ANTI-MONEY LAUNDERING IN THE EU

Time to get serious

CEPS-ECRI Task Force Report

Eero Heinäluoma
Chairman

Karel Lannoo
Rapporteur

Richard Parlour
Co-rapporteur

ecri EUROPEAN CREDIT RESEARCH INSTITUTE

CEPS

Anti-Money Laundering in the EU

Time to get serious

CEPS-ECRI Task Force Report

Chairman

Eero Heinäluoma
Member of the European Parliament;
former Minister of Finance, Finland

Rapporteur

Karel Lannoo
CEPS & ECRI

Co-rapporteur

Richard Parlour
Financial Markets Law International

Centre for European Policy Studies (CEPS)
Brussels
January 2021

CEPS is an independent think tank based in Brussels. Its mission is to produce sound policy research leading to constructive solutions to the challenges facing Europe and the world. ECRI is a think tank that investigates credit markets and retail finance. It is managed by CEPS.

This report is based on the discussions of a Task Force. Its contents convey the general tone and direction of the discussions, but its recommendations do not necessarily reflect a common position reached by all members of the Task Force. Nor do they represent the views of the institutions to which the members, the Chairman or the rapporteurs belong. The members of the Task Force participated in extensive discussions over the course of several meetings, took part in a survey and submitted comments on earlier drafts of the report. A list of participants, observers, invited guests and speakers appears in Annex at the end of this report.

The members and rapporteurs wish to thank the chair, Eero Heinäluoma, MEP and former Finnish Minister of Finance for his guidance and insights. The rapporteurs are indebted to the Task Force members and observers for their input and detailed comments, which have added value and balance to the final report. They also acknowledge the professional assistance of Beatriz Pozo and Luisa Sigl.

ISBN 978-94-6138-782-0

CEPS
Place du Congrès 1, B-1000 Brussels
Tel: 32 (0) 2 229.39.11
e-mail: info@ceps.eu
internet: www.ceps.eu

Contents

List of Boxes and Tables

Executive summary and policy recommendations

There is no doubt that a new approach is needed to combating money laundering. For the past three decades policymakers have struggled to implement effective anti-money laundering (AML) policies. While the scope of action has expanded greatly, the success of AML policies has been very limited. Launderers and criminals, aided by technology, have become ever more inventive, which has necessitated continual adaptation of the regulatory framework.

Given the ongoing monitoring and law enforcement challenges, the EU Commission and some member states have come out in favour of the creation of an **EU-wide AML supervisory agency**. This body might assist in reducing some of the coordination and cooperation issues in AML enforcement, particularly those that cross borders. However, rather than the supervisory dimension, the **regulatory side needs to be addressed first**. Here, a radically new approach is needed, based on the EU's principles of proportionality. A thorough benefit/cost analysis of the AML rules thus far could guide the way to a more measured and effective approach. Every day, banks and other 'obliged entities' complete thousands of suspicious transactions reports, of which only a handful are followed up on by financial intelligence units (FIUs), whether owing to lack of capability, capacity or even political direction.

It is an illusion to believe that a single, Europe-wide supervisory agency could, in the current circumstances, be the sole solution. **AML supervision requires the cooperation of a multitude of supervisory entities**, financial and non-financial supervisors, FIUs and law enforcement officials, as well as the obliged entities themselves. In the EU context, this means well in excess of 100 supervisory agencies, and many tens of thousands of obliged entities. It raises the issue of EU competence, certainly in the law enforcement and judicial domains. But it is beyond debate that improvement is needed. We would argue in favour of **a step-by-step approach**, building upon the framework already put in place by the European Banking Authority (EBA), and expanding this gradually (first by means of increasing the effectiveness of data exchange), with a distinct and more effective governance structure.

Before acting at the EU level, member states should put their own houses in order. On the financial supervisory side alone, 57 different entities sit around the table at the EBA in its newly created Standing Committee, which demonstrates the diversity at the national level. On the non-financial side, the structure is even more complex, and clearly much less integrated at the EU or international levels.

A real bottleneck in AML effectiveness lies with the FIUs, which are designated to process both cash transaction reports (CTRs) and suspicious activity reports (SARs). The FIUs are organised, resourced and staffed very differently across the member states — even their legal bases differ substantially — and their performance leaves much to be desired. According to figures from Europol, out of the 1.1 million SARs reported across the EU in 2019, only 10% have been further investigated by public authorities (with large differences between countries), and only 1.1% of criminal profits are eventually confiscated at the EU level. Moreover, FIU.net, the EU platform of FIUs, can for some byzantine political reason no longer be hosted by Europol but is searching for a new home, meaning that any debate on its functioning is now delayed indefinitely, further reducing AML efficacy.

To be credible, AML policies need **strong enforcement mechanisms**. But here as well, there are many flaws. AML-related crimes are treated differently across the EU. For the "hard core" money-laundering matters, cooperation among prosecutors remains tentative, too slow to tackle cross-border cases. The recent creation of the European Public Prosecutor's Office (EPPO) will facilitate collaboration, but its mandate is limited to European Union financial interests, and it will take time to become effective. For

"soft" money laundering, such as tax avoidance, approaches differ widely across the EU as to whether this should be considered a crime or an administrative offence.

Given the diversity of approaches and structures in the member states related to money laundering and law enforcement, **turning parts of the AML directive into a regulation is a step forward, but it is not a panacea**: The regulation will need to be well formulated, an outcome that cannot be guaranteed given the decision-making process. In addition, the regulatory framework does not resolve the problem of lack of cooperation between FIUs and law enforcement authorities. Regulations assume the same type of situation across all member states, but the threats faced by them, the types of criminality, their modus operandi, criminal culture and groupings differ widely, so a regulation could reduce flexibility and counter the risk-based approach that ensures resources are targeted where they are needed. There is little investment devoted to AML enforcement – tiny in comparison to the costs of AML compliance for financial institutions – and monies need to be targeted wisely. Any rule therefore needs to cover those areas that are suited to a regulation and must not defeat flexibility and targeting.

Let it be clear, there has been no shortage of (verbal) action at the international and EU levels on AML and combating the financing of terrorism (CFT). In this report, we focus mostly on the EU and the international dimension. Plenty of good analysis on money laundering is available, on what does not work, and on why it is so difficult to make headway against it. However, **good data on money laundering and underlying criminality are missing**; most are approximations based on no, or dubious, statistical models. While gaining a clear picture of money laundering and underlying criminality is a challenge, given the nature of such activity, without it there is no effective course of action. Authorities could start by improving feedback on the process, extent of illicit activity and trends in criminal behaviour, reports submitted, cases acted upon, and, critically, what results are obtained.

AML is affected by market and technological developments. Technology can facilitate the monitoring of money-laundering activities by private entities and notification to public authorities. Closer cooperation between both can also be a way forward, but the framework needs to be correctly structured, to take mandate, justice, effectiveness, data protection and competition policy concerns into account.

This task force notes and recommends:

PILLAR ONE: Governance Observations and Recommendations

At the regulatory level:

- **Enforcement of current AML directives** in an effective manner, which has an impact on underlying criminality, is key. This should not be a matter of 'compliance for compliance's sake'. The EU member states are still behind with implementation of the fourth and fifth AML directives, which need to be implemented urgently and applied. These updates contain key elements for an effective AML framework;
- **Turning the directive into a regulation** is recommended, to ensure a single set of rules across the EU, but much depends on the exact formulation, its coverage and the final outcome of the decision process. The EU will need to be mindful regarding a proper definition of money laundering, along with the objective of the money laundering regime. This needs to include a nexus to the underlying criminality, and be in compliance with the principles of proportionality and fundamental rights;
- Enforcement is also critical for the 2000 **directive on criminal offences** that created the Financial Investigation Units (FIUs), which was recently updated, with 2021 as the implementation

deadline. The judicial process across the Member States could do with more co-ordination, especially in relation to cross border cases and with third countries;

- In relation to new laws, properly structured **benefit/cost analysis** and regulatory impact analysis is needed. If there is no discernible impact on underlying criminality there should be no new laws. There is no point saddling obliged entities with more compliance burdens, which would merely hinder normal economic activity and have little impact on crime;
- Structure of new laws is one thing; effectiveness and efficiency quite another. Crucially, we must focus on measuring what matters. We recommend a switch to using objectives and key results (OKRs) which will improve effectiveness. The linkages between AML and underlying predicate offences need focus, otherwise we stay in a regime of compliance for compliance sake with zero impact.

At the supervisory level:

- Action should start at **member state level** to **streamline AML supervisory structures**, to allow for better cooperation between those involved within member states, vertically as well as horizontally, as well as across the EU and internationally;
- At the financial supervisory level, given the urgency of the situation, priority should be given to working with the new **AML Committee within the EBA**, and upgrading this, with a dedicated governance structure within EBA, in close cooperation with the national supervisory authorities and the European Central Bank (ECB);
- A **single agency raises questions** about the scope and competences, mandate, legal base, powers, accountability, governance and funding. Many potential models exist, on which there is no clarity as yet. It also raises concerns about the supervision of the non-financial sector.

At the enforcement level:

- Joint action regarding the **proper functioning of FIUs** at national level, and their **cooperation** at the EU level is recommended. The nature, specific powers and tasks of the FIUs should be better harmonised. The EU-wide interconnection of the FIUs is in limbo after a decision from the European Data Protection Supervisor that the FIU.net platform can no longer be hosted by Europol because of data protection reasons. Policy makers need to urgently address FIU cooperation at EU level;
- The member states should establish a **uniform template** for suspicious transaction reports (STRs) and SARs, to be integrated in the centralised platform, FIU.net (though this should not be the only way for obliged entities to communicate intelligence to FIUs);
- **Data sharing** between enforcement bodies involved (including the judiciary) needs to be improved, including across national borders. This relates not just to types of data but amounts and the speed of data sharing, and its security.

Regarding data protection and identity verification:

- Much remains to be done in this domain, even at the EU level. Registries of ultimate beneficial owners (**UBOs**) need to be better structured and accessible, and Legal Entity Identifiers (**LEIs**) more widely used. This applies as well for the EU in its dealings with third countries. Even before considering ultimate beneficial ownership, the utility of data held by general corporate registries—their type, amount, accessibility, searchability and granularity—needs to be addressed. Certain registries have taken backward steps in recent years, removing information on shareholders, addresses, accounts, dates of birth, etc. This only makes due diligence harder.

At the societal level:

- Well-functioning AML systems are based upon close cooperation between the public and private sectors. The **private sector is at the forefront** in detecting cases and transmitting information to the authorities. In many countries, the vast majority of the investigative capacity (in some cases up to 95%) is housed in the private sector. A framework needs to be set for secure information exchange between them, respecting distinct mandates, data protection, free competition and professional secrecy. Taking examples from progress in fighting corruption, a lot of the success will come from the achievement of cultural change.
- Public/private data sharing is exemplified by groups of financial institutions sharing anti-fraud data, and nascent versions of public/private partnerships such as joint money-laundering intelligence teams (in the UK, the Baltic and Nordic states) and the Europol Financial Intelligence Public Private Partnership.

At all levels:

- There is no doubt that **governance capabilities** at each level **need to be reviewed** to ensure that all relevant parties are connected and can communicate effectively and efficiently with each other. Governance is not merely about structure, however, and the decision-making processes need to be reassessed, in terms of both quality and speed. From a review by the Financial Action Task Force (FATF) of AML policies to implementation of its recommendations by member states has taken more than a decade. That is clearly far too long.

PILLAR TWO: Risk Management Observations and Recommendations

Adopt **objectives and key results (OKRs) and key performance indicators (KPIs)** which relate to the underlying criminal threats which AML laws are intended to impact. These need to be thought through, rather than being measures which are adopted purely as they are. The right metrics are needed to combat the threat. Data collection techniques in this area are also in need of improvement.

- Allow firms to develop and use risk-based systems to improve effectiveness;
- Carry out effective benefit/cost analysis (rather than cost/benefit analysis) of proposed new measures;
- Adopt active, coordinated defences, rather than the static three lines of defence model.

PILLAR THREE: Capability Observations and Recommendations

Growing money laundering threats require strengthened capabilities and tools.

- Encourage training and spending on specialised financial police;
- Increase funding and support of law enforcement, particularly of undercover operations and IT systems, enabling law enforcement to follow the money trail from commission of crimes;
- Improve training standards to a new EU level, including the courts process, policy makers, investigators and intelligence analysts.

1. Introduction

It has been more than three decades since the Sommet de l'Arche in Paris established the Financial Action Task Force (FATF) to combat money laundering. So where have we come to in Europe, and what remains to be done?

Curtailing money laundering has been around as a policy objective for a long time, but the target has broadened significantly. From crime and drug-trafficking-related proceeds, the mandate has grown over the past two decades to include tax eavsion, terrorist financing, human trafficking, state-sponsored and corporate bribery. Europol now monitors 44 crimes. At the same time, the breadth and means to launder money have also increased. Liberalisation of capital movements internationally, the single market, technological progress and competition for instant international payments have multiplied the challenges for banks and money transmitters, as well as for supervisors. The cases uncovered continue to be a small fraction of the 2% - 5% of global GDP (€1.7-4 trillion) that is estimated to be laundered annually.

