companies need to carry out due diligence to **identify the business they work with** and fight money laundering and other tax crimes, in addition to ensuring that they work with organizations with **security and guarantees**. Even so, on the great majority of occasions, as in the financial sector, such as banks, it is a **mandatory requirement of legal KYB AML compliance.** In addition, companies must analyze and verify the business and financial information of their partners from all over the world. In this way, companies protect themselves from document fraud and guarantee transactions' security.

The concept of KYB is reasonably innovative. In 2016, the US’ Financial Crimes Enforcement Network (FINCEN) addressed the AML blind spot by introducing Know Your Business rules in its Customer Due Diligence Requirements for Financial Institutions[[112]](#footnote-112). Other global regulators subsequently introduced similar regulations: the EU’s 5th Anti Money Laundering Directive (5AMLD), for example, emphasized KYB processes, with the adopted the EU’s 6th Anti Money Laundering Directive (6AMLD) set to increase the penalties and punishments for KYB non-compliance.

Know Your Business has the [same objective](https://www.w2globaldata.com/what-does-it-mean-to-know-your-business-kyb/) as KYC in the sense that it is a way for obligated entities to assess and understand the AML/CFT risk that new and existing business relationships pose. The KYB process should enable firms to examine the entities that they are dealing with and help them to determine whether they are authentic or are being used to conceal the identities of owners for illegitimate purposes.

Accordingly, KYB should focus on [ultimate beneficial ownership](https://complyadvantage.com/insights/ultimate-beneficial-owner/) (UBO) in order to reveal who is benefitting from the financial activities of suspect businesses. Ultimate beneficial owners are those natural persons who directly or indirectly own more than 25% (in some jurisdictions, 10-20%) of shares of the company or otherwise exercise significant control over it[[113]](#footnote-113). It is highly important since criminals or other high-risk individuals may set up businesses in low regulation, offshore jurisdictions in order to deal anonymously with legitimate businesses in other parts of the world and avoid the scrutiny of standard AML/CFT measures. Similarly, firms must know whether a business, or its employees, are subject to international sanctions, have been exposed to political corruption, or have been the subject of news reports that could indicate they are involved in criminal activity.

To comply with KYB requirements, firms should assess the level of risk that their business relationships present and deploy a proportionate AML response, involving some or all of the following controls:

**Due diligence**. Firms should perform suitable due diligence on the businesses with which they have relationships in order to collect information that identifies the company. Such information may include the company name, registration number, registered office address, and other relevant data. For instance, in the Netherlands the relevant data at least includes (i) the legal form, statutory name, trade name, address with premises number, postal code, place of business, and country of registered office; (ii) if the company is registered with the Kamer van Koophande (which is the state company registry in the Netherlands), the registration number with the Kamer van Koophande and how the identity has been verified; (iii) for those acting for the company or legal entity at the institution: the surname, first names and date of birth[[114]](#footnote-114).

In the Russian Federation, the following data of the legal entity should be provided: company name, legal form, taxpayer identification number or code of the foreign organization, information on available licenses to carry out activities subject to licensing, domain name, index of the website page on the Internet, using which the legal entity renders services (if any); in addition, (i) for legal entities registered in accordance with the legislation of the Russian Federation, also Principal State Registration Number and address of the legal entity; (ii) for legal entities registered under the laws of a foreign state, also the registration number, place of registration and address of the legal entity in the territory of the state in which it is registered[[115]](#footnote-115).

It is also important to collect and verify company documents, such as a certificate of incorporation to prove the legal existence of the company, proof of registered office address, and documents disclosing control structure (board members/ directors). Also, the ultimate beneficial owners (UBOs) of the company should be verified. To do so, documents disclosing beneficial ownership structure are to be provided. Subsequently, those identified UBOs should be verified based on KYC rules. Where there is an increased AML risk, firms should perform enhanced due diligence, subjecting businesses to an increased degree of AML scrutiny. Firms may refer to a range of official and private resources in order to conduct KYB checks, such as publicly available government registries.

**Transaction monitoring**. Certain transactional behaviors may indicate that a business is involved in money laundering or terrorist financing activity. Unusual frequencies or volumes of a transaction, transactions just under-reporting thresholds, or transactions with high risk countries often represent money laundering red flags.

**Sanctions screening**. Firms should screen businesses and their employees against international sanctions lists such as the OFAC, the UN, and the EU sanction lists.

**PEP screening**. Businesses that are exposed to political corruption may present an increased level of money laundering risk. Accordingly, firms should screen businesses to establish their politically exposed person (PEP) status.

**Adverse media monitoring**. Firms should monitor businesses for their involvement in adverse or negative news media stories that might indicate their involvement in criminal activity. The monitoring process should be ongoing and include traditional screen and print media and online sources.

KYB goes beyond the need to establish UBO and should be considered an **ongoing AML process**. This means that firms must conduct KYB throughout a business relationship, regularly checking businesses against sanctions lists, for political corruption exposure, and for any other indication that they might be involved in financial criminal activity.

***Reporting suspicious activity***

In accordance with international standards, financial institutions and designated non-financial businesses and persons (DNFBPs) have an obligation to put in place procedures, systems, and controls to ensure that their employees recognise and report circumstances where they suspect or there are reasonable grounds to know or suspect that their products or services are being used for the purposes of money laundering or terrorist financing or that a firm's clients are involved in money laundering or terrorist financing[[116]](#footnote-116). Such institutions and persons must report that information in a timely manner to their jurisdiction’s financial intelligence unit (FIU).

It would be impossible for governments to catch all the criminals involved in money laundering independently, and the same can be said for businesses and financial institutions. But when both the private and public sectors cooperate in order to combat this ubiquitous crime, their success rate dramatically increases.

The FATF 40 Recommendations recognise two different approaches to reporting. The first relates to reporting suspicions - referred to as a “Suspicious Activity Report” (SAR) or “Suspicious Transaction Report” (STR). The second is not universally applied and requires routine reporting of transactions above a specified threshold - this is known as currency transaction reporting. Even though currency transaction reporting is not included as a principal requirement, the Interpretive Note to Recommendation 29 FATF states that «countries should consider the feasibility and utility of a system where financial institutions and DNFBPs would report all domestic and international currency transactions above a fixed amount»[[117]](#footnote-117). As was mentioned in the previous chapter, as a general rule, regulated entities in the Netherlands should additionally investigate the customer if the occasional transaction exceeds 15,000 euros[[118]](#footnote-118). In Russia, by default, mandatory control should be imposed on the transactions of more than one million rubles or its equivalent in the foreign currency[[119]](#footnote-119).

The first stage of the suspicious activity reporting process is the responsibility of the onboarding or transaction team. A subjective conclusion must be reached that there are grounds for suspicion of money laundering, terrorist financing, or sanctions breaches concerning a particular client or matter.

The escalation process should then lead to the money laundering officers, who can determine whether the report should be escalated externally. This decision should be communicated to the onboarding and compliance teams before it’s escalated to the external authorities[[120]](#footnote-120).

Usually, a suspicious activity report will incorporate detailed information on the company and the incident to advance the investigation. Such information includes the type of activity of the company; the type of suspicious transaction (currency exchange, cash conversion, remittance, use of foreign bank accounts, purchase of goods, gaming activities, use of shell companies, etc.); the volume and currency of the transaction; the alleged jurisdiction where the money came from; the origin of the money; the security measures taken and other important information regarding such suspicious activity.