Money laundering has been criminalised not just in Europe but the world over. Predicate offences have widened from drug trafficking to the proceeds of all crimes. Europol has established itself internationally in anti–money laundering (AML) terms. The Egmont Group has grown into a large international organisation of 159 financial intelligence units, representing the operational arm of AML/combating financing of terrorism (CFT) deterrence to complement the strategic arm of the FATF. Fifteen EU Member States (plus the European Commission) are direct FATF members, and the remaining thirteen are members of Moneyval, the European regional version of FATF. Moneyval also includes non-EU/European Economic Area (EEA) member states such as Russia and Ukraine.

The term 'money laundering', unheard of in 1989, is now in common parlance. However, the amount of proceeds of crime recovered as a result of successful money-laundering prosecutions, as compared to the amount thought to be actually laundered, is around 1% at best. It is small wonder that commission of the predicate offences remains rife and is increasing, particularly in relation to emerging criminality, such as cybercrime, wildlife and other environmental crimes. So why is the European AML system so ineffective in reducing the impact of the underlying crimes upon European citizens, and what can we do about it?

Public awareness of the extent and the reach of the problem has grown a lot, certainly since the financial crisis, as has the expectation that it will be adequately addressed. There is still a long way to go, however, in terms of changing not just the perception of AML but the culture necessary to defeat money laundering. Authorities have over the past few years stepped up their actions against laundering, as evidenced by several high-profile cases in Europe and elsewhere. European policy makers have indicated that the current approach is not sufficient and are consulting on what steps to take to move forward. Some countries have even called for the creation of a new EU-wide body.

In this context, CEPS decided to launch a task force to debate and propose effective solutions for Europe. There is certainly no shortage of studies and reports on AML, by international bodies, EU institutions, advisors and experts on the challenges faced. However, when looking at these, we found that many studies take a highly specific view of money laundering, from a certain niche perspective, or merely describe the various legal frameworks, without adopting an all-encompassing strategic view or looking at the efficacy of the system overall. Effective policies to tackle money laundering require the full involvement of the private sector, which is a key contributor to defend against it. This is in the private

sector's interest since the costs of non-compliance have rocketed, as shown in some recent cases, and have started to affect financial stability.

2. Objective

Attempting to halt, or at least significantly reduce money laundering is a **moral imperative** in any democratic society, where all citizens are free and equal under the law, in a fair system of cooperation. A democratic regime comprises political institutions which guarantee citizens' rights and obligations, with a responsible and accountable executive, an independent judiciary and a freely elected representative assembly of citizens, set in a constitution with suitable and effective checks and balances to avoid misuse of power.

Laundering the proceeds of criminal, illegal or black market activities should in any open democracy be dealt with forcefully, as it undermines the very fabric of society and its political institutions. Such actions require a firm, immediate and effective reaction. Lack of clarity, delays and inefficiency will only invite further money laundering; it will be like an infectious disease that spreads further and deeper. Questions may be raised about the responsiveness of policy makers, however, considering the fairly recent focus on money laundering in policy, particularly on the law enforcement side, and given the disconnect between money laundering itself, which can seem to be a victimless offence, and the ravages of the predicate crimes.

Despite all the reports, there are **few good data** available about extent of money laundering or the underlying predicate offences, and such data as there are may be held in a variety of different places. Most available data are of a macro nature, based upon proxies and estimates. Existing numbers are derived from rough projections of the size of the shadow economy or estimates based upon foreign direct investment (FDI) flows compared to real investment, or the role of shell companies (see Unger, 2020, for an overview). A good regulatory process should in essence start here, but obviously, in this case, this is not easy, as criminals do not declare their activities. In the EU, tax evasion alone is estimated at €825 bn. Tax avoidance adds another €150 bn.

Bringing the different data together in an official barometer of money laundering could provide indications of the success of the policy. Such a barometer in fact exists, but it needs to be revisited. The private venture Basel AML Index measures the risk of money laundering and terrorist financing in 141 countries around the world, defined broadly as a country's vulnerability to money laundering/terrorist financing and its capacities to counter it. It covers 16 indicators in five domains at the country level, regarding quality of the framework, bribery and corruption, financial transparency, public accountability and political risk. But it classifies as 'low risk' European countries such as Bulgaria in 4th, Montenegro in 16th and Croatia in 22nd place, for example, countries that all have much lower rankings for Transparency International (respectively the 74th, 66th and 63rd, on a total of 180 countries).

The Basel Index is also in contrast to the designation of Major Money Laundering countries in the US annual International Narcotics Control Strategy Report, which lists (without ranking) Italy, the Netherlands, Spain for the EU, but also the UK and the US itself. Overall, the Basel AML Index gives the impression that smaller jurisdictions, very often without any serious financial market infrastructure, are the countries which are at high risk in relation to money laundering. However, money launderers need serious financial markets in which to operate effectively, and the general view worldwide is that the major financial centres are also the major places for money laundering, which the US report confirms.

This shows the difficulty of compiling a general index for such purposes and avoiding political considerations in order to produce intelligence of value, relevance and accuracy for financial institutions.

Many resources are being spent on confronting money laundering, in both the public and private spheres. Thousands of civil servants control tax declarations; financial investigation units and the police monitor suspicious transactions and activities. Financial institutions, and other entities dealing with cash transactions, employ thousands of staff purely to check huge numbers of false positives generated by a computer surveillance programme (this is often 95% - 98% of the total number flagged), let alone carry out investigations or proactive due diligence. Increasingly, it is also a matter for a financial institution's proprietary information technology to detect unusual transactions, often using algorithms that they will have to explain to authorities one day.

3. Definition and scope of current regulation

One of the first instances of money laundering in the literature arises two thousand years ago. The monies used to bribe Judas to betray Jesus ended up being spent on the purchase of some fields outside Jerusalem, known as the 'Fields of Blood'. It gives us the expression 'blood money'. The term money 'laundering' dates back to the gangster Al Capone, who in the 1920s kept his illegally obtained cash in a washing machine. The initial definition as developed by the FATF referred specifically to the proceeds of drug trafficking that were recycled in the official banking system. The definition was gradually enlarged to include the proceeds of any criminal enterprise, and after 2001, terrorist financing, corruption and tax evasion.

Regulating money laundering is difficult because the concept is elusive; it is a moving target. It is dependent on circumstances of time, place and the groups under scrutiny. The U.S. Bank Secrecy Act of 1970 represents the historic starting point for efforts to detect and sanction money laundering, though the term was not commonly used until the early 1990s. Banks were (and still are) required to provide information to the Department of the Treasury concerning transactions involving more than $10,000 in cash, whether or not that transaction was thought to be suspicious (so-called Cash Transaction Reports, or CTRs). The Money Laundering Control Act of 1986 was explicitly a component of the U.S. war on drugs, specifically cocaine from Latin America. From then on, money-laundering regulation has expanded in scope, depth and geographical reach.

Regulation has to take into account the practical mechanisms of money laundering, often described by the FATF as having three sequential elements: placement, layering and integration. **Placement** is the introduction of the funds into the financial system, whether through cash deposits or more complex, advanced methods. **Layering** is a set of activities intended to distance the funds from their point of criminal origin. **Integration** involves converting "illegal proceeds into apparently legitimate business earnings through normal financial or commercial operations". In actual fact, few laundering operations follow these steps precisely, or in that order, and they often have different features altogether. Nor do any AML laws worldwide distinguish offences on the basis of placement, layering or integration, so this has become a case of jargon and does not necessarily recognise the ingenuity or fluidity of laundering schemes.

In addition, regulation must be adapted to the specific payment practices of the financial sector, their interconnectedness through correspondent banking accounts, the role of the central banks in providing

payments infrastructure and the competitive context. Central to AML rules is customer due diligence (CDD), but there is little agreement as to what this should cover, in terms of depth, breadth or quality. The general corporate and other registries of the EU member states do not help much with performing CDD. The banking sector is increasingly challenged by non-bank payment providers, which have managed to take a lot of market share over recent years, and even more since the Covid crisis (the business-to-consumer payment market worldwide alone is estimated at €30 trillion). This competition puts pressure on the banks to increase the speed of payments and reduce their costs.

In a world of almost completely free capital flows (save for certain instances of exchange controls), any regulation must be international in scope; otherwise, it is like 'fighting windmills'. Hence the role of the FATF in establishing 40 key principles for the combat of money laundering and terrorist financing, in carrying out mutual evaluations of FATF members, in liaising with FATF-style organisations such as Moneyval, in blacklisting non-cooperative jurisdictions, in taking action against bank secrecy or anonymous accounts. Even in the EU, this has not been easy, as the 2003 decision on the savings tax directive proved, with 10-year transition periods for Austria, Belgium and Luxembourg, and the request for a similar commitment from third countries, including Switzerland and offshore financial centres. On the other side, there is the extraterritorial application of rules and sanctions. International organisations such as the UN, and countries such as the United States, often impose sanctions, and fines for non-compliance, even for foreign-based entities, or even merely in relation to entities' usage of the USD as the currency of the transaction concerned. The US is by far the most sanctioning country, but the effectiveness of sanctions has to be questioned, and there is often a political dimension to sanctions, such as in relation to Iran for example.

Strict AML supervision is also required from a macro perspective. Excessive dependence on dark and undocumented accounts increases the vulnerability of a financial regime to sudden shocks, on which more research could be done.[1] It creates holes in the financial system if large amounts suddenly seem to be fraudulent or tainted. This is even more the case for smaller financial centres, as evidenced in the cases of Cyprus or Malta and the impact of the Greek financial crisis. The size of fines is unpredictable, and can lead to international tensions, as was the case with the 2014 fine of $9 billion on BNPParibas by U.S. authorities for processing transactions for nations subject to U.S. sanctions. That wiped out the entire revenue of the bank for the year. On the other hand, some fines are never paid—the U.S. Securities and Exchange Commission recently disclosed that this was the case for 50% of the fines it levied. Other countries have proposed a financial crime levy to assist governments in fighting financial crime. But this seems hard to justify against the huge fine revenue extracted from banks.

Principles of better regulation, with focus on ex ante (and ex post) impact assessments, benefit/cost and regulatory impact analysis, consultation, and application of the principles of proportionality and subsidiarity should be applied to AML efforts. Any new law in this domain should be very well justified as a result of rigorous impact assessments demonstrating necessity, proportionality and fundamental rights compliance, in particular privacy and data protection. Further, there is the need for effective enforcement of the rules and analysis of the impact on underlying criminality. Until recently, the cost of laundering money has appeared to be quite low.

Regulating money laundering is a classic collective choice problem. If not properly regulated and enforced, the temptation will be high for a bank to accept dirty money and 'clean' it. If not, the nearest competitor will do it, and there are examples of criminal organisations learning from rejection by one

[1] More research could be done along the 1996 Macroeconomic Implications of Money Laundering publication by the IMF.

financial institution and opening with ease at others (not necessarily with complicity or negligence on the part of the latter but as the criminals honed a better front story). Unless there are clear rules in place, properly monitored, with a strong enforcement culture, laundering will continue to happen. Even if the sector could regulate itself, laundering could occur elsewhere, anywhere cash or near cash can be used, in whatever form.

In the EU context, the rules have to take into account the functioning of the single market for financial institutions and payment providers, with home-country control. They should comply with the key Treaty freedoms of free movement of capital, people and goods and free provision of services throughout. From the law enforcement perspective, the EU is much less advanced, and national legislation differs as to what may be classified simply as an administrative offence, rather than a full-blown crime. The result is that illegality does not always equate to criminality.

In order to have a better chance of securing compliance with the aims of AML, there need to be clean lines of authority. This is at its base a combination of clarity of aim and legislation, as well as political leadership. One secondary aspect is the behaviour of all the relevant groups concerned, moving the balance of benefit/cost analysis, and making better use of peer group pressure and other psychological techniques, creating a strong AML culture across the EU.[2] Another is the control dimension. This is where compliance gets expensive in terms of costs of monitoring, supervision, detection, investigation, prosecution and enforcement. So from a policy effectiveness standpoint, more comprehensive authority and an improved culture will lessen the enforcement burden. Regard must be paid to the possibility of distortions, whether by governments, for example, by ordering law enforcement to focus on money laundering relating only to missing trader intra community (MTIC) fraud (concerning abuse of the value-added tax (VAT) regime), or by markets, where CEOs, who are rewarded for the profitability of their institutions, are tempted to turn a blind eye to due diligence. Finally, avoiding error is critical, whether by instituting effective training programmes (including training of police and the judiciary in the workings of financial markets and their abuse by launderers) or by ensuring that governance structures are comprehensive, the decision-making process is smooth and justifiable, and the daily rhythm works efficiently.

3.1 International and European AML policy

The consensus to tackle money laundering stemming from drug trafficking led to the creation of the Financial Action Task Force in 1989 by the G-7. Today, the FATF is the driving force in fight against money laundering internationally. The group initially consisted of 15 OECD member countries and the European Commission, but it was gradually enlarged to include what are now the 37 member countries and a network of nine regional FATF-style bodies, totalling 205 member countries. The FATF, by setting standards and adopting recommendations, works mostly through peer group pressure but has gained considerable influence. Its recommendations are referred to in a variety of international instruments, such as the UN Security Council resolutions against terrorism and the EU's AML directives, which have in turn reinforced its legitimacy.

[2] Psychologists often categorise target groups as falling into three categories for compliance purposes. The first 20% are usually compliant and will always be so. There is another 20% at the other end of the scale, who are rarely compliant. The 60% in the middle are thought to be compliant to some degree or another, depending to some extent on their view of the benefit cost equation for them of the scenario which they face. They are the opportunists, who may decide against compliance if they feel they can "get away with it", or if they are non-compliant that the penalty will be insignificant.

Key elements of the work of the FATF are:

- Typologies of money laundering: identifying risks and methods used by criminals and terrorists to access the financial system or otherwise launder proceeds or obfuscate funding. This work has evolved from annual to ad hoc reports. Recent work focuses on virtual assets and their use in illicit transactions, and illegal wildlife trafficking;
- The recommendation to create financial intelligence units (FIUs): independent agencies tasked with receiving and analysing suspicious transactions from financial institutions and other obliged entities (by which is meant those entities which fall to be regulated under an AML regime). The FIUs are gathered internationally under the **Egmont Group**, a network of 165 countries' FIUs, for information and expertise sharing;
- A mutual evaluation process to assess the implementation of FATF recommendations. It checks, through a peer monitoring system, the technical compliance and effectiveness of a member states with 11 'immediate outcomes' (see Table 4 below in Pillar 2 Risk Management);
- A blacklisting of non-cooperative jurisdictions and public warnings about high-risk jurisdictions. The International Cooperation Review Group now regularly reviews countries that pose a risk for the financial system and makes public statements.

Despite these successes, FATF standards have been developed by a single-agenda ad hoc body with selective membership and a limited degree of transparency and accountability in its operations. FATF is an expert body that serves to depoliticise the discussion on AML typologies and measures, but happening outside the normal political processes and scrutiny. Its recommendations are presented as given, and the recommendations have been mostly adopted without criticism by the EU Commission and legislators. In this sense, the process has been legitimised at EU and global level, by FATF and non-FATF members, it is argued. The FATF is thus constrained by its structure as an intergovernmental body. Its effectiveness and efficiency could be improved by an annual monitoring of areas of criminality to identify trends, rather than focus on identifying 'new typologies'. It too could do with addressing objectives and key results (OKRs) of the regime, in order to increase effectiveness. Furthermore, it can take many years for changes to FATF recommendations to be translated into national laws and countermeasures, as the FATF has no or limited power of enforcement; it mostly works through peer pressure.

Table 1. AML multi-actor structures and networks

	Global	EU – Europe	Member states
Regulatory policy	**FATF**	EU institutions **Moneyval**	National institutions
Supervision	Basel Committee/FSB	ECB/EBA/ESAs/EDPS (EU Agency)	Central bank, FSA, specialised supervisor
Investigation	**Egmont Group**	**Europol/FIU.net**	**FIU**
Enforcement	UN/International Courts	CJEU/EPPO/Eurojust	Public prosecutors, Courts
Private sector/ NGO	Wolfsberg group International NGOs Transparency International		TMNL National NGOs
PPPs		EFIPPP	JMLIT, SAMLIT, AMLC, etc.

The EU was the first international jurisdiction to adopt a comprehensive framework on AML, following up on the FATF 40 Recommendations but through binding acts and directives, enforceable before the European Court of Justice. In the various directives on AML, the EU has followed the FATF work by gradually expanding the scope of money laundering predicate offences. Academics have compared this extension to 'a chameleon' adjusted to provide responses to every security threat arising. This raises questions regarding the observance of the principle of legality at EU level and the extent to which policy choices in these fields may lead to uncritical over-criminalisation. The danger of this approach is the failure to distinguish between the essential features behind the criminal and regulatory response to tax offences on the one hand, and serious and organised crime on the other (Mitselegas and Vavoula, 2016).

Indeed, the EU directives still do not include a harmonised definition of money laundering, which has been one of the problems obstructing proper implementation by the member states. Failure to implement fully the fourth AML directive led the EU Commission on 2 July 2020 to refer Austria, Belgium and the Netherlands to the European Court of Justice, with a request for financial sanctions. The incomplete implementation by these countries concerns fundamental aspects of the anti–money laundering framework, such as betting and gambling legislation (Austria), mechanisms under which the financial intelligence units exchange documents and information (Belgium), and the information to be provided on the beneficial ownership of corporate and other legal entities (Netherlands). Proceedings against two member states are pending before the Court, and three other member states have received reasoned opinions. Also, the FATFs assessment of the 19 EU member states implementation of its 'immediate outcomes' is mixed at best (see Table 3 below).

An overview of the five EU AML directives largely mirrors the extension of the scope of money laundering and development of the 40 Recommendations within the FATF. The function of FIUs was the subject of a separate decision.

- The First AML Directive (91/308/EEC of 10 June 1991) defined money laundering as the proceeds of criminal activity, in particular but not only from drug trafficking. It required member states to ensure that financial institutions require identification of their customers when opening an account, and for every transaction above €15,000. All the information regarding suspected transactions should be forwarded to the national authorities responsible for combating money laundering, the FIUs. It established a 'Contact Committee' to facilitate the harmonised implementation of the directive;
- The role of and cooperation among FIUs was elaborated in a Council decision (2000/642/JHA of 17 October 2000). As "there should be an improvement in cooperation between contact points competent to receive suspicious transaction reports pursuant to Council Directive 91/308/EEC", it defines the role and the modalities of cooperation between FIUs. This follows changes to improve police and judicial cooperation in the EU further to the Amsterdam Treaty (1997). This decision was recently replaced and extended by an EU directive (2019/1153 of 20 June 2019);
- The Second AML Directive (2001/97/EC of 4 December 2001) extended the scope of the previous one in terms of both the crimes covered and the range of professions and activities cited as having potential responsibility—auditors, accountants, tax advisors, real estate agents, dealers in high values, casinos, notaries and lawyers;
- The Third AML Directive (2005/60/EC of 26 October 2005) forbade anonymous accounts and obliged financial institutions to apply customer due diligence provisions, including investigation of possible terrorist financing. It repeats the obligation for member states to establish an FIU;

- The **Fourth AML Directive** (2015/849 of 20 May 2015) considerably broadened the previous ones and emphasised 'tax crimes' as a predicate for money laundering. It paid more attention to the matters of supervision and sanctioning than the preceding directives. It requires the EU to identify high-risk third countries, nations with deficiencies in their AML policies. It requests the EU Commission to make a biannual assessment of money laundering and terrorist financing risks affecting the internal market and relating to cross-border activities. It had to be implemented by 26 June 2017;
- The **Fifth AML Directive** (2018/843 of 30 May 2018) focused on enhanced powers for FIUs and supervisory authorities to obtain direct access to information and demanded increased transparency around beneficial ownership and trusts. It also extends the scope of obliged entities to virtual currency exchanges, hence covering bitcoin and other digital currencies. The member states were required to translate this directive into national legislation by 10 January 2020.

The weakness of these legal instruments is that they are in the form of directives, which leave member states broad leeway when it comes to implementation: they did not harmonise the definition of the crime and the sanctions applied, for the reasons discussed above. The advantage is that it gives member states the opportunity to tailor implementation of the directives to local circumstances, and to go further (thus enabling a risk-based approach). The fourth directive considerably enlarged the scope of what is considered a criminal offence in money laundering, extending to 'fraud', 'corruption', "tax crimes relating to direct taxes and indirect taxes and as defined in the national law of the Member States". The latter is further explained in recital 11, which states: "While no harmonisation of the definitions of tax crimes in Member States' national law is sought, Member States should allow, to the greatest extent possible under their national law, the exchange of information or the provision of assistance between EU Financial Intelligence Units." A further clarification would be required to facilitate cross-border judicial and police cooperation in this domain. Yet if tax evasion is not an offence under national law, why would an FIU exchange information?

In the meantime, the **revision of the EU treaties, the Lisbon Treaty (2009),** provided the possibility for the EU to set minimum rules, by unanimity, concerning the definition of criminal offences, which include illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment and computer crime (Article 83). This has not yet happened, however. In 2012, the EU Commission proposed a legislative act on that basis, and again in 2016, but it was not adopted by the member states, indicating that various approaches co-exist.

The draft Fifth AML Directive was accompanied by an extensive impact assessment (2016) of different options to strengthen the EU's existing framework to fight terrorism and to enhance transparency with respect to beneficial owners of corporate entities and trusts. The impact assessment only covered additional benefits that could be generated by the proposed targeted amendments but did not make an attempt to quantify the costs of regulating AML for the service providers. To our knowledge, no such cost assessment was made on the AML measures in the EU to date, but many numbers have been circulated on the basis of private-sector surveys, most often rough estimates. The 2016 report further analysed various means for better cooperation among FIUs, adding that there was no appetite among member states for an EU-wide FIU. It also looked into the impact of virtual currencies.

3.2 The new AML role of EBA in the ESA regulation review

The difficulty of making progress on the basis of Lisbon Treaty Article 83, and the need for a more harmonised approach pushed the EU to propose a more important role in AML for the European Banking Authority (EBA). This was announced as part of Commission President Jean-Claude Juncker's last State of the Union speech in 2018, as a new amendment to the Review of the European Supervisory Authorities (ESAs) regulations. The amendment was adopted by the end of 2019 and is being implemented.

The amendments give a unique central coordination and information-sharing role to the EBA, in cooperation with national authorities, the other ESAs and the European Central Bank (ECB) in the fight against money laundering and terrorist financing (Article 9a of the ESA review). The EBA has a new statutory objective to prevent the abuse of the financial system by money laundering and terrorist financing. This means that it has to consider AML/CFT issues in all its activities.

The EBA has the legal obligation to set the standard, coordinate and monitor the EU financial sector's AML/CFT efforts.

- *Standard setting*: By setting EU standards as to how supervisors and financial institutions should comply with AML/CFT rules in a proportionate, risk-based manner, EBA can ensure that these are implemented consistently and effectively across the EU. The amendments create a new Standing Committee within EBA, the AMLSC, to coordinate measures and to prepare all draft decisions for the Board of Supervisors (see the mandate). It is composed of member states' relevant authorities, a representative of the other ESAs and the ECB.
- *Coordinate*: The EBA established new supervisory colleges of AML/CFT supervisors, which in some instances convert existing ones, to foster effective cooperation and information exchange between competent authorities responsible for AML and prudential supervision, as well as with other authorities, like FIUs:
    - This gives supervisors much more information on risks and allows them to learn from each other more quickly and effectively;
    - FATF considers AML/CFT colleges an international good practice;
    - The EBA participates in the discussions and monitors them. It also provides feedback to the competent authorities on the functioning of the colleges and on other issues, including the supervision of particular institutions;
    - If there is a third-country dimension, the EBA will have a leading coordination role. In case a country or dependency is on the list of non-cooperative money laundering jurisdictions, the EBA shall not conclude equivalence agreements (Article 33, ESA review). This may soon raise problems for the UK in its dealings with offshore financial centres in British Overseas Territories, such as the British Virgin Islands, Cayman Islands and Gibraltar.

  All necessary colleges should be set up by January 2022.
- *Monitor*: EBA shall develop draft regulatory standards to identify risks and vulnerabilities in AML/CFT supervision, as well as standards on information sharing between competent authorities. In February 2020, the results of the first round of the EBA's AML Implementation review were published. They assess the approaches of a selection of competent authorities and issue recommendations for all supervisory authorities.

The EBA has also been given the power to:

- Ask competent authorities to **investigate individual financial institutions** when it believes that they are in breach of AML rules, and to consider imposing sanctions (Article 9b, ESA review). Where an authority does not comply with the request, the EBA may take direct action toward the financial institution in question (Article 19e).
- Carry out **peer reviews of competent authorities** on their fitness to tackle AML risks.
- Set up a central **AML/CFT database** to collect and store all information on weaknesses of individual financial institutions' systems that competent authorities have identified. The database will be used to analyse risks and share information. There will be a technical consultation at the end of this year or the beginning of next year.
- Where appropriate, transmit information to the new European Public Prosecutor's Office (EPPO).