When a SAR has been filed, each institution should have a specific policy and process to follow. Staff responsible for contacting customers should receive training and fully understand the responsibility of not “tipping off” the customer about a possible SAR filing, since some states consider such acts as criminal offences[[121]](#footnote-121). Additionally, firms must observe local data protection and legislative requirements. Financial institutions cannot mention a SAR, whether they are considering filing one or having filed one.

***Record keeping***

To demonstrate how much control compliance teams have over the onboarding process, it is required to secure and accessible records. These records are the essential evidence in the audit trail of any money laundering or terrorist financing investigation and are to include information on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit the reconstruction of individual transactions (including the amounts and types of currency involved, if any) to provide, if necessary, evidence for the prosecution of criminal activity.

It is required to keep all relevant information of the client[[122]](#footnote-122), such as client identification and verification documents, information on the transaction, customer due diligence prepared during the onboarding process, printouts that identify whether the client is sanctioned, a politically exposed person (PEP), or the subject of any adverse media, any information secured on the client’s source of wealth and source of funds, and other relevant information.

While there is no definitive set of record-keeping requirements for every business type, there must be enough documentation that underpins a firm’s onboarding process to demonstrate why a specific client was onboarded and what steps they went through. The length of time firms must retain this information depends on local laws and regulations. According to FATF, the term of record-keeping should be for at least five years after the business relationship is ended, or after the date of the occasional transaction[[123]](#footnote-123). The period of 5 years from the termination of the customer relationship is also applicable under the Russian[[124]](#footnote-124) and Dutch law[[125]](#footnote-125).

It is also required to keep records about the formal risk-based assessment, anti-money laundering, counter-terrorist financing, and sanctions compliance policies. Any changes to these policies must be recorded.

To make the AML compliance program effective, it is important to create a solid compliance culture. This helps identify and reduce money laundering risks and leads to more effective compliance solutions. A company with a solid AML culture takes the initiative in combating money laundering at all levels of management. Thus, senior management won’t underestimate the importance of AML compliance, and AML-responsible employees won’t see compliance as a burden. Therefore, having a strong compliance culture within a company will prevent a company from infringement of AML laws and subsequently sanctions for such offences.

What is more, it’s much more convenient for companies to use new technologies for AML compliance, since manual verification can be much more time-consuming and may lead to mistakes, which can be much more costly than using an artificial intelligence (AI)-powered solution[[126]](#footnote-126).

It is also important to mention that the effectiveness of a particular AML compliance program is determined in the process of independent audits[[127]](#footnote-127). If the company successfully complies with all required regulations (while avoiding the administrative burdens of over-compliance and the legal dangers of under-compliance), the program can be considered successful. Therefore, companies should constantly evaluate the effectiveness of their measures in meeting compliance standards.

Institutions that have implemented and maintained effective AML compliance programs have likely placed significant importance on getting the governance framework right. This means that «they have the full commitment of their boards of directors and senior management teams to the AML compliance effort; that AML roles and responsibilities have been clearly delineated for all key players in the company; and that the company places a high value on compliance and backs up its commitment by aligning its performance and incentive systems with its compliance goals»[[128]](#footnote-128).

In a globalised and liberalised trade and economy, the fight against money laundering has justifiably been declared an international threat due to the fact that manipulative mechanisms against public order are created for money laundering and the increasing power of organised crime leads to the erosion of institutions of key importance to society[[129]](#footnote-129). In addition, given market forces, a vicious chain of increasingly illegal practices for profit is detrimental to fair competition.

Accordingly, financial institutions must constantly establish effective processes to detect and prevent dirty money from entering the financial system. Money laundering has many economic, socio-economic, and business consequences if AML rules are not developed and applied.

To conclude, AML compliance isn’t just another regulatory burden. It’s designed to create a safe business environment beneficial for both financial institutions and their customers. But it’s not enough to simply create an AML compliance program; it is essential to keep it up to date, which is a time-consuming process.

# CONCLUSION

The problem of combatting money laundering is urgent since the number of such crimes is significant and is causing considerable damage to economic growth. That is why it is the task of states to elaborate and adopt a whole range of measures to combat money laundering. Having reviewed in this paper the concepts of money laundering and terrorism financing, and the role of international bodies as standard setters in combatting money laundering, it is possible to conclude that the AML system is developing on an ongoing basis. Not only do criminals find new ways to launder illegal finds, but also legislation in this sphere develops constantly, and the innovations in combatting the above-mentioned crimes are evolving. Combating money laundering and terrorist financing is a key priority for the whole world and international organizations since it contributes to global security, the integrity of the financial system, and sustainable growth.

Even though it may seem that AML is over-regulated, there are still many loopholes, that should be further reviewed. With the constant improvement in technology, criminals will always have the opportunity to find new ways to commit financial crimes. The advancement and adoption of artificial intelligence, deep fake technology, use of cryptocurrencies, and many other innovations make the fight against money laundering and terrorist financing much more comprehensive. It is therefore essential that the financial sectors of states are prepared to counter the commission of such crimes and to preserve the integrity of the financial system.

Comparing the AML legislation in the EU with the example of the Netherlands, and the Russian Federation, the following conclusions could be made. Since both legislations are based on the international standards established by the FATF, the general principles of AML measures that are to be taken are rather the same. However, certain differences in the implementation (such as the amount of penalties imposed for non-compliance with AML requirements, criminal liability for legal entities, and the amount of the transaction to be monitored, required data to be provided by the customer, etc.) are minor. However, the results of such implementation differ due to the various reasons, including political factors.

Even though, as was stated by the FATF Mutual Evaluation Reports, the Netherlands and Russia are almost on the same level of compliance with the FATF Recommendations, it may be not enough to build an effective compliance model. FATF made certain recommendations to these jurisdictions, such as to ensure that the punishments are dissuasive and proportionate and to pay more attention to the assessment of the risks that are attributable to the jurisdiction, such as corruption, political involvement in money laundering and schemes of transferring of the illicit funds abroad.

As for now, the Members States of the European Union and other jurisdictions must apply additional measures in order to mitigate risks, that are referred to Russia due to the suspension of its membership in the FATF in order to prevent the international financial system from such jurisdiction.

Notwithstanding the effectiveness of the measures that are on the international and national levels, it is also essential for private businesses to participate in anti-money laundering activities. To comply with anti-money laundering requirements in the private sector, it is obligatory for the regulated businesses to implement effective compliance programs, which may include various aspects to be considered. Therefore, it is important to pay attention to meeting such criteria to ensure that the company will not be liable for non-compliance and not to bear heavy fines, be suspended in operations, that license will not be revoked as a punishment for violations of AML compliance measures.

Since private businesses are primarily the ones who are involved in money laundering schemes since the illicit funds are placed in them, they should pay a lot of attention to prevent such events. Thus, to make the AML compliance program effective, it is highly important to implement all the necessary measures and conduct them with scrutiny. Therefore, it is essential to ensure that all the elements of the AML compliance program, such as risk assessment, transaction monitoring and reporting, record keeping, and completing verifications of the clients, and other elements, work efficiently.

With that said, the international financial system faces various challenges, which come from innovations in technology, the political situation in different jurisdictions and other important factors, on an ongoing basis. Therefore, improvements of the AML/CFT regulation are likely to be expected.