EBA resources for AML have increased with introduction of the new rules (from two to seven full-time staff up to thirteen full-time staff in 2021). Twenty EBA staffers are trained on AML/CFT issues in relation to prudential supervision, governance and internal control. However, considering the broad scope of the EBA's mandate, these resources remain limited when compared to the depth of the problem and the number of persons working on prudential supervision at EU level, for example. At national level as well, insufficient resources dedicated to supervisors are a concern.

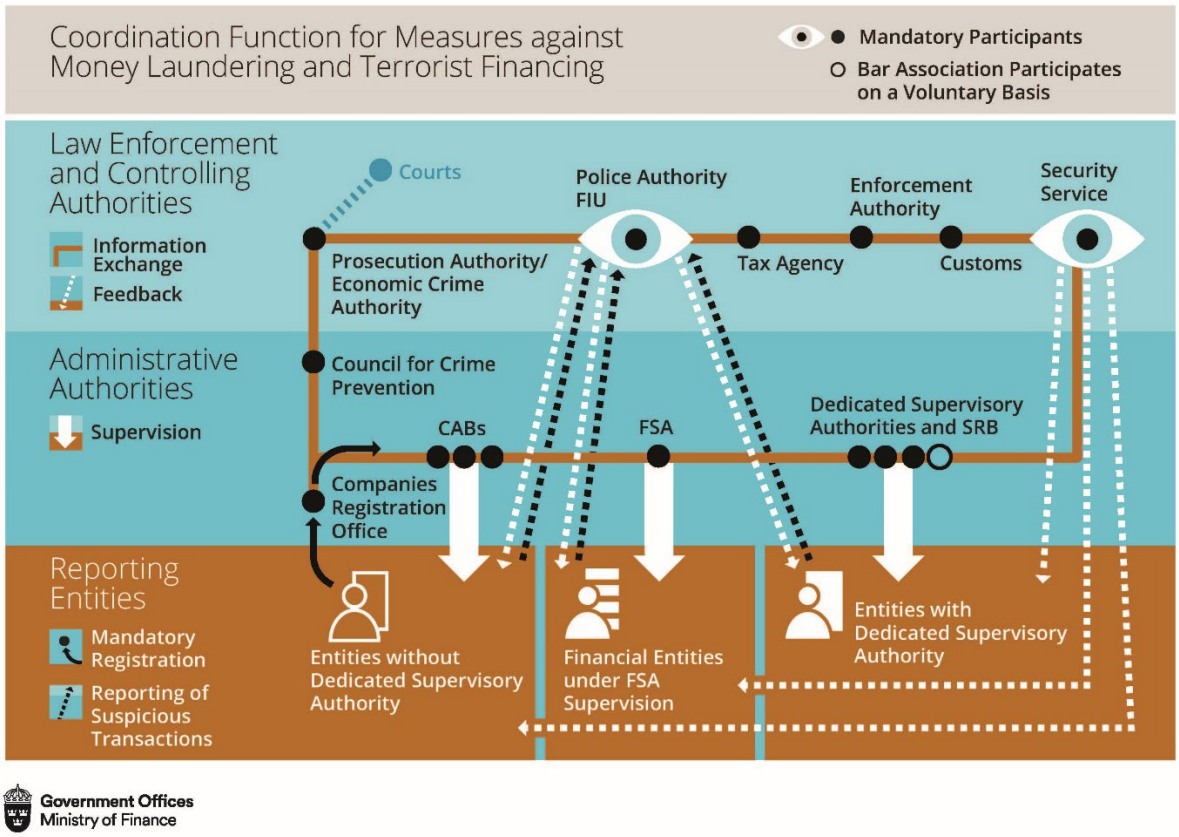
With minimum harmonisation of the several AML directives, the potential for EBA to lead the way is limited. However, the new powers signal a move away from merely aggregating information toward a more proactive, preventive role. They strengthen information sharing and the supervision of individual financial entities.

4. Pillar 1 AML Supervision

4.1 AML supervision in the EU member states and the role of the SSM

AML supervision is organised differently in the various EU member states, which renders EBA's coordination task more difficult (see Table 6 at the end). The newly created AML Standing Committee of EBA brings together 57 different authorities from EU and EEA member countries in the financial sector alone. Two models can be distinguished, one with the central bank in charge, prevalent in the majority of member states, the other designating a Financial Services Authority (FSA) for supervisory purposes. In between are several hybrid models. This heterogeneity could be an argument for a single entity at European level, but it could also indicate how difficult it might be to have such an entity function efficiently, if responsibilities are spread over different competent authorities. Equally, a certain flexibility is required if implementation of a risk-based approach is to work for supervision. It is a fine balance to achieve, which needs to be guided by agreed objectives and results. On the non-financial side, the supervisory structure is even more complex, and depends on how a given profession is organised and how AML legislation translates in action, which is often carried out in a self-regulatory way. The Wirecard case, the payment company that went bankrupt, indicated that much remains to be done in the supervision of the audit profession. But there are also the accountants, notaries, gaming industries, real estate brokers, etc. Table 2 gives an overview of a national supervisory structure in the case of Sweden, for example.

Table 2. The AML supervisory structure in Sweden



Note: This graph depicts the Swedish system for combating money laundering and terrorist financing, as regulated chiefly by the Act on Measures against Money Laundering and Terrorist Financing (2017:630). The entities without a dedicated supervisory authority are defined in items 15–16, 18–19 and 21–22 in the second section of the Act and are subject to supervision by the County Administrative Boards of Skåne, Stockholm and Västra Götaland. The entities with a dedicated supervisory authority are defined in items 13–14, 17 and 20 in the same section and are subject to supervision by the Estate Agents Inspectorate, the Gambling Authority, the Inspectorate of Auditors and the Bar Association.

Source: Government Offices of Sweden.

Apart from EBA, member states are grouped in different constellations in other international fora, such as the FATF and Moneyval. There is no shortage of international networks, as show in Table 1 above.

Analogy is often made to the Single Supervisory Mechanism (SSM) to point to what an overarching agency could do in the domain of AML. Through the creation of the SSM within the ECB, the EU managed to overcome the diversity of prudential supervision structures in the member states and create a unitary body. An SSM-like structure could be set up by the EU for AML, with the supervision of the large cases (like the large banks) by the single agency, whereas small cases would be left to the member states. The big problem, however, is that the lists of the predicate offences to money laundering must refer to national law, and this is where the analogy with the SSM ends. The ECB can act directly all over the Eurozone, through the withdrawal of a licence in case EU law was violated, which an AML authority could not do since that particular competence remains national under the EU Treaty.

At the same time, the SSM model raises questions about the role of the SSM itself. The SSM regulation limits the ECB's task to prudential supervision of banks, while it notes in recital 29 that "the ECB should cooperate, as appropriate, fully with the national authorities which are competent to ensure a high level

of consumer protection and the fight against money laundering." The SSM may, in its day-to-day tasks, come across many cases that could help to uncover money laundering, which need to be followed up as closely as possible. The ECB says that it takes into consideration the assessments of the AML/CFT supervisors in its prudential control. It can for example ask banks to strengthen governance arrangements or reassess board members and principal functionaries. The ECB can, as part of its fit and proper assessments, reject board members outright, although it depends on national authorities to share information on personal tax files.

Ultimately, either national supervisors or the ECB can withdraw a banking licence in case of serious doubts about the business model of a bank, which the ECB did in the case of ABLV bank in July 2018 (see below). However, it did so only after the U.S. Treasury in February uncovered blatant money laundering. This raised questions about the possible conflicts of interest within the ECB, as the governor of the central bank of Latvia should have been aware and sits on the Governing Council of the ECB. It led the ECB to publish disclaimers about its responsibility and limitations as prudential supervisor in case AML breaches occur. Several commentators argued that the ECB should have known, and called for a bigger role for the ECB in this domain. At the initiative of the ESAs, a multilateral agreement was signed in early 2019 between the ECB, the national competent authorities and the AML/CFT supervisors of banks in the EEA to clarify the exchange of information: it sets that the ECB and national competent authorities will share information with AML/CFT supervisors in member states and requires assessments from AML/CFT supervisory authorities at least once a year to support its annual supervisory review process.

4.2 The role of the FIUs and Europol

Less well known but critical to AML supervision is the role of the FIUs, and of Europol as the host of the network of FIUs. FIUs collect information about suspicious activity and some of them cooperate in cross-border cases at the EU level with Europol, the European law enforcement agency. FIUs channel the information to the judicial authorities, but the overall recovery of illicit assets is not very effective (the rate of confiscation of criminal assets could be as low as 1.1% according to Europol).[3] One of the central reasons for this lack of success is complexity in enforcement, with many different authorities and agents involved (bank supervisors, FIUs, tax authorities, customs, judicial authorities, etc.), which have different powers, history, structure, culture, training, tools and resources across the member states. The EU has a single market but not a single enforcement and judicial area. Improving cooperation among law enforcement and judicial authorities, and ensuring adequate resources and training, is essential.

An FIU is "a central, national unit which, in order to combat money laundering, is responsible for receiving (and to the extent permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information which concern suspected proceeds of crime or are required by national legislation or regulation" (EU Council Decision 2000/642/JHA). FIUs process suspicious transaction reports (STRs) and suspicious activity reports (SARs) and forward these to the judicial authorities. FIUs are most often part of finance ministries, a few of them being law enforcement bodies or located in the judiciary, but in some cases they are stand-alone independent agencies (see Table 6 for an overview). The EDPS called for a clarification on this point so that they do not include the police or judicial authorities.

[3] Europol, Does Crime still pay? Criminal Asset Recovery in the EU, Survey of Statistical information 2010-2014, 2016, p. 4.

There have been long-standing problems with the functioning of FIUs: lack of staff, lack of information technology tools, competing demands, lack of cooperation from banking supervisors, and the undependable quality of intra-EU police reporting and coordination. The FIUs are nationally focused, and they are overwhelmed by thousands of STRs. Common templates for STRs, tools and standards, and support of joint analysis and training are being considered. At the same time, flexibility needs to be maintained and bureaucracy kept under control. The European Commission is examining various potential solutions. A single point of data gathering for STRs was proposed, but FIUs and national regulators are said not to be in favour of centralised filing. Their reasons include linguistic barriers, legal issues and subsidiarity, as well as the decentralised nature of markets, security and data protection. But also the ever-expanding and unclear money laundering concept in EU law makes it difficult for FIUs to focus.

A Commission report on cooperation between FIUs sets out the scale and the depth of the problem:

- Many FIUs face big operational problems, primarily related to funding but also to their structure and role. Trying to resolve these butts up against legal limitations in many member states;
- The number of SARs made by reporting entities to FIUs is very dissimilar across the EU, although reporting has improved greatly in recent times (see Table 7);
- Exchange of information between FIUs and cross-border reports have been sparse, although here, too, there has been improvement recently. FIU.net was set up for that very purpose, but it faces recurring problems. The EU Commission is currently looking into an appropriate structure for FIU.net, as Europol was judged no longer to be appropriate by the supervisor EDPS because of data privacy, and its mandate;
- There is a need for more centralised monitoring of and support for FIUs;
- Cooperation with prudential supervisors is currently extremely limited, often related to issues of confidentiality.

Overall, it seems that the immediate problem for AML enforcement rests more with the FIUs, and the structure of cooperation among them, than with the financial supervisors. However, once these issues are sorted out, problems relating to judicial systems and prosecutorial authority will become more apparent.

4.3 AML and related policies

4.3.1 GDPR and data sharing

The iconic **General Data Protection Regulation** (GDPR) of 2016, the pillar for data rights in the EU, is often seen as an obstacle to AML policies. However, in several of its provisions, GDPR is intended to be enabling in nature: it is not intended to block data processing but to ensure when and how data processing can be lawful. When in the public interest, the GDPR allows member states to restrict certain obligations and rights. Boldness and creativity should thus be encouraged in the field of AML to find practical ways to observe data protection principles while sharing information. Coordination between AML and data protection agencies and the setting of clear and simple guidelines is vital.

The GDPR provides flexibility. Several provisions foresee making exceptions to data protection rules, in particular by allowing restrictions of individual rights when those are necessary in the fight against money laundering (recital 19, for example). Processing of data can be lawful for compliance with legal

obligations to which the data controller is subject (Article 6.1c) or for the performance of tasks in the public interest (Article 6.1e). In these cases, the right to be forgotten does not apply (Article 17.3). The rights of those subject to data collection, in particular, the rights of access, correction and blocking, can also be restricted by law if doing so is necessary and proportionate (Article 23). In addition, the European Court of Justice has recognised that AML can justify restrictions on human rights, which are also applicable for data protection. Nonetheless, the practicalities need to be tested more fully.

AML legislation has never been considered particularly problematic by data protection authorities. However, in the early days, the data protection authorities of at least one Member State judged that individuals had a right to see the information disclosed about them in a Suspicious Activity Report. This is clearly at variance with tipping off provisions and under certain laws gives rise to an action for defamation. For the AML system to work, however, those disclosing suspicions need to have legal immunity from suit for breach of data protection laws and defamation laws. FIUs and those involved in the law enforcement process need to ensure that this sensitive information is held securely and not breached or leaked. However, in recent years, data processing and sharing measures have become more invasive by nature, with lower reporting thresholds, advanced technology and increased use for electronic payments, which allows banks and other providers to collect more information. A greater interest from the public in the impact of AML measures on personal privacy is expected, increasing the importance of explaining necessity and proportionality and setting clear and acceptable guidelines.

Data controllers are accountable (Article 5 of the GDPR) for the processing of personal data. The responsibility to prove compliance lies with operators rather than supervisors. This can be achieved through documentation, data protection impact assessments, appointment of a data protection officer or other means.

As regards proportionality, the European Data Protection Supervisor (EDPS), in charge of controlling the correct application of the GDPR, has issued guidelines on proportionality and a Necessity Toolkit. The EDPS encourages the following of a risk-based approach, clearly identifying the criteria for the assessment of money laundering risk and encouraging the use of these criteria when drafting and submitting SARs.

The EDPS is the data protection supervisory authority of Europol, monitoring the processing of personal data relating to Europol's activities. It is responsible for hearing and investigating complaints from people who believe that Europol mishandled their personal data. Europol relies on national competent authorities to provide them with the majority of the personal data it processes. Because of Europol's current legal framework, the EDPS ruled that the decentralised network of FIUs (FIU.net) can no longer be hosted by Europol, as FIUs often deal with many suspicious activities outside the context of criminal law, and the framework for the exchange of such information between member states on FIU.net is inadequate. The European Commission is temporarily taking over the function of hosting the FIU.net system and assessing what form the future cooperation and support mechanism for FIUs will take.

In its opinion on the EU Commission's May 2020 AML communication, EDPS argued that public/private partnerships (PPPs) for the sharing of operational information on intelligence suspects by law enforcement authorities with obliged entities would result in a high risk for privacy rights and data protection. It also advised the Commission to be careful not to overstep the legal basis for PPPs to process personal data. Hence, while data sharing is increasingly seen as the way forward, the EDPS has warned strongly against it.

4.3.2 Integrated identification solutions

The upside of GDPR is harmonised, eventually digital, integrated identification. While a lot has been done already by the EU in this domain, with the Electronic Identification, Authentication and Trust Services (eIDAS) solutions and the Ultimate Beneficial Owner (UBO) registry, and internationally through the Legal Entity Identifier (LEI), much remains to be done, certainly for FIUs. Correct and comprehensive application of these measures remains an issue, and too many private entities and countries continue to protect secrecy even in situations where it is unwarranted.

Under the Fifth AML Directive, varying national customer identification and verification requirements are applicable across the EU. Fragmented national approaches to digital identity solutions are detrimental to the development of innovative cross-border solutions and the provision of cross-border financial services, adding to their costs and obstructing the fight against money laundering, as obliged entities need to collect data differently in each country. This is exacerbated by:

- a myriad of identification and verification processes, which implies using different documents and formats;
- diverse additional requirements, such as the use of certain delivery channels;
- differing access rights or abilities with respect to public information that could be used for verification purposes;
- constraints with respect to the portability and the reuse of customer due diligence data because of distinct approaches in member states toward reliance on third parties and uncertainties with regard to the application of the GDPR. As a result, there is little recycling of these data.

The Fifth AML Directive requires member states to open up access to registries of the UBOs of companies, but there are still too many practical difficulties. Information can be incomplete or misleading. Access to and transparency of registries is not uniform. Arrangements can be made with third countries where identification is more difficult, such as Switzerland. Implementation of the directive in the member states is behind schedule: 17 of the 27 member states do not yet have a centralised registry with the beneficial owners of companies that is available to the public. Twelve member states have legal arrangements that allow the hiding of the UBO, according to a recent European Commission report.

The use of a Legal Entity Identifier, mandated by the Financial Stability Board (FSB) since the 2008 financial crisis, could help to identify the UBO of entities, but here as well, much remains to be done by FSB members to disseminate its use. The LEI is an alphanumeric code developed by the International Organization for Standardization (ISO) that enables clear and unique identification of legal entities participating in financial transactions. It serves to resolve inefficiencies in financial ecosystems like high costs due to matching based on names and weak controls, and adapts the name-based system to the digital world. It can facilitate retrieval of granular data from a variety of sources.

Most FSB members' jurisdictions have mandated that certain entities have an LEI. It has a coverage of close to 100% for derivatives markets, as well as a high percentage of securities and fixed-income markets, but its use remains far too low with respect to non-financial corporations. Only 1.77 million LEIs have been issued around the world to date. "LEI has far to go to meet the G-20's objective", according to a recent FSB report. Its utilisation is uneven across countries: it ranges from 2% to 7% of all eligible legal entities in Canada, the EU and the United States but is much lower elsewhere. More effort should be made both at national and international levels to promote LEI adoption.

For AML purposes, an LEI could contribute in five ways to making compliance more efficient and accurate:

- Facilitating know-your-customer (KYC) processes, especially on a cross-border basis;
- Facilitating more efficient screening and a reduction in false positives, enabling screening of real-time transactions;
- Simplifying the management of lists;
- Providing enhanced data analytics by using LEI as a correlation identifier;
- Enabling more reactive capacity and better communication across investigative organisations;
- Serving to validate beneficial owners where they have legal identifiers.

GLEIF, the global foundation behind LEI, is working to use LEIs within digital certification systems and is devising a company identity that will give a person a one-stop verifiable credential that proves that he or she is representing a company. However, care should be taken to ensure that users are aware of LEI limitations, such as an erroneous interpretation that those with an LEI are somehow guaranteed to be free of financial crimes.

For LEIs to be useful, adoption has to become more widespread, which requires sustained effort internationally.

4.3.3 Fair taxation

Somewhat surprisingly, **tax avoidance** only came up more recently in the scope of AML legislation, in the context of the Fourth AML Directive of 2015. The EU has also enacted legislation separately, following international focus on base erosion and profit shifting (BEPS), in the anti–tax avoidance directive of 2016 to ensure effective taxation. However, recent debates have shown that EU countries still have a long way to go since tax systems differ significantly in the EU, not just in relation to how they function but also in what is tolerated in terms of tax avoidance. An EU-wide fair taxation system, where different revenues are taxed evenly, remains far off.

Corporate tax law harmonisation has barely advanced in the EU over recent years but has been more the subject of soft law measures, by which coordination among member states is promoted, as well as through state aid policy actions. In this way, the biggest distortions are addressed. But effective taxation is a moving target because of economic developments, such as in the digital economy and the growing importance of intangible asset classes. This makes tax systems no longer adapted to the new dynamics of generating revenues.

Overall, average corporate tax rates have declined, whereas personal income tax rates have remained stable or even increased, which raises an issue of equity. When large corporations can easily avoid or minimise taxes through international tax planning, and if on top of that the system is no longer adapted to the increasing weight of intangibles, there is an urgent policy problem to be addressed. At international level, this is mostly in the hands of the Organisation for Economic Co-operation and Development (OECD), which has been successful in addressing technical aspects of corporate taxes, such as transfer pricing, has taken action with regard to BEPS and is advancing on digital taxes. Work on blacklisting non-cooperative jurisdictions or tax havens has become more political, as the list was dropped in 2009, from 38 jurisdictions in 2000. The same process is happening in the context of the FATF non-cooperative jurisdictions initiative, where the blacklist is likewise becoming shorter.

The EU has in some sense followed the OECD. It also has **two lists, an EU list of non-cooperative tax jurisdictions** and **an EU high-risk third country (anti–money laundering) list**. The tax jurisdiction and AML lists may overlap in terms of some of the countries they feature, but they have different objectives, criteria, compilation processes and consequences. The EU's non-cooperative tax jurisdiction list is in the hands of the EU Council, whereas the EU's AML list is established by the European Commission based on EU anti–money laundering rules. The high-risk third country (AML) list aims to safeguard the EU's financial system against excessive exposure to third countries with deficiencies in their AML/CTF regimes. Based on this list, banks and other obliged entities must apply higher due diligence controls to financial flows involving the high-risk third countries, if not they risk penalties or sanctions. It includes countries such as the Bahamas, Mauritius, and Pakistan. The EU list of non-cooperative tax jurisdictions deals with the problems of potential erosion of member states' tax bases posed by third countries that do not comply with international good governance standards as applied to taxation. It is managed directly by the member states, through the Code of Conduct Group, with the support of the Commission. The list is composed of a grey list (including i.e. Morocco) and a separate black list (including i.e. Cayman Islands), the former of which responded to EU concerns on the way to being cooperative. The EU states that, as a result of this process, which started in 2017, 120 harmful tax regimes worldwide have been eliminated, and dozens of countries have started to apply tax transparency standards. This has enabled the EU to confront tax avoidance by individuals and corporations (see the statement of Commissioner Paolo Gentiloni).

4.4 Recent EU initiatives

The **European Commission** has recently been active on the AML front. In its recent Action Plan, it proposed 1) to turn certain parts of the AML directives into a regulation and 2) to consider creating an EU-wide body to deal with AML, to ensure better implementation and compliance with the rules. It also calls for 3) having a single rulebook, through delegated acts and addition of provisions in other rules to ensure consistency for AML purposes. On the 4) law enforcement side, it proposes a more formal network for FIU.net and a mechanism for information exchange across jurisdictions, while respecting data protection. In the 5) international sphere, it proposes that the EU speak with one voice in the FATF, for better protection of the EU's financial interests.

In a July 2019 communication, the Commission had already hinted at the creation of an EU-wide AML body. It also published a report on recent money laundering cases involving EU credit institutions, in response to an EU Council request, and a supranational risk assessment report with regard to 47 products and services falling under 11 different sectors that are considered potentially vulnerable to money laundering/terrorist financing risks (see Table 5 at the end). The first report concluded that many of the banks examined pursued chancy business from an AML/CFT perspective, without establishing commensurate controls and risk management. The second report found that many products/services pose significant risk. Moreover, while coordination for the financial sector as per EU Commission recommendations is effective, this is not so for the non-financial sector, where the oversight framework is very patchy, covering tax advisors, auditors, external accountants, notaries, and other independent legal professionals and estate agents. The report adds that, to date, no member state has made any notification to the Commission concerning the first report on the supra-national risk assessment of money laundering.

Neither the Action Plan nor the 2019 communication make any mention of the ECB's role for AML as prudential supervisor in the Single Supervisory Mechanism. If a single entity has to be created, the

easiest way is to do it within or close to the ECB, which has the expertise and the legal basis (although formally this is limited to prudential supervision and financial stability) and can act more independently vis-à-vis member states than can the EBA. Back in 2012, when discussion about further reform of banking supervision took place, the European Commission likewise did not consider giving the ECB a bigger role, leaving the matter aside until the member states decided otherwise and created the SSM.

The **EU Council** gave a strong political mandate to the Commission to resume pursuit of structural change in oversight in its conclusions of 5 December 2019. It identified a range of shortcomings with respect to banks, AML authorities, prudential supervisors and intra-EU cooperation and concluded that there is fragmentation in both AML rules and supervision. The Council therefore called upon the Commission to address some AML deficiencies through a regulation and to analyse the pros and cons of an EU-wide body in this domain. It also underlined the need to strengthen the coordination work carried out by the EU Financial Intelligence Units Platform. This was reiterated in the conclusions of 5 November 2020, with a clear endorsement for an EU supervisor. Before that, the EU Council had adopted its own AML action plan, which relied more upon the ESAs, and EBA in particular, called for cooperation between the different supervisors in the supervisory colleges and recommended integrating AML/CFT into the prudential supervisory process. The ministers asked for a "post-mortem" review of recent AML cases, in the wake of the Den Danske case in 2017-18, which involved about €200 billion in suspect transactions channelled through the Estonian affiliate of the bank over the preceding decade.

To add to momentum toward creating a unitary agency, **six EU member states—the five largest and Latvia** — called in a joint position paper for a European supervisory mechanism to prevent money laundering and terrorist financing. It foreshadowed the European Commission's communication by advocating for a set of harmonised, directly applicable rules and a new layer of supervision, comprising of a dedicated central supervisor that controls the high-risk financial institutions, or alternatively a separate committee within EBA that builds on its new powers but is "exempted from the one country one-vote rationale and distinct from the current EBA governance for prudential supervision" (joint position paper, p. 4). This proposal is limited to the financial sector, but the hope is that it "can provide important input for ML/FT mechanisms in other sectors." Other elements in supervision, such as FIUs and law enforcement, would remain at the national level.

The **European Parliament,** for its part, in a July 2020 resolution welcomed the proposed changes to the EU AML institutional structure, based upon "its deep concern regarding the EBA's ability to carry out an independent assessment owing to its governance structure". The Parliament focused more on the tax dimension of AML and prescribed a "European framework for cross-border tax investigations and other cross-border financial crimes". It criticised 'golden visas', asking member states to "phase out all existing citizenship by investment (CBI) or residency by investment (RBI) schemes as soon as possible".