# LIST OF REFERENCES

1. UNITED NATIONS CONVENTION AGAINST ILLICIT TRAFFIC IN NARCOTIC DRUGS AND PSYCHOTROPIC SUBSTANCES. Vienna, 1988

2. INTERNATIONAL CONVENTION FOR THE SUPPRESSION OF THE FINANCING OF TERRORISM. United Nations, 1999.

3. Official Journal of the European Communities. COUNCIL DIRECTIVE of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering. 28. 6. 91.

4. Official Journal of the European Communities. CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION (2000/C 364/01). 18.12.2000

5. Official Journal of the European Communities. DIRECTIVE 2001/97/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering. 28.12.2001

6. Official Journal of the European Union. DIRECTIVE 2005/60/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. 25.11.2005

7. Official Journal of the European Union. 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, 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. 5.6.2015.

8. Official Journal of the European Union. DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. 19.6.2018.

9. Official Journal of the European Union. DIRECTIVE (EU) 2018/1673 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on combating money laundering by criminal law. 12.11.2018.

10. JUDGMENT OF THE COURT (Grand Chamber). 22 November 2022. ECLI:EU:C:2022:912. Document 62020CJ0037.

11. EUROPEAN COMMISSION. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010. Brussels, 20.7.2021 COM(2021) 421 final. 2021/0240 (COD).

12. FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, 2022, —142 p.

13. Wet ter voorkoming van witwassen en financieren van terrorisme. URL: [https://wetten.overheid.nl/BWBR0024282/2022-11-01#Hoofdstuk1](https://wetten.overheid.nl/BWBR0024282/2022-11-01%22%20%5Cl%20%22Hoofdstuk1). Accessed in April 2023.

14. Wetboek van Strafrecht. URL: <https://wetten.overheid.nl/BWBR0001854/2023-01-01#BoekTweede> Accessed in April 2023.

15. Federal Law "On Combating the Legalisation (Laundering) of Proceeds of Crime and the Financing of Terrorism" of 07.08.2001 N 115-FZ

16. Criminal Code of the Russian Federation of 13.06.1996 N 63-FZ.

17. Code of the Russian Federation on Administrative Offences of 30.12.2001 N 195-FZ.

18. Federal Law of 04.03.2022 N 31-FZ "On Amendments to the Code of the Russian Federation on Administrative Offenses".

19. Order of the Bank of Russia No. OD-283 dated 11.02.2022 "On Revocation of the License for Banking Operations of Joint-Stock Company "Conservative Commercial Bank" JSC Bank "KKB" (Astrakhan)

20. International Standards on Combating Money Laundering and the Financing Of Terrorism & Proliferation. The FAFT Recommendations. Adopted by the FATF Plenary in February 2012. Updated March 2022.

21. Decision to impose an administrative fine as referred to in Article 30 of the Prevention of Money Laundering and Financing of Terrorism Act on Coinbase Europe Ltd. 18 January 2023. URL: <https://www.dnb.nl/media/v4bd2ru0/besluit-tot-het-opleggen-van-een-bestuurlijke-boete-aan-coinbase.pdf>. Accessed in April 2023.

22. A.V. Kuchumov, E.V.Pecheritsa. THE CONCEPT OF "LAUNDERING" (LEGALIZATION) OF INCOME: ESSENTIAL AND LEGAL ASPECTS. Economic Vector No3(30) 2022, pp. 115-122.

23. P. Dare, S. Thornhill. ICA International Advanced Certificate in Anti Money Laundering, Course Manual. G208/11633. Twelfth Edition, October 2019, 286 p.

24. Felix Timm, Andrea Zasada, Felix Thiede. Building a Reference Model for Anti-Money Laundering in the Financial Sector. University of Rostock, Institute of Computer Science, Rostock, Germany. Conference paper at Proceedings of the 18th Conference on Learning, Knowledge, Data, Analytics at Potsdam. September 2016

25. Nduka, B.(O).E. and Sechap, G. (2021), "Refocusing designated non-financial businesses and professions on the path of anti-money laundering and combating the financing of terrorism compliance", Journal of Money Laundering Control, Vol. 24 No. 4. URL: <https://doi.org/10.1108/JMLC-11-2020-0125>. Accessed in April 2023.

26. SUSANNAH HAMMOND, TODD EHRET. Thomson Reuters. Cryptocurrency regulations by country. 37 p.

27. ComplyAdvantage. 6AMLD: Looking Ahead to the 6th EU Anti-Money Laundering Directive.

28. Bastrykin, Alexander. 2021. "Investigation of Money Laundering and Terrorist Financing: Practice of the Investigative Committee of Russia". Vestnik of Saint Petersburg State University. Law 3. pp. 493–501.

29. PISARENKO A.P. NATIONAL "ANTI-MONEY LAUNDERING" SYSTEM OF THE RF: COMPLIANCE WITH FATF REQUIREMENTS AND EVALUATION OF EFFECTIVENESS. Journal of Taganrog Institute of Management and Economics. No 2/2019. pp. 58-61

30. International Finance Corporation, Anti-Money-Laundering (AML) & Countering Financing of Terrorism (CFT) Risk Management in Emerging Market Banks, Good Practice Note, 2019, 77 p.

31. The Wolfsberg Group, Wolfsberg Statement Guidance on a Risk Based Approach for Managing Money Laundering Risks, 2006, 7 p.

32. The Joint Money Laundering Steering Group, Prevention of money laundering/ combating terrorist financing, GUIDANCE FOR THE UK FINANCIAL SECTOR, Part 1, June 2020 (amended July 2022), 215 p.

33. Beaumier, Carol M. "Anti-money-laundering compliance: elements of a successful program." Bank Accounting & Finance, vol. 21, no.2, Feb.-Mar. 2008, pp. 39+. Gale Academic OneFile.

34. UNITED NATIONS OFFICE ON DRUGS AND CRIME – RESEARCH REPORT Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes. OCTOBER 2015. 138 p.

35. FATF, Anti-money laundering and counter-terrorist financing measures – Russian Federation, Fourth Round Mutual Evaluation Report, FATF, Paris,
December 2019. 344 p.

36. European Union Agency for Criminal Justice Cooperation. Eurojust Report on Money Laundering. October 2022, 54 p.

37. FATF, Report on the State of Effectiveness Compliance with FATF Standards, FATF, Paris, April 2022, 56 p.

38. Address by Michel Camdessus Managing Director of the International Monetary Fund at the Plenary Meeting of the Financial Action Task Force on Money Laundering. Paris, February 10, 1998. URL: <https://www.imf.org/en/News/Articles/2015/09/28/04/53/sp021098>. Accessed in April 2023.

39. The official website of the Financial Action Task Force. Frequently Asked Questions. URL: <https://www.fatf-gafi.org/en/pages/frequently-asked-questions.html#tabs-36503a8663-item-6ff811783c-tab> Accessed in April 2023.

40. The official website of the Council of Europe. Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism. Financing of proliferation. URL: <https://www.coe.int/en/web/moneyval/implementation/financing-proliferation>. Accessed in April 2023.

41. The official website of the United Nations. Global Programme against Money Laundering URL: <https://www.unodc.org/unodc/en/money-laundering/global-programme-against-money-laundering/.html>. Accessed in April 2023.

42. The official website of the FATF. History of the FATF. URL: <https://www.fatf-gafi.org/en/the-fatf/history-of-the-fatf.html>. Accessed in April 2023.