4.5 Assessment

Better implementation is the key to making AML policy work, but the concept of money laundering is elastic, and the regulatory and supervisory framework complex, as it stretches over different policy areas. The main problem lies with the member states, or with the mixture of pure single market and more intergovernmental competences at EU level to ensure proper interaction between the authorities involved. Yet even purely at the national level, this is not working effectively or efficiently, so how could an EU body work better, and what powers would it have? Given the Lisbon Treaty, they will need to be

limited to domains where the EU has clear authority, taking into consideration the 'Meroni doctrine', concerning the appropriateness of delegation of EU responsibilities to regulatory agencies. An EU entity would have difficulties in deciding on sanctions, or in having assets frozen, for example. This is where problems start.

Looking at the policymaking process, the benefits of up-to-date AML policies are evident in higher revenues for the state, greater transparency and confidence in economic life, better public accounts, reduction of crime, increased public safety and health and, more broadly, the cohesion of civil society and legitimacy of states. However, as indicated earlier, the success of the policies adopted thus far is minimal, and the cost of compliance, for both public and private sectors, is growing. A recent estimate set compliance costs at €81.4 bn for four EU countries alone, with proportionally larger costs for bigger firms. The effectiveness and impact of policy intervention remains to be publicly explained, it has been argued (Pol, 2020). Hence, before considering further measures and an eventual European agency, a profound review of the approach taken so far is required. A far better understanding of underlying criminality is essential, together with rigorous benefit/cost analysis and regulatory impact analysis.

Turning the directive, or parts of it, into a regulation may help resolve the inconsistencies in interpretation and practical application, though not entirely on its own. There is the ever-expanding concept of money laundering in EU law. A regulation will give the impression that all is set at EU level, but can still leave open important options for national implementation, hence undermining its impact, as is the case in the 2014 statutory audit regulation (EU 537/2014), for example. The regulation should advance a more proportional risk-based approach in AML, which is critical, rather than increasing box ticking and compliance costs for banks. This will require a thorough dialogue with the private sector on its formulation.

More immediately important is ending the deadlock in how FIU.net is handled. The functioning of FIUs is the main current bottleneck in AML, and requires an urgent initiative to adapt them to the single market, to increase adoption of technology and benefit from all the concomitant advantages. FIU.net should operate a centralised platform that enables activity and behaviour patterns to be identified, and action to be taken.

The initiatives of some member states to bring together the different entities involved in AML/CFT from the private and public sectors in a joint task force are worth emulating to allow for a more efficient EU-wide approach. In the United Kingdom, the Joint Money Laundering Intelligence Taskforce (JMLIT) established a public/private partnership, taking a holistic system approach against economic crime. This was followed by similar arrangements in The Netherlands (AMLC), Sweden and Denmark. At EU level, it led to the very recent creation of EFIPPP, Europol Financial Intelligence Public Private Partnership between FIUs and banks.

AML policy is strongly related to unfinished single-market policies, such as corporate taxation and company law. In both these areas, there is strong resistance to synchronisation from the member states, and whatever certain states may want in terms of more effective AML policies is negated by the diversity of corporate tax regimes and facilities to create shell companies, and the limited or nonexistent transparency of UBOs. Moreover, corporate tax harmonisation requires unanimous decision among the member states. Progress on the Common Consolidated Tax Directive proposal would be a good step indicating that EU members are earnest about tackling money laundering.

In relation to the non-financial sector, there are no entities at EU level corresponding to the European Supervisory Authorities. For tax advisors, auditors, external accountants, notaries, independent legal professionals and estate agents, there are no European authorities, but mostly self-regulating entities based nationally with sometimes loose cooperation at the EU level.

In the realm of law enforcement, cooperation has advanced a lot since the Lisbon Treaty was adopted. Important differences remain, however, as to what is considered tax crime for money laundering in the EU member states and which penalties should apply. There are countries with severe sentences for tax crime but lenient ones for money laundering and countries in which the reverse is true, as well as countries where both crimes are sentenced similarly (Unger, 2020). To make this work at the European level is extremely difficult, as seen in the case of implementation of the European Arrest Warrant. The establishment of the Office of the European Public Prosecutor (EPPO) will advance matters, but it will only deal with matters affecting the EU's financial interest, at least to start with.

5. Fault lines in anti-money laundering

Money laundering has become a serious concern among financial institutions. Although action to combat it has been taking place for about 30 years, it is only more recently, and partly as a result of some high-profile cases, that it has become a top priority. AML should be part of basic risk management in all governments and all financial institutions, it should be reflected in the governance structure with integrated, proactive, aggressive and interoperable defences, as well as externally, in the supervisory structure. In practice, recent cases demonstrate that there are serious fault lines in compliance.

5.1 Recent high-profile cases in AML

European authorities have recently stepped up their actions against money laundering. The most well-known cases recently involve Nordic banks, in dealings through entities in the Baltics with Russia. U.S. authorities have been active for a longer time, using a somewhat different focus, with an enormous fine levied against the French bank BNP Paribas in 2014, for example.

The way banks respond to these cases differs significantly from organisation to organisation. It is only recently that public reaction has led to pressure on banks to become more proactive in publicising their AML policies. This may be a good step toward finding the right approach in policy-making, but not if it reveals an organisation's defences to the criminal fraternity. At the same time, it should be noted that the public furore has focused on the banks' role as gatekeepers, and the impact on underlying criminality has been almost entirely absent from media coverage. A sense of balance, cooperation between the various organisations fighting money laundering, be they public or private, needs to be restored.

The most well-known recent case is undoubtedly Den Danske Bank, given the total amount that passed through the bank's books, about €200 billion in transaction flows between 2007 and 2015. The scheme concerned the transactions of 15,000 non-resident clients originating from the Estonian branch of the bank, which was brought to light by a whistle-blower. This raised questions about the role of the Danish FSA and the functioning of the supervisory college of the bank in the Nordics. But the bank is the only one that disclosed total flows in relation to non-resident customers, and therefore difficult to compare with others. Other banks have, and only in some instances, published actual money laundering or

transactions that violated sanctions, numbers that are by their nature much smaller. The Chairman and CEO left the bank ultimately.

In a report on the case, the Danish FSA proposed the following as remedies: 1) better and more effective lines of defence in banks; 2) duty to disclose and criminal liability, as well as improved protection of whistle-blowers; and 3) tougher consequences when bank management fails to live up to its responsibilities. As to the European dimension, the EBA board examined the case, but it concluded there was no breach of EU law by the Danish FSA in applying the AML directive and in not properly supervising the bank. EBA did so believing partly that an action against the regulator was not the correct instrument in a case that had happened five years earlier. This raised some concerns since the bank, and indirectly also the Danish FSA, reacted too little and too late in response to the whistle-blower's complaint. The EU Commission did not accept the EBA's decision but has not acted further thus far.

The attention paid to the case, however, demonstrates the debate focuses on the symptoms rather than the causes. The criminal gangs concerned, and the impact of the money laundering scheme on society and commerce, have largely been absent from discussion. It does need to be recognised that banks and other obliged entities can only do so much against laundering operations as gatekeepers. Bank staff are not trained investigators or detectives, and they are not law enforcement; they perform a vital function for society in oiling the wheels of the global economy. In the early days of AML, law enforcement was better resourced and supported, politically, financially and technologically. It penetrated criminal gangs and followed the money trail. The banks provided evidence of the transactions necessary to convict. News of the busting of large criminal networks was made public.

More recently governments' strategy seems to have changed from one of requiring banks and other obliged entities to sift the electronic and other records for evidence of criminality, to being held to blame when money laundering operations are uncovered. This change in strategy is unhelpful. There is little or no impact on underlying criminality, save for encouraging its growth. The cost savings for governments in terms of reduction of the size of financial crime police units is more than outweighed by the massive increases in compliance costs for the financial sector, reducing access to financial markets for honest borrowers (witness the rise of alternative financing methods as a reaction to more cautious bank lending), and the economies of member states lose out in balance and in the long term. Banks have been forced to pay massive fines. Although transparency is seen as key in fighting criminal pursuits that lead to money laundering and corruption, there is no transparency offered by regulators or governments as to how the revenue generated by fines has been used. Curiously, all governments simultaneously claim there is no money available to support financial law enforcement. This strategy must change, not only to protect the populace against terrorist bombings, cybercriminals, drug overdoses and the like, but also to support action against environmental crimes, as well as for the sake of enhancing economic growth.

The table below demonstrates the large differences among individual cases, and the responses by the banks, shareholders and the authorities. In some cases there are fines, in other cases settlements for undisclosed violations. In still other cases, decisions are yet awaited. This points again to the difficulty of having a streamlined, EU-wide (let alone global) approach, in the face of very different legal systems. The cases mentioned, but also others given less attention, have led to a sea change in AML risk management within the banks concerned, which is analysed in the following section.

Table 3. Recent high-profile cases in AML in the EU banking sector

	Year	Case	Impact	Fines	Sources
Swedbank	2020	Failure to apply AML procedures in Baltic subsidiaries on about €37 bn of transactions between 2014 and 2019	New CEO and management team	€360 mn fine by Swedish FSA for failure to apply AML rules	Report and detailed explanation on company's website
ING	2018	Failure to apply AML procedures (total amount not disclosed)	No discharge of board members for 2018 accounts. CFO steps down	Settlement of €775 mn with Dutch authorities	
ABLV (Latvia)	2018	Unclear: involved in more than €1 bn in criminal money laundering	ECB withdraws licence; bank liquidated	Unclear whether case led to lawsuits	AML policy on company's website
Den Danske Bank	2018	Failure to apply AML procedures on about €200 bn in transactions through its non-resident accounts from 2007 to 2015 in the Estonian branch	CEO, chair and several managers and employees left the bank. Estonia operations were terminated. Improved procedures	Ongoing, preliminary charge by Danish authorities; lawsuits by private investors as well	Report by Danish FSA and report by the bank, detailed explanation on company's website
BNPParibas	2014	Transactions with countries blacklisted by United States	US authorities required certain senior staff to step down	Settlement with U.S. authorities of $9 bn	Report by the French Assemblée Nationale

5.2 A confused AML risk management framework

EU rules require credit institutions to have governance arrangements in place to ensure sound and effective risk management. Internal control mechanisms should prevent failures, such as money laundering, in the compliance framework. But the cases highlighted above, as well as others, point to huge deficiencies in putting these frameworks into place. This was analysed in a 2019 European Commission report. It sees weaknesses in the different **lines of defence** that a bank is recommended by regulators to have in place to counter money laundering. These lines of defence consist of:

- **The front office**: recognising or reporting suspicious customers and types of transactions.
- **Risk management and compliance**: ensuring that the front office, at all levels, is duly informed and clear procedures are in place. Units are properly staffed to respond and comply with the rules. They follow the procedure of submitting suspicious transaction reports to the local FIUs. Senior management is informed and acts in cases of failure.

- **Internal risk audit**: a unit that controls (1) and (2) independently from management, with a direct reporting line to the audit committee and executives. The internal audit should allow for the raising of a case by a **whistle-blower**, who should be protected in so doing.

For large banking groups, which are thought to be the primary targets for money laundering, though no proper research has been conducted on this, the challenge is to have these policies consistently applied at corporate level, in the EU and third countries, in branches and subsidiaries, and in correspondent banking relationships. The variety of organisational models of banks, the degree of integration of control systems in often merged cross-border entities, and diverse administrative requirements and languages makes this problematic for compliance departments to monitor. Indeed, large banks are often collections of smaller entities that have been bought out or merged, with little attempt to create a truly single identity or culture, and often with a plethora of legacy systems. To improve the organisational strength of such entities, regulators need to be more assiduous in ensuring there is a plan, resources and the will to consummate bank mergers so that they can operate more efficiently and protect themselves better against financial crime. Sadly, this need is usually overlooked. Such policies often clash with commercial and customer onboarding objectives, or create conflict among bank staff. In the case of Den Danske Bank, for example, the laundering happened at the Estonian branch, where employees actively covered up violations, which were insufficiently held in check by headquarters. The information technology system of the branch was not integrated with the rest of the group. The branch fell under the watch of the Danish FSA for prudential matters, but under the Estonian authorities for AML. It seems that the lessons from earlier egregious collapses resulting from unrestrained nefarious and speculative activity, the BCCI and Barings Bank cases of the 1990s, were forgotten.

- **Auditors:** An external audit must ensure that accounts reflect a fair and proper view of the company. Auditors need to check that internal controls are taking place, i.e. that the KYC rules are applied, and that the business is a going concern. Irregularities need to be reported to the authorities. The complexities described above, with different legal frameworks and responsible authorities, render the task of auditors more difficult. EU law harmonised the conditions for statutory audit (regulation EU 537/2014) but left many options to the member states, such as for the provision of non-audit services by auditors. The regulation created a thin structure for EU-wide cooperation, the Committee of European Auditing Oversight Bodies (CEAOB), which is managed by the European Commission. This confusing picture has received scant attention, but further harmonisation will be required to help prevent more cases of money laundering.