43. The official website of the Financial Action Task Force. URL: <https://fatfgaf.org/faq/membercountriesandobservers/index.html>. Accessed in April 2023.

44. The official website of the International Monetary Fund. URL: <https://www.imf.org/external/np/leg/amlcft/eng/aml2.htm>. Accessed in April 2023

45. The official website of the World Bank. URL: <https://www.worldbank.org/en/topic/financialmarketintegrity>. Accessed in April 2023

46. The official website of the Wolfsberg Group. URL: <https://www.wolfsberg-principles.com/about/mission>. Accessed in April 2023.

47. The official website of the Transparency International. Our impact. URL: <https://www.transparency.org/en/our-impact> . Accessed in April 2023.

48. The official website of the European Federation of Journalists. EU Court of Justice decision to “invalidate” transparency in beneficial ownership is a blow to the right to know. URL: <https://europeanjournalists.org/blog/2022/11/25/eu-court-of-justice-decision-to-invalidate-transparency-in-beneficial-ownership-is-a-blow-to-the-right-to-know/>. Accessed in April 2023.

49. HARRIS KYRIAKIDES. CYPRUS ENACTS THE 5TH ANTI MONEY LAUNDERING DIRECTIVE INTRODUCING CRYPTO ASSETS. April 9, 2021. URL: <https://www.legal500.com/developments/thought-leadership/cyprus-enacts-the-5th-anti-money-laundering-directive-introducing-crypto-assets/>. Accessed in April 2023.

50. The European Commission is stepping up its AML/CFT game. URL: <https://www.pwc.com/mt/en/publications/financial-crime-news/european-commission-stepping-up-its-aml-cft-game.html>. Accessed in April 2023.

51. FATF, Anti-money laundering and counter-terrorist financing measures - The Netherlands, Fourth Round Mutual Evaluation Report, FATF, Paris, August 2022, URL: <http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-netherlands-2022.html>. Accessed in April 2023.

52. The official website of the FATF. The Netherlands' measures to combat money laundering and terrorist financing. Paris, 24 August 2022. URL: <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-netherlands-2022.html>. Accessed in April 2023.

53. The official website of the Financial Intelligence Unit – the Netherlands. Reporting entities. URL: <https://www.fiu-nederland.nl/en/home/reporting-entities/>. Accessed in April 2023.

54. The official website of Autoriteit Financiële Markten. URL: <https://www.afm.nl/en/over-de-afm/wat-doen-wij>. Accessed in April 2023.

55. David Schreuders, Nosh Van Der Voort. Financial Crime in the Netherlands: Overview. Thomson Reuters Practical Law. URL: <https://uk.practicallaw.thomsonreuters.com/w-019-7456?transitionType=Default&contextData=(sc.Default)&firstPage=true#co_anchor_a152616>. Accessed in April 2023.

56. Lisa van der Wal, Menco Rasterhoff. Anti-Money laundering Laws and Regulations Netherlands. May 19, 2022. URL: <https://iclg.com/practice-areas/anti-money-laundering-laws-and-regulations/netherlands>. Accessed in April 2023.

57. The official website of De Nederlandsche Bank. DNB imposes administrative fine on Coinbase Europe Limited for providing crypto services without the legally required registration until 22 September 2022. URL: <https://www.dnb.nl/en/sector-news/enforcement-measures-2023/dnb-imposes-administrative-fine-on-coinbase-europe-limited-for-providing-crypto-services-without-the-legally-required-registration-until-22-september-2022/> Accessed in April 2023.

58. The official website of the Investigative Committee of Russia. A criminal case has been opened against blogger Elena Blinovskaya for tax evasion and money laundering on a particularly large scale. April 27, 2023. URL: <https://sledcom.ru/news/item/1784724/>. Accessed in April 2023.

59. The official website of RBC.RU. Central Bank revokes license of WebMoney settlement bank. URL: [https://www.rbc.ru/economics/11/02/2022/6205e76c9a79472edafbb22f Accessed in April 2023](https://www.rbc.ru/economics/11/02/2022/6205e76c9a79472edafbb22f%20Accessed%20in%20April%202023).

 60. The official website of the Kommersant. Lack of a license has not prevented transfers. April 8, 2022. URL: https://www.kommersant.ru/doc/5295827. Accessed in April 2023.

61. The official website of Lenta.ru. General Prosecutor's Office of the Russian Federation files lawsuit against banker to confiscate 10 billion rubles. January 13, 2023. URL: https://lenta.ru/news/2023/01/13/trubizinn/. Accessed in April 2023.

62. The official website of the Central Bank of the Russian Federation. The banking license of JSC Bank KKB was revoked. 11 February 2022. URL: <http://www.cbr.ru/press/pr/?file=11022022_073806pr1.htm> Accessed in April 2023.

63. The official website of the Bank of Russia. The "Know Your Customer" platform is launched. 1 July 2023. URL: <https://cbr.ru/press/event/?id=13979> Accessed in April 2023.

64. FATF, Anti-money laundering and counter-terrorist financing measures – Russian Federation, Fourth Round Mutual Evaluation Report, FATF, Paris, December 2019, URL: <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-russian-federation-2019.html> Accessed in April 2023.

65. The official website of the FATF. The Russian Federation's measures to combat money laundering and terrorist financing. Paris, 17 December 2019. URL: <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-russian-federation-2019.html> Accessed in April 2023.

66. The official website of the FATF. FATF statement on the Russian Federation. Paris, 24 February 2023 URL: <https://www.fatf-gafi.org/en/publications/Fatfgeneral/fatf-statement-russian-federation.html>. Accessed in April 2023.

67. The official website of the FATF. "Black and grey" lists. URL: <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>. Accessed in April 2023.

68. A. Terentiev, E. Ruzleva, P. Miledin, G. Peremitin. Dubai's second largest bank, ENBD, starts blocking investment accounts of Russians. April 14, 2023. URL: <https://www.forbes.ru/finansy/487619-vtoroj-krupnejsij-bank-dubaa-enbd-nacal-blokirovat-investicionnye-sceta-rossian> Accessed in April 2023.

69. The official website of Business FM. Bank of Cyprus closes accounts to Russians. April 15, 2023. URL: <https://www.bfm.ru/news/523348>. Accessed in April 2023

70. The Bank Fines 2020 Report. URL: <https://finbold.com/bank-fines-2020/>. Accessed in April 2023.

71. The Official Website of the ABN AMRO. Jarco de Swart. ABN AMRO accepted settlement offer in the anti-money laundering investigation in the Netherlands. 19 April 2021. URL: <https://www.abnamro.com/en/news/abn-amro-accepted-settlement>. Accessed in April 2023.

72. THE ELEMENTS OF AN EFFECTIVE AML-CFT FRAMEWORK, CHAPTER III, URL: <https://www.unodc.org/roseap/uploads/archive/documents/2009/02/TOCAMLO/08-CHAPTER_III.pdf> . Accessed in April 2023.

73. The official website of the Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Circular 3/2017 (GW) - video identification procedures. Reference number GW 1-GW 2002-2009/0002. 10.04.2017. URL: <https://www.bafin.de/DE/Startseite/startseite_node.html;jsessionid=7D5B246CC38E44EC72973C986F2933FB.2_cid500>. Accessed in April 2023.