At the next stage, there is the role of the **government authorities**: the supervisory and law enforcement authorities, and the FIUs and tax authorities.

- **Prudential and conduct supervisory authorities**: AML supervision is a task for prudential authorities in most member states, as it is part of the core risk management tasks of a financial institution. Moreover, it can have financial stability implications. Some countries have a specially dedicated entity. The newly formed EBA AML Standing Committee brings together these different bodies, 57 in total, including those of the EEA countries (see Table 6 at the end).
- The **FIUs** process suspicious transaction and suspicious activity reports, as well as cash transaction reports in certain countries, and pass these on to law enforcement for action.
- **Tax authorities** can act to pursue tax evasion and counter tax avoidance.

- **Law enforcement authorities** are charged with assimilating the intelligence, assembling evidence and prosecuting cases.

Each of these lines is organised differently across the EU, let alone in the rest of the world, which makes consistent application of AML/CFT challenging. Cross-border cases demand strong cooperation among these entities, which is time-consuming, but no AML supervisor appears until recently in charge of supervising groups (although it is explicitly mentioned in the Fourth AML Directive, and now the task of EBA). Certain international networks, such as the Egmont Group and Moneyval, have come to support these needs to some degree, but this has yet to translate into any significant impact on underlying criminality.

The European Commission detected unease among prudential supervision authorities in using their far-reaching powers against money laundering, "as the prudential framework only exceptionally refers explicitly to such concerns" (EC 2019 report, p. 11). The Single Supervisory Mechanism is seen as an additional layer for coordination, but not considered an AML/CFT authority, according to recital 28 of the SSM regulation. The first head of the SSM executive board, Danielle Nouy, often reiterated that AML/CFT supervision is not the SSM's business.

An additional problem is that home-country control, the basis of prudential supervision in the EU, does not apply in relation to AML, where the host country is in charge, as was clear in the Den Danske Bank case. AML issues were not consistently factored into the review of the credit institutions' prudential framework, it appears, while they may have far-reaching consequences. This also applies at corporate headquarters, where AML/CFT issues are not prominent, according to the EU Commission's 2019 report. The differences in the supervisory architecture for prudential and AML purposes renders cooperation more difficult. The same applies with regard to law enforcement authorities. Hence, the EU is faced with an **AML governance spaghetti**, in the context of growing cross-border activity and more centralised prudential supervision.

Concerning enforcement, judicial systems and penalties differ widely in the EU, a situation that will not change soon since member states zealously guard these powers.

5.3 New technologies and AML

Over the past five to ten years there has been a drive to create uniformity in vendor systems utilised by the financial sector, with consistent standards, scenario planning and functions. In the same period, there have also been significant developments through enhanced computer power and artificial intelligence, use of blockchain and other technologies, which create opportunities to streamline analysis and reporting, and target risk resources, moving away from traditional, rules-based monitoring to identifying behaviours, network analysis and clustering of risk attributes. As such, there is opportunity for EU financial institutions and non-financial firms to enhance their surveillance mechanisms and focus on effectiveness.

In certain respects, technology has improved both the identification of financial crime and delivery of more actionable information.[4] Data collection and analytical tools have become more powerful, and technology is advancing. The application of blockchain technology to transactions, for example, could allow for better control of them. There is a need for progress across three key dimensions, however:

[4] This section is based upon a contribution of HSBC to the task force and on the response of a task force member.

- *Data:* The issue is not so much the lack of data (certain databases for use in AML are in bad shape, however) but whether the right data are collected, their quality, the processing power and analytical capability, in order to assess it and use it more effectively. There is a need for more in-depth and relevant data that can be updated dynamically.
- *Analytics:* With better data, AI and machine learning could be used to develop better models of analysis that allow the carrying out of more complete risk assessments. This will have to be an iterative process, rolling out the best analytical models that provide a view spanning a number of different risks and combining and aggregating data across all sectors and regions. There are many data analysis techniques, though, and the end result will only be as good as the algorithm concerned.
- *Communication:* The crux of the matter is understanding how to get the right information in a timely manner to the appropriate people to get the correct decision, including providing insight, data and intelligence to law enforcement. That would require an operating model and a framework that are more agile and complex than the ones in use today.

One of the problems with technology is that once a good system is up and running, it may hinder effectiveness or reduce the attractiveness of developing further advanced technology to manage financial crime risks. New technologies may, for example, result in a reduction in the number of SARs being filed, appearing to present a decline in potential suspicious activity and raw data that will need to be explained to the authorities. AI systems could effectively lock large numbers of innocent people out of financial markets if not implemented and executed correctly. It could also act as a brake on innovation, not just of financial products but of law enforcement and supervision techniques.

In the future, transaction monitoring could be integrated into dynamic risk assessment and could use new, more effective and faster technology as support tools for decision-making. This dynamic risk assessment may be based on four pillars, as outlined below. Analysis via each of them will result in a probability of 'suspicious' activity taking place. At the heart of the issue, however, is that suspicion is a human concept, and it is very difficult to teach a computer to be suspicious, as opposed to highlighting unusual transactions in relation to set parameters. Human intelligence must not be left out of any AML assessment system, following four pillars:

- *Subject matter expertise*: Considers what is already known about suspicious activities.
- *Outlier detection:* Considers behaviours that are different in comparison with the average profile for a specific segment of customers.
- *Anomaly detection:* Looks at sudden changes in the behaviour of customers over time.
- *Network analysis*: Shows linkages and interconnectivity between different players in the system.

A policy environment is needed that supports these technologies. That includes better regulation, particularly on AI, and knowledge sharing that encourages innovative thinking and response. It should facilitate the detection of suspicious transactions and new fraud patterns across regions, instruments and techniques. More cooperation within the private sector is therefore needed, as much as is possible, and between the public and private sectors, within the limits of national constitutions, the EU Treaty provisions and the respect of fundamental rights.

Box 1. Transaction Monitoring Netherlands

Five Dutch banks (ABN AMRO, ING, Rabobank, Triodos Bank and de Volksbank) have decided to establish Transaction Monitoring Netherlands (TMNL) in the collective fight against money laundering and the financing of terrorism. The TMNL initiative will be an addition to the banks' individual transaction monitoring activities. TMNL will focus on identifying unusual patterns in payments traffic that individual banks cannot identify. The five banks have studied whether collective transaction monitoring is technically and legally feasible under the aegis of the Dutch Banking Association, as well as the question whether TMNL can add material value in the fight against money laundering. Research showed that collective transaction monitoring will allow for better and more effective detection of criminal money flows and networks in addition to what banks can achieve individually with their own transaction data. It also showed that combining transaction data will provide new (inter-bank) information that will be useful in the fight against financial crime. In addition to the banks fulfilling their own responsibility as gatekeepers, effectively dealing with money laundering and the financing of terrorism requires a national (linkage to official agencies and others) approach. The banks are therefore working closely with government partners such as the ministries of finance, justice and security, the Fiscal Information and Intelligence Service (FIOD), the financial intelligence unit (FIU) and the police. The aim is to collectively significantly increase the return from identification to detection, prosecution and conviction of criminality.

There has been progress through joint private-sector initiatives, such as Transaction Monitoring Netherlands (see box above). In public/private partnerships (PPPs), there are the Joint Money Laundering Intelligence Task Force (JMLIT) in the United Kingdom, the Swedish Anti-Money Laundering Intelligence Initiative (SAMLIT), and other initiatives in Denmark, Finland and the Netherlands (AMLC), as well as evolving work by Europol to direct financial institutions to identify and provide information that is of use to law enforcement. The same has happened in the United States, with the recent announcement by the U.S. FIU Financial Crimes Enforcement Network (FinCEN) that it will examine AML effectiveness and outcomes, in order to refocus on higher-value AML activities. It aims to increase information sharing and public/private partnerships and to leverage new technologies and risk management techniques—and thus increase the efficiency and effectiveness of the U.S. AML regime. These initiatives can be expected to continue to develop, along with (i) automated reporting to support the FIU's own data investigation and (ii) efforts to cut down on resource-intensive manual processes that do not generate meaningful results or actionable intelligence.

A firm is able effectively to manage and identify client or external entity risk and exposure on a local, regional and global scale. Areas of emphasis should include flexibility on the application of non-risk-driven uniform processes such as collection of adverse media and politically exposed persons (PEP) data and use of transaction monitoring in businesses or client types. This flexibility may enable private-sector bodies to focus their resources on areas of priority for the public sector.

However, information shared within PPPs requires appropriate legal protection, and respecting a clear division of competences between private and public sectors. A well-defined safe harbour should be provided for institutions when disclosing information in a controlled manner and for the broader public interest of preventing financial crime. The private sector has no guarantee or legal certainty that they will be exonerated of liability in cases where national and EU law have been violated. This is where bank secrecy, GDPR and EU competition policy considerations come into play. For the last of these three,

exchange of data is allowed if it contributes to the public good and if it is confined to the stated purpose, but a framework is needed to guard against collusion, which can bolster the larger players in the field. It can also raise conflict of interest and governance issues.

Ethical considerations should also be taken into account. To retain the trust of the customer, there is a need to be transparent, address bias and explain publicly what is to be done. Care needs to be taken so as not to stifle innovation, to avoid instilling anti-competitive behaviours, to eschew creating market access barriers or encouraging financial exclusion. In this context, the work of the European Commission High-Level Expert Group on Artificial Intelligence needs to be advanced. Authorities also must recognise that criminal organisations are developing their own AI, to improve their own money laundering techniques, and that needs to be monitored and countered.

6. Pillar 2 Risk Management

6.1 Measure what matters

Not everything that counts can be counted and not everything that can be counted counts. This area of European policy development stands out for the lack of underlying data which ordinarily would be collected, collated and analysed in order to identify policy options and then select the best ones. A lot of the reason for this is the nature of the area itself and the activities carried out. Criminals do not report on their activities, and it is hard for governments and policy makers to establish what a true picture is. That being said, there is room for development of 'dark number' theory in order to gain a better understanding of what is happening.

There are many reports on money laundering and measures taken to stop it, ranging from FIUs, regulators and consultancies, but there is little co-ordination between them. The taxonomy of financial crime thus needs some attention to improve commonality so that all those concerned in fighting financial crime know that they are talking about the same thing.

If anti money laundering is to improve, both measures of effectiveness, and measures of efficiency are needed. Our initial research leads us to the conclusion that the adoption of objectives and key results as measures of effectiveness, and adoption of KPIs as measures of efficiency would be extremely useful. The use of OKRs is a relatively new development in industry. It has been used to considerable effect in the development of leading technology companies in particular.

The original objectives of anti-money laundering were to reduce the incidence of the underlying harms, specifically those caused by trafficking in illegal drugs. It was postulated that by removing the possibility of retaining the proceeds of drug crime the criminals would do something else which benefitted the normal economy. The current objectives of the AML regime are unclear, but appear to involve one or more of the following, depending on the standpoint of those concerned:

- Implement FATF Recommendations
- Be seen to implement FATF recommendations
- Implement EU directives
- Be seen to implement EU directives
- Pass an FATF inspection
- Pass a regulatory inspection
- Reduce false positives

Objectives are vital as if you do not know where you are going, you are already there, and will never make any progress. Objectives set out what is to be achieved. They need to be significant, concrete, involve action and be inspirational. Key Results act as benchmarks. They monitor how we get to our objectives. They need to be specific, time bound, aggressive yet realistic.

So what kinds of objectives and key results (OKRs) could be considered in terms of progressing AML effectiveness around Europe? If we were to address the AML Governance Objective, then a way forward may be along the following lines:

- Objective: Remove the fault lines across Europe
    - KR1: Create a single EU AML body
    - KR2: Agree on a multilateral MoU between law enforcement and FIUs
    - KR3: Establish PPP (Public Private Partnership) in relation to information to be shared between the public and private sector (building upon the work in several Member States to establish Joint Money Laundering Intelligence Teams)

If we were to address the AML Risk Management Objective, then a way forward may be along the following lines:

- Objective: Meaningful Risk-Based Approach
    - KR1: Measurements and KPIs developed on predicate offences
    - KR2: Annual Member State evaluation system
    - KR3: FATF review to EU implementation in 24 months maximum

If we were to address the AML Capability Objective, then a way forward may be along the following lines:

- Objective: Establish effective law enforcement capability
    - KR1: Commitment to minimum inalienable budgets
    - KR2: Training of law enforcement in financial markets and financial crime
    - KR3: EU level training standards for whole of enforcement process

It appears that the financial sector by and large has adopted few KPIs. When asking Money Laundering Reporting Officers (MLROs) across the financial sector as to what KPIs they use in assessing the efficiency of their AML processes, the usual response has been the number of Suspicious Activity Reports that have been filed. Some mention their training states, so the numbers of staff who have undertaken training, how often the training has been carried out, and in certain cases which staff have passed a test. These are measures which are easy to record, but when asked further as to how these measures improve AML, or have an impact on underlying predicate criminality, there is little clarity. We would therefore suggest the adoption of KPIs to improve efficiency of processes within financial institutions. This requires more imagination. Some financial institutions take the following measurements, for example:

- General MI (Management Information)
- Risk tolerance breach retain decisions
- New applications declined
- Customer risk rating classifications
- Business wide risk assessment status

It would help to tie such KPIs into the KPIs used by the business as a whole, such as the speed of opening new accounts, or the speed of making secure payments. Yet such KPIs as are adopted need to be tied into the OKRs that have been set. There is no point setting a KPI if it merely serves to keep a bad process.