74. Brandon Spear, Mitigating digital fraud risk to drive B2B business growth April, 2022 URL: <https://customerthink.com/mitigating-digital-fraud-risk-to-drive-b2b-business-growth/> . Accessed in April 2023.

75. Customer Due Diligence Requirements for Financial Institutions. Financial Crimes Enforcement Network (FinCEN), Treasury. URL: <https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions>. Accessed in April 2023.

76. The official website of the National Crime Agency (NCA). Money laundering and illicit finance. URL: <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance>. Accessed in April 2023.

1. UNITED NATIONS OFFICE ON DRUGS AND CRIME – RESEARCH REPORT Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes. OCTOBER 2011. p. 5. [↑](#footnote-ref-1)
2. Address by Michel Camdessus Managing Director of the International Monetary Fund at the Plenary Meeting of the Financial Action Task Force on Money Laundering. Paris, February 10, 1998. URL: <https://www.imf.org/en/News/Articles/2015/09/28/04/53/sp021098>. Accessed in April 2023. [↑](#footnote-ref-2)
3. The official website of the Financial Action Task Force. Frequently Asked Questions. URL: <https://www.fatf-gafi.org/en/pages/frequently-asked-questions.html#tabs-36503a8663-item-6ff811783c-tab> Accessed in April 2023. [↑](#footnote-ref-3)
4. Art. 3 of the UNITED NATIONS CONVENTION AGAINST ILLICIT TRAFFIC IN NARCOTIC DRUGS AND PSYCHOTROPIC SUBSTANCES. Vienna, 1988 [↑](#footnote-ref-4)
5. A.V. Kuchumov, E.V.Pecheritsa. THE CONCEPT OF "LAUNDERING" (LEGALIZATION) OF INCOME: ESSENTIAL AND LEGAL ASPECTS. Economic Vector No3(30) 2022, p. 116 [↑](#footnote-ref-5)
6. P. Dare, S. Thornhill. ICA International Advanced Certificate in Anti Money Laundering, Course Manual. p. 20. G208/11633. Twelfth Edition, October 2019 [↑](#footnote-ref-6)
7. Felix Timm , Andrea Zasada , Felix Thiede. Building a Reference Model for Anti-Money Laundering in the Financial Sector. University of Rostock, Institute of Computer Science, Rostock, Germany. Conference paper at Proceedings of the 18th Conference on Learning, Knowledge, Data, Analytics at Potsdam. September 2016 [↑](#footnote-ref-7)
8. Nduka, B.(O).E. and Sechap, G. (2021), "Refocusing designated non-financial businesses and professions on the path of anti-money laundering and combating the financing of terrorism compliance", Journal of Money Laundering Control, Vol. 24 No. 4. URL: <https://doi.org/10.1108/JMLC-11-2020-0125>. Accessed in April 2023. [↑](#footnote-ref-8)
9. Art. 2 of the INTERNATIONAL CONVENTION FOR THE SUPPRESSION OF THE FINANCING OF TERRORISM. United Nations, 1999 [↑](#footnote-ref-9)
10. P. Dare, S. Thornhill. ICA International Advanced Certificate in Anti Money Laundering, Course Manual. p. 20. G208/11633. Twelfth Edition, October 2019 [↑](#footnote-ref-10)
11. The official website of the Council of Europe. Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism. Financing of proliferation. URL: <https://www.coe.int/en/web/moneyval/implementation/financing-proliferation>. Accessed in April 2023. [↑](#footnote-ref-11)
12. European Union Agency for Criminal Justice Cooperation. Eurojust Report on Money Laundering. October 2022, p. 2 [↑](#footnote-ref-12)
13. European Union Agency for Criminal Justice Cooperation. Eurojust Report on Money Laundering. October 2022, p.50 [↑](#footnote-ref-13)
14. The official website of the United Nations. Global Programme against Money Laundering URL: <https://www.unodc.org/unodc/en/money-laundering/global-programme-against-money-laundering/.html>. Accessed in April 2023. [↑](#footnote-ref-14)
15. The official website of the FATF. History of the FATF. URL: <https://www.fatf-gafi.org/en/the-fatf/history-of-the-fatf.html>. Accessed in April 2023. [↑](#footnote-ref-15)
16. FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, 2022. [↑](#footnote-ref-16)
17. The official website of the Financial Action Task Force. URL: <https://fatfgaf.org/faq/membercountriesandobservers/index.html>. Accessed in April 2023. [↑](#footnote-ref-17)
18. FATF (2022), Report on the State of Effectiveness Compliance with FATF Standards, FATF, Paris, p. 3. [↑](#footnote-ref-18)
19. The official website of the International Monetary Fund. URL: <https://www.imf.org/external/np/leg/amlcft/eng/aml2.htm>. Accessed in April 2023 [↑](#footnote-ref-19)
20. P. Dare, S. Thornhill. ICA International Advanced Certificate in Anti Money Laundering, Course Manual. G208/11633. Twelfth Edition, October 2019, p.42 [↑](#footnote-ref-20)
21. The official website of the World Bank. URL: <https://www.worldbank.org/en/topic/financialmarketintegrity>. Accessed in April 2023 [↑](#footnote-ref-21)
22. P. Dare, S. Thornhill. ICA International Advanced Certificate in Anti Money Laundering, Course Manual. G208/11633. Twelfth Edition, October 2019, p.49 [↑](#footnote-ref-22)
23. The official website of the Wolfsberg Group. URL: <https://www.wolfsberg-principles.com/about/mission>. Accessed in April 2023. [↑](#footnote-ref-23)
24. P. Dare, S. Thornhill. ICA International Advanced Certificate in Anti Money Laundering, Course Manual. G208/11633. Twelfth Edition, October 2019, p.54 [↑](#footnote-ref-24)
25. The official website of the Transparency International. Our impact. URL: <https://www.transparency.org/en/our-impact> . Accessed in April 2023. [↑](#footnote-ref-25)
26. Official Journal of the European Communities. COUNCIL DIRECTIVE of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering. No L 166/77. 28. 6. 91. [↑](#footnote-ref-26)
27. Official Journal of the European Communities. DIRECTIVE 2001/97/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering. 28.12.2001 [↑](#footnote-ref-27)
28. Official Journal of the European Union. DIRECTIVE 2005/60/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. 25.11.2005 [↑](#footnote-ref-28)
29. Ibid, Article 40. [↑](#footnote-ref-29)
30. Official Journal of the European Union. 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, 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. 5.6.2015. Article 11 (c). [↑](#footnote-ref-30)
31. Ibid, Article 30. [↑](#footnote-ref-31)
32. Official Journal of the European Union. DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. 19.6.2018. Article 1 point 2(b). [↑](#footnote-ref-32)
33. Ibid, Article 9. [↑](#footnote-ref-33)
34. SUSANNAH HAMMOND, TODD EHRET. Thomson Reuters. Cryptocurrency regulations by country. p.9, p.21 [↑](#footnote-ref-34)
35. Official Journal of the European Union. DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. 19.6.2018. Article 18a. [↑](#footnote-ref-35)
36. JUDGMENT OF THE COURT (Grand Chamber). 22 November 2022. ECLI:EU:C:2022:912. Document 62020CJ0037. [↑](#footnote-ref-36)
37. Official Journal of the European Communities. CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION (2000/C 364/01). 18.12.2000 [↑](#footnote-ref-37)
38. Official Journal of the European Union. 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, 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. 5.6.2015 [↑](#footnote-ref-38)
39. Official Journal of the European Union. DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. 19.6.2018 [↑](#footnote-ref-39)
40. JUDGMENT OF THE COURT (Grand Chamber). 22 November 2022. ECLI:EU:C:2022:912. Document 62020CJ0037. [↑](#footnote-ref-40)
41. The official website of the European Federation of Journalists. EU Court of Justice decision to “invalidate” transparency in beneficial ownership is a blow to the right to know. URL: <https://europeanjournalists.org/blog/2022/11/25/eu-court-of-justice-decision-to-invalidate-transparency-in-beneficial-ownership-is-a-blow-to-the-right-to-know/>. Accessed in April 2023. [↑](#footnote-ref-41)
42. A.V. Kuchumov, E.V.Pecheritsa. THE CONCEPT OF "LAUNDERING" (LEGALIZATION) OF INCOME: ESSENTIAL AND LEGAL ASPECTS. Economic Vector No3(30) 2022, p. 119 [↑](#footnote-ref-42)
43. Official Journal of the European Union. DIRECTIVE (EU) 2018/1673 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on combating money laundering by criminal law. 12.11.2018. Article 2 (1) [↑](#footnote-ref-43)
44. Ibid, Article 8. [↑](#footnote-ref-44)
45. ComplyAdvantage. 6AMLD: Looking Ahead to the 6th EU Anti-Money Laundering Directive. p.6. [↑](#footnote-ref-45)
46. HARRIS KYRIAKIDES. CYPRUS ENACTS THE 5TH ANTI MONEY LAUNDERING DIRECTIVE INTRODUCING CRYPTO ASSETS. April 9, 2021. URL: <https://www.legal500.com/developments/thought-leadership/cyprus-enacts-the-5th-anti-money-laundering-directive-introducing-crypto-assets/>. Accessed in April 2023. [↑](#footnote-ref-46)
47. EUROPEAN COMMISSION. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) 1094/2010, (EU) 1095/2010. Brussels, 20.7.2021 COM(2021) 421 final. 2021/0240 (COD) [↑](#footnote-ref-47)
48. The European Commission is stepping up its AML/CFT game. URL: <https://www.pwc.com/mt/en/publications/financial-crime-news/european-commission-stepping-up-its-aml-cft-game.html>. Accessed in April 2023. [↑](#footnote-ref-48)
49. FATF, Anti-money laundering and counter-terrorist financing measures - The Netherlands, Fourth Round Mutual Evaluation Report, FATF, Paris, August 2022, URL: <http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-netherlands-2022.html>. Accessed in April 2023. [↑](#footnote-ref-49)
50. The official website of the FATF. The Netherlands' measures to combat money laundering and terrorist financing. Paris, 24 August 2022. URL: <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-netherlands-2022.html>. Accessed in April 2023. [↑](#footnote-ref-50)
51. FATF, Anti-money laundering and counter-terrorist financing measures - The Netherlands,

Fourth Round Mutual Evaluation Report, FATF, Paris, 2020, p. 14 [↑](#footnote-ref-51)
52. Wet ter voorkoming van witwassen en financieren van terrorisme. Article 1a, clause 3. URL: [https://wetten.overheid.nl/BWBR0024282/2022-11-01#Hoofdstuk1](https://wetten.overheid.nl/BWBR0024282/2022-11-01%22%20%5Cl%20%22Hoofdstuk1). Accessed in April 2023 [↑](#footnote-ref-52)
53. The official website of the Financial Intelligence Unit – the Netherlands. Reporting entities. URL: <https://www.fiu-nederland.nl/en/home/reporting-entities/>. Accessed in April 2023. [↑](#footnote-ref-53)
54. The official website of Autoriteit Financiële Markten. URL: <https://www.afm.nl/en/over-de-afm/wat-doen-wij>. Accessed in April 2023. [↑](#footnote-ref-54)
55. Wet ter voorkoming van witwassen en financieren van terrorisme. Article 3, clause 5(b). URL: <https://wetten.overheid.nl/BWBR0024282/2022-11-01#Hoofdstuk1>. Accessed in April 2023 [↑](#footnote-ref-55)
56. David Schreuders, Nosh Van Der Voort. Financial Crime in the Netherlands: Overview. Thomson Reuters Practical Law. URL: <https://uk.practicallaw.thomsonreuters.com/w-019-7456?transitionType=Default&contextData=(sc.Default)&firstPage=true#co_anchor_a152616>. Accessed in April 2023. [↑](#footnote-ref-56)
57. Wetboek van Strafrecht. Article 420ter. URL: <https://wetten.overheid.nl/BWBR0001854/2023-01-01#BoekTweede> Accessed in April 2023. [↑](#footnote-ref-57)
58. Lisa van der Wal, Menco Rasterhoff. Anti-Money laundering Laws and Regulations Netherlands. May 19, 2022. URL: <https://iclg.com/practice-areas/anti-money-laundering-laws-and-regulations/netherlands>. Accessed in April 2023. [↑](#footnote-ref-58)
59. Wet ter voorkoming van witwassen en financieren van terrorisme. Article 31, clauses 1 and 4. URL: <https://wetten.overheid.nl/BWBR0024282/2022-11-01#Hoofdstuk1>. Accessed in April 2023 [↑](#footnote-ref-59)
60. Decision to impose an administrative fine as referred to in Article 30 of the Prevention of Money Laundering and Financing of Terrorism Act on Coinbase Europe Ltd. 18 January 2023. URL: <https://www.dnb.nl/media/v4bd2ru0/besluit-tot-het-opleggen-van-een-bestuurlijke-boete-aan-coinbase.pdf>. Accessed in April 2023. [↑](#footnote-ref-60)
61. Wet ter voorkoming van witwassen en financieren van terrorisme. Article 23b, clause 1. URL: <https://wetten.overheid.nl/BWBR0024282/2022-11-01#Hoofdstuk3A>. Accessed in April 2023 [↑](#footnote-ref-61)
62. The official website of De Nederlandsche Bank. DNB imposes administrative fine on Coinbase Europe Limited for providing crypto services without the legally required registration until 22 September 2022. URL: <https://www.dnb.nl/en/sector-news/enforcement-measures-2023/dnb-imposes-administrative-fine-on-coinbase-europe-limited-for-providing-crypto-services-without-the-legally-required-registration-until-22-september-2022/> Accessed in April 2023. [↑](#footnote-ref-62)
63. Bastrykin, Alexander. 2021. "Investigation of Money Laundering and Terrorist Financing: Practice of the Investigative Committee of Russia". Vestnik (Herald) of Saint Petersburg University. Law 3. p. 494. [↑](#footnote-ref-63)
64. PISARENKO A.P. NATIONAL "ANTI-MONEY LAUNDERING" SYSTEM OF THE RF: COMPLIANCE WITH FATF REQUIREMENTS AND EVALUATION OF EFFECTIVENESS. Journal of Taganrog Institute of Management and Economics. No 2/2019. p. 59 [↑](#footnote-ref-64)
65. Federal Law "On Combating the Legalisation (Laundering) of Proceeds of Crime and the Financing of Terrorism" of 07.08.2001 N 115-FZ. Article 5, clauses 1 and 2. [↑](#footnote-ref-65)
66. Federal Law "On Combating the Legalisation (Laundering) of Proceeds of Crime and the Financing of Terrorism" of 07.08.2001 N 115-FZ. Article 6, clause 1. [↑](#footnote-ref-66)
67. Articles 174, 174.1 of the “Criminal Code of the Russian Federation” of 13.06.1996 N 63-FZ. [↑](#footnote-ref-67)
68. Article 205.1of the “Criminal Code of the Russian Federation” of 13.06.1996 N 63-FZ. [↑](#footnote-ref-68)
69. The official website of the Investigative Committee of Russia. A criminal case has been opened against blogger Elena Blinovskaya for tax evasion and money laundering on a particularly large scale. April 27, 2023. URL: <https://sledcom.ru/news/item/1784724/>. Accessed in April 2023. [↑](#footnote-ref-69)
70. Article 15.27 of the "Code of the Russian Federation on Administrative Offences" of 30.12.2001 N 195-FZ [↑](#footnote-ref-70)
71. Article 15.27.1 of the "Code of the Russian Federation on Administrative Offences" of 30.12.2001 N 195-FZ [↑](#footnote-ref-71)
72. Clause 10 of the Federal Law of 04.03.2022 N 31-FZ "On Amendments to the Code of the Russian Federation on Administrative Offenses" [↑](#footnote-ref-72)
73. Article 15.27.3 of the "Code of the Russian Federation on Administrative Offences" of 30.12.2001 N 195-FZ [↑](#footnote-ref-73)
74. Federal Law "On Combating the Legalisation (Laundering) of Proceeds of Crime and the Financing of Terrorism" of 07.08.2001 N 115-FZ. Article 13. [↑](#footnote-ref-74)
75. Order of the Bank of Russia No. OD-283 dated 11.02.2022 "On Revocation of the License for Banking Operations of Joint-Stock Company "Conservative Commercial Bank" JSC Bank "KKB" (Astrakhan) [↑](#footnote-ref-75)
76. The official website of RBC.RU. Central Bank revokes license of WebMoney settlement bank. URL: <https://www.rbc.ru/economics/11/02/2022/6205e76c9a79472edafbb22f> Accessed in April 2023. [↑](#footnote-ref-76)
77. The official website of the Central Bank of the Russian Federation. The banking licence of JSC Bank KKB was revoked. 11 February 2022. URL: <http://www.cbr.ru/press/pr/?file=11022022_073806pr1.htm> Accessed in April 2023. [↑](#footnote-ref-77)
78. The official website of the Kommersant. Lack of a license has not prevented transfers. April 8, 2022. URL: <https://www.kommersant.ru/doc/5295827> . Accessed in April 2023. [↑](#footnote-ref-78)
79. The official website of Lenta.ru. General Prosecutor's Office of the Russian Federation files lawsuit against banker to confiscate 10 billion rubles. January 13, 2023. URL: <https://lenta.ru/news/2023/01/13/trubizinn/> . Accessed in April 2023. [↑](#footnote-ref-79)
80. The official website of the Bank of Russia. The "Know Your Customer" platform is launched. 1 July 2023. URL: <https://cbr.ru/press/event/?id=13979> Accessed in April 2023. [↑](#footnote-ref-80)
81. Federal Law "On Combating the Legalisation (Laundering) of Proceeds of Crime and the Financing of Terrorism" of 07.08.2001 N 115-FZ. Article 7.8, clause 4. [↑](#footnote-ref-81)
82. FATF (2019), Anti-money laundering and counter-terrorist financing measures – Russian Federation,

Fourth Round Mutual Evaluation Report, FATF, Paris <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-russian-federation-2019.html> Accessed in April 2023. [↑](#footnote-ref-82)
83. FATF (2019), Anti-money laundering and counter-terrorist financing measures – Russian Federation, Fourth Round Mutual Evaluation Report, FATF, Paris. p. 12. [↑](#footnote-ref-83)
84. The official website of the FATF. The Russian Federation's measures to combat money laundering and terrorist financing. Paris, 17 December 2019. URL: <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-russian-federation-2019.html> Accessed in April 2023. [↑](#footnote-ref-84)
85. FATF, Anti-money laundering and counter-terrorist financing measures – Russian Federation, Fourth Round Mutual Evaluation Report, FATF, Paris, 2019. p. 16. [↑](#footnote-ref-85)
86. The official website of the FATF. FATF Statement on the Russian Federation. URL: <https://www.fatf-gafi.org/en/publications/Fatfgeneral/Ukraine-june-2022.html> . Accessed in April 2023. [↑](#footnote-ref-86)
87. The official website of the FATF. FATF statement on the Russian Federation. Paris, 24 February 2023 URL: <https://www.fatf-gafi.org/en/publications/Fatfgeneral/fatf-statement-russian-federation.html>. Accessed in April 2023. [↑](#footnote-ref-87)
88. The official website of the FATF. "Black and grey" lists. URL: <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>. Accessed in April 2023. [↑](#footnote-ref-88)
89. Ibid [↑](#footnote-ref-89)
90. The official website of the FATF. FATF statement on the Russian Federation. Paris, 24 February 2023 URL: <https://www.fatf-gafi.org/en/publications/Fatfgeneral/fatf-statement-russian-federation.html>. Accessed in April 2023. [↑](#footnote-ref-90)
91. A. Terentiev, E. Ruzleva, P. Miledin, G. Peremitin. Dubai's second largest bank, ENBD, starts blocking investment accounts of Russians. April 14, 2023. URL: <https://www.forbes.ru/finansy/487619-vtoroj-krupnejsij-bank-dubaa-enbd-nacal-blokirovat-investicionnye-sceta-rossian> Accessed in April 2023. [↑](#footnote-ref-91)
92. The official website of Business FM. Bank of Cyprus closes accounts to Russians. April 15, 2023. URL: <https://www.bfm.ru/news/523348>. Accessed in April 2023 [↑](#footnote-ref-92)
93. The Bank Fines 2020 Report. URL: <https://finbold.com/bank-fines-2020/>. Accessed in April 2023. [↑](#footnote-ref-93)
94. The Official Website of the ABN AMRO. Jarco de Swart. ABN AMRO accepted settlement offer in the anti-money laundering investigation in the Netherlands. 19 April 2021. URL: <https://www.abnamro.com/en/news/abn-amro-accepted-settlement>. Accessed in April 2023. [↑](#footnote-ref-94)
95. International Finance Corporation, Anti-Money-Laundering (AML) & Countering Financing of Terrorism (CFT) Risk Management in Emerging Market Banks, Good Practice Note, 2019, p. 16 [↑](#footnote-ref-95)
96. THE ELEMENTS OF AN EFFECTIVE AML-CFT FRAMEWORK, CHAPTER III, URL: <https://www.unodc.org/documents/southeastasiaandpacific/2009/02/TOCAMLO/08-CHAPTER_III.pdf>. Accessed in April 2023. [↑](#footnote-ref-96)
97. INTERPRETIVE NOTE TO RECOMMENDATION 18 (INTERNAL CONTROLS AND FOREIGN BRANCHES AND SUBSIDIARIES) INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION. THE FATF RECOMMENDATIONS. ADOPTED BY THE FATF PLENARY IN FEBRUARY 2012. Updated March 2022 [↑](#footnote-ref-97)
98. The Wolfsberg Group, Wolfsberg Statement Guidance on a Risk Based Approach for Managing Money Laundering Risks, 2006, p. 6 [↑](#footnote-ref-98)
99. P. Dare, S. Thornhill. ICA International Advanced Certificate in Anti Money Laundering, Course Manual. G208/11633. Twelfth Edition, October 2019, p.103 [↑](#footnote-ref-99)
100. Ibid. [↑](#footnote-ref-100)
101. The FATF Recommendation 10. INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION. THE FATF RECOMMENDATIONS. ADOPTED BY THE FATF PLENARY IN FEBRUARY 2012. Updated March 2022 [↑](#footnote-ref-101)
102. International Finance Corporation, Anti-Money-Laundering (AML) & Countering Financing of Terrorism (CFT) Risk Management in Emerging Market Banks, Good Practice Note, 2019, p. 27 [↑](#footnote-ref-102)
103. The Joint Money Laundering Steering Group, Prevention of money laundering/ combating terrorist financing, GUIDANCE FOR THE UK FINANCIAL SECTOR, Part 1, June 2020 (amended July 2022), p. 161 [↑](#footnote-ref-103)
104. The FATF Recommendations 12, 13, 19. INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION. THE FATF RECOMMENDATIONS. ADOPTED BY THE FATF PLENARY IN FEBRUARY 2012. Updated March 2022 [↑](#footnote-ref-104)
105. INTERPRETIVE NOTE TO RECOMMENDATION 10 (CUSTOMER DUE DILIGENCE). INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION. THE FATF RECOMMENDATIONS. ADOPTED BY THE FATF PLENARY IN FEBRUARY 2012. Updated March 2022 [↑](#footnote-ref-105)
106. International Finance Corporation, Anti-Money-Laundering (AML) & Countering Financing of Terrorism (CFT) Risk Management in Emerging Market Banks, Good Practice Note, 2019, p.29 [↑](#footnote-ref-106)
107. Wet ter voorkoming van witwassen en financieren van terrorisme. Article 33. URL: <https://wetten.overheid.nl/BWBR0024282/2022-11-01#Hoofdstuk1>. Accessed in April 2023. [↑](#footnote-ref-107)
108. Federal Law "On Combating the Legalisation (Laundering) of Proceeds of Crime and the Financing of Terrorism" of 07.08.2001 N 115-FZ. Article 7, clause 1 point 1. [↑](#footnote-ref-108)
109. International Finance Corporation, Anti-Money-Laundering (AML) & Countering Financing of Terrorism (CFT) Risk Management in Emerging Market Banks, Good Practice Note, 2019, p 37 [↑](#footnote-ref-109)
110. The official website of the Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Circular 3/2017 (GW) - video identification procedures. Reference number GW 1-GW 2002-2009/0002. 10.04.2017. URL: <https://www.bafin.de/DE/Startseite/startseite_node.html;jsessionid=7D5B246CC38E44EC72973C986F2933FB.2_cid500> . Accessed in April 2023. [↑](#footnote-ref-110)
111. #  [Brandon Spear](https://customerthink.com/author/brandonspear/), Mitigating digital fraud risk to drive B2B business growth April , 2022 URL: <https://customerthink.com/mitigating-digital-fraud-risk-to-drive-b2b-business-growth/>. Accessed in April 2023.

 [↑](#footnote-ref-111)
112. #  Customer Due Diligence Requirements for Financial Institutions. Financial Crimes Enforcement Network (FinCEN), Treasury. URL: <https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions>. Accessed in April 2023.

 [↑](#footnote-ref-112)
113. GENERAL GLOSSARY, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION. THE FATF RECOMMENDATIONS. ADOPTED BY THE FATF PLENARY IN FEBRUARY 2012. Updated March 2022 [↑](#footnote-ref-113)
114. Wet ter voorkoming van witwassen en financieren van terrorisme. Article 33. URL: <https://wetten.overheid.nl/BWBR0024282/2022-11-01#Hoofdstuk1> . Accessed in April 2023. [↑](#footnote-ref-114)
115. Federal Law "On Combating the Legalisation (Laundering) of Proceeds of Crime and the Financing of Terrorism" of 07.08.2001 N 115-FZ. Article 7, clause 1 point 1. [↑](#footnote-ref-115)
116. P. Dare, S. Thornhill. ICA International Advanced Certificate in Anti Money Laundering, Course Manual. G208/11633. Twelfth Edition, October 2019, p. 202. [↑](#footnote-ref-116)
117. INTERPRETIVE NOTE TO RECOMMENDATION 29 (FINANCIAL INTELLIGENCE UNITS). INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION. THE FATF RECOMMENDATIONS. ADOPTED BY THE FATF PLENARY IN FEBRUARY 2012. Updated March 2022 [↑](#footnote-ref-117)
118. Wet ter voorkoming van witwassen en financieren van terrorisme. Article 3, clause 5(b). URL: <https://wetten.overheid.nl/BWBR0024282/2022-11-01#Hoofdstuk1>. Accessed in April 2023. [↑](#footnote-ref-118)
119. Federal Law "On Combating the Legalisation (Laundering) of Proceeds of Crime and the Financing of Terrorism" of 07.08.2001 N 115-FZ. Article 6 clause 1. [↑](#footnote-ref-119)
120. P. Dare, S. Thornhill. ICA International Advanced Certificate in Anti Money Laundering, Course Manual. G208/11633. Twelfth Edition, October 2019, p. 213 [↑](#footnote-ref-120)
121. International Finance Corporation, Anti-Money-Laundering (AML) & Countering Financing of Terrorism (CFT) Risk Management in Emerging Market Banks, Good Practice Note, 2019, p 38 [↑](#footnote-ref-121)
122. Recommendation 11 of the FATF. INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION. THE FATF RECOMMENDATIONS. ADOPTED BY THE FATF PLENARY IN FEBRUARY 2012. Updated March 2022 [↑](#footnote-ref-122)
123. Recommendation 11 of the FATF. INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION. THE FATF RECOMMENDATIONS. ADOPTED BY THE FATF PLENARY IN FEBRUARY 2012. Updated March 2022. [↑](#footnote-ref-123)
124. Federal Law "On Combating the Legalisation (Laundering) of Proceeds of Crime and the Financing of Terrorism" of 07.08.2001 N 115-FZ. Article 7, clause 1 point 4. [↑](#footnote-ref-124)
125. Wet ter voorkoming van witwassen en financieren van terrorisme. Article 33. URL: <https://wetten.overheid.nl/BWBR0024282/2022-11-01#Hoofdstuk1> . Accessed in April 2023. [↑](#footnote-ref-125)
126. International Finance Corporation, Anti-Money-Laundering (AML) & Countering Financing of Terrorism (CFT) Risk Management in Emerging Market Banks, Good Practice Note, 2019, p 40 [↑](#footnote-ref-126)
127. Ibid, p. 46 [↑](#footnote-ref-127)
128. Beaumier, Carol M. "Anti-money-laundering compliance: elements of a successful program." Bank Accounting & Finance, vol. 21, no.2, Feb.-Mar. 2008, pp. 39+. Gale Academic OneFile. [↑](#footnote-ref-128)
129. A.V. Kuchumov, E.V.Pecheritsa. THE CONCEPT OF "LAUNDERING" (LEGALIZATION) OF INCOME: ESSENTIAL AND LEGAL ASPECTS. Economic Vector No3(30) 2022, p. 118 [↑](#footnote-ref-129)