6.2 Risk-based approach

In order to reduce compliance burdens and increase effectiveness, the concept of risk-based deterrence has been introduced. Although highly attractive conceptually, the risk-based system has been stymied since it has become the regulator who decides what the risk is, rather than allowing firms to carry out their own risk function, with regulators checking that the risk process works and the firm developing its risk assessment skills. This initiative needs to become less dirigiste to succeed.

6.2.1 Derisking

Many financial institutions are attempting to de-risk in order to cut down the risk of regulatory action and fines. Some of this action appears to be quite blunt, in refusing to carry accounts which relate to business allegedly carried out in certain countries, or certain types of customer. This can result in severe difficulties for certain communities. That part of the financial sector relating to the accounts of money remittance companies held by large banks is a case in point. A further issue is that forcing certain types of customers, or certain types of transaction, out of the financial sector merely serves to drive such business underground and therefore makes such business (which may include criminal monies as well as legitimate funds) less transparent and more difficult for law enforcement to observe.

6.2.2 Balance

Balance is a key element to remember. There is no point placing so great a compliance burden on your economy that you drive out good money as well as bad, plummet in the Global Financial Centres Index and drive your economic success to other rival centres. Similarly, there is a need to achieve balance within a financial institution. As compliance burdens increase, profitability reduces and the customer is not served, nor will economic growth be as high as it could be.

6.2.3 Competition and financial inclusion

The nexus between AML and competition needs to be given close attention as certain events are not working as they should. An example of this is in the payments sector, and more specifically in relation to money remittance. Many countries have migrant workers who come to Europe to earn better salaries than in their home countries. Understandably, they wish to send home some of their earnings to help their families in the countries which they have come from. These are often in small amounts, of just €100 or so. Paying a transfer fee charged by a traditional financial institution in the region of €25 is clearly uneconomic, so remittance companies have been established which collect monies and transfer in bulk to the destination country where the amount is unbundled and remitted to the local accounts of the family. In this scenario the transferors are paying far less than €25. However, the transfers across border still have to go through the traditional banking system, and certain such banks have been closing the accounts of the remittance companies, citing dissatisfaction with the AML procedures of the remittance companies, but the real reason is believed to be competition. In many cases the AML procedures of the remittance companies have been stronger than those of the banks.

AML procedures in certain financial institutions have become so cumbersome that individuals which do not satisfy certain “blue tape” requirements end up being shut out of the financial system altogether, despite the fact that the monies they wish to pass through the system being entirely legitimate. Competition authorities and regulators need to keep an eye on this as otherwise such individuals will start to use underground banking systems, which will not be in the interests of the financial sector or

the economy as a whole. A further aspect of competition is the differentiation in implementation of AML laws between states, giving rise to regulatory arbitrage.

6.2.4 Defence system strategy

In assessing how deterrence should work, many regulators and companies have latched on to a principle of three lines of defence. This follows the old military principle of castle building, the outer wall representing the first line of defence, the inner wall the second line of defence, and the keep the final line. This concept of defence as applied to financial institutions and corporations has the customer facing business staff as the front line (the organisation's outer wall), the legal and compliance functions as the second line (the organisation's inner wall) and senior management and audit as the third and final line (the organisation's castle keep). But this concept is outmoded, ineffective and encourages the wrong mentality in crime fighting. It is a static model, it is reactive, and it encourages a defensive soon-to-be-victim siege mentality. Better is a system of integrated active defence, where all anti-money laundering assets are designed to work together, an application to the financial sector of a concept currently used by the world's militaries to great effect in defences such as Integrated Air Defence Systems and Integrated Carrier Battle Groups.

6.2.5 Whistleblowing and security of reporting and reports

There is increasing legal protection of those blowing the whistle on illegal practices, though this is not without its flaws. There continue to be cases of whistleblowers, far from being given protection, being actively harassed and prejudiced against. Those receiving such sensitive information should work to create an alternative credible source for the disclosed information, enable independent anonymous disclosure and protect sources. If protection cannot be assured, this valuable intelligence source will be lost and the AML system will suffer as a result. In this context, it should also be recognised that those making suspicious activity reports or suspicious transaction reports are also whistleblowers and should be given protection.

7. Pillar 3 Capability

7.1 Training

Training of law enforcement in how financial markets work is generally below what it could be. Virtually all law enforcement officers are given some financial investigation training, but this is not the same as instruction in the operation of financial markets such that law enforcement has a chance of recognising egregious behaviour, apprehending the perpetrators and obtaining necessary evidence. Some kind of specialist financial police are needed, properly trained and supported, in all countries. Commitment currently ranges from Financial Investigation Units consisting of just one law enforcement officer, to specialist financial police like the Guardia di Finanza with a force of around 70,000 persons.

It is not just amounts and types of training, but the way in which it is carried out which is important. Training using accelerated learning techniques has been shown to be much more effective than standard techniques. Recent Europol training has included gamification techniques, which are a further step forward and should be taken up by others involved too. The SIRIUS game, developed between Europol's SIRIUS Project and the Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research (CENTRIC) has been developed for investigators to gain practical experience in requesting data from online service providers, such as internet providers and social media platforms.

7.2 Funding

Proper funding for supervisory and investigation authorities is of utmost importance. Money laundering is estimated to cost the global economy between $800 billion and $2 trillion annually, according to the United Nations Office on Drugs and Crime report 2020. This amounts to 2%–5% of the global gross domestic product.

Also compliance has a huge cost. The True Cost of Financial Crime Compliance Global Report, released in April 2020 by LexisNexis, estimated that the annual cost of financial crime compliance worldwide is around $181 bn, in Europe being $137 billion, followed by North America ($32 billion), Asia Pacific ($6 billion), Latin America ($5 billion), and South Africa ($2 billion). These estimates were determined by polling 898 financial crime compliance decision makers, compiling an average spending amount for large, medium and small institutions in a particular market, then multiplying the average by the number of such firms in a given market. The most expensive countries for financial crime compliance are the United Kingdom ($50 billion) and Germany ($48 billion), followed by the United States ($26 billion), France ($21 billion), Italy ($16 billion), and Canada ($5 billion).

Law enforcement costs are considerable too, but such figures are very hard to come by and very hard to compare due to differences in responsibilities and structures between countries. Nonetheless, certain key figures suggest a need for a proper investigation as to FIU and law enforcement effectiveness. The US Federal Bureau of Investigation was funded to $9,952.9 million in 2020, comprising 35,534 positions, 244 lawyers and 13,213 agents (source US Department of Justice). The budgetary request for FINCEN, the US FIU, for 2020 amounted to $124.7 million and 359 full time staff (source US Treasury). For 2020, the Europol's Management Board approved an estimate of €174.8 million as budgetary funds and an additional 66 Temporary Agents (TA) next to a steady level of 235 Contract Agents (CA). Compared to this, following the proposal of the European Commission, the budgetary authority granted an EU contribution of €154.1 million and 24 TAs in 2020. In view of the forthcoming Europol Regulation recast, a boost of resources of Europol to implement the enhanced mandate and continuously increasing demand in the forthcoming Multiannual Financial Framework (MFF) 2021-2027 would be required. It is difficult to see how AML effectiveness around Europe ban be increased without increases in personnel. Such numbers are tiny in comparison to both the level of fines imposed across Europe and in terms of the amounts spent by European financial institutions on AML compliance.

7.3 Digitalisation

AML compliance has become an end in itself, far more bureaucratic than it used to be, with the real objectives having become lost in a mass of organisational data kleptomania. Digitalisation of business has given rise to a search for an automated AML nirvana, reducing human input to a bare minimum. Yet money laundering deterrence is a human issue and programming errors can increase costs dramatically, as battles to reduce false positives have shown. The crux of AML is the suspicion of transactions or activity being derived from criminal actions. It is very difficult to teach a computer to be suspicious. True, computers can be a very useful support tool, and can be very helpful in identification of unusual transactions (which may or may not turn out to be suspicious or criminal in nature or provenance), but using them as decision tools can have unfortunate side effects. For example, most, if not all computer systems designed to identify suspicious transactions produce a very high number of "false positives". The rate of false positives is often around 95-98%. These false positives have to be checked by human

investigation to see whether they are in fact ones which the financial institution should be concerned about and report. For some financial institutions, this entails 5,000 staff or more engaged purely on this task. This is a largely mindless, demotivating task for which the human brain is not designed. To give a sense of perspective, 5,000 staff is more than four times the size of the staff of Europol, and more than four times the size of the staff of the City of London Police, the police force which takes the lead on financial crime in the UK. This staffing figure represents just one financial institution. Few of those financial institution staff are trained investigators. It is difficult to see the benefit of this to the overall effort to defeat money laundering and its underlying predicate offences across Europe. This part of the system appears broken.

7.4 Digital identity

Digital identity of legal persons is an area which has seen some progress. Whereas all jurisdictions have a unique identifying number for each entity, which stays with them despite name changes, there was no unique identifier globally. The LEI initiative is in the process of trying to resolve this, and now has around 1.7 million entities using a unique global number. Across the EU, as a percentage, the LEI registration numbers range from 2% up to 8.9% of nationally registered companies in the UK.

Digital identity of individuals is a goal pursued by a number of companies, without a solution at present. Each initiative looks at storing various biometrics, but all systems at present suffer from lack of coverage, recognition, and reliability. There are also questions over individual privacy, data protection, inclusion and cybersecurity.

7.5 Artificial Intelligence (AI)

There is much discussion about the use of AI in supporting anti money laundering as data volumes and transaction complexities grow. This does show promise as a decision support tool. Yet this is also an area clouded in mystique. There is fundamental confusion about what exactly AI is. A recent survey by IBM highlighted that around 50% of projects described as AI projects in fact had no discernible AI element to them at all. Again, taxonomy is important. We take the definition here of AI as expounded by the European Commission High Level Experts Group on AI (broken down into the various elements):

"Artificial intelligence (AI) systems are software (and possibly also hardware) systems, designed by humans that, given a complex goal, act in the physical or digital dimension, by perceiving their environment through data acquisition. These systems interpret the collected structured or unstructured data, act on the knowledge, or process the information, derived from this data and design a path and the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions."

As a scientific discipline, AI includes several approaches and techniques, such as:

- Machine learning (of which deep learning and reinforcement learning are specific examples),
- Machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimisation), and
- Robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems).

There are many companies selling newly created "AI" systems intended to assist in the fight against money laundering and financial crime. The foundation for all of these systems is the algorithm which has been put together for the system. These algorithms are kept secret as they are the basis of profitability of the system. However, as there is so little transparency over the algorithms, there is a growing concern as to their trustworthiness. Fundamental legal tenets demand knowledge as to how decisions have been reached which affect individuals and corporations, as well as evidence.

The European Commission High Level Experts Group on AI has produced some Ethics Guidelines for Trustworthy Artificial Intelligence. There are three key principles. AI systems must be:

1. Lawful - respecting all applicable laws and regulations,
2. Ethical - respecting ethical principles and values,
3. Robust - both from a technical perspective while taking into account its social environment.

These are sound principles from which to start, though naturally open to differing interpretations. Accordingly, the European Commission High Level Experts Group on AI has worked towards setting out certain requirements of AI systems. There are seven requirements:

1. Human agency and oversight
2. Technical robustness and safety
3. Privacy and data governance
4. Transparency
5. Diversity, non-discrimination and fairness
6. Societal and environmental wellbeing
7. Accountability

What is meant by these requirements is set out in some detail by the European Commission High Level Experts Group on AI. It must be pointed out that the Group on AI has to date not received much input from the financial sector, or from law enforcement in relation to development of these principles, nor as to their interpretation and application in the context of anti-money laundering. This is clearly a concern which will need to be addressed. In the meantime, there is growing evidence of use of AI systems by the criminal fraternity in the following areas:

- Deep fakes: these are methods of creating images, video and audio which are very close to reality, designed to commit crimes
- Forging documents
- Automating exploitation of stolen data
- Opening bank accounts
- Overcoming supposition
- Trafficking via AI planning and navigation, by the use of drones, etc.
- Chatbot cybercrime: examples to date include chatbots encouraging Facebook users to download malware
- Phishing and whaling: AI systems learning your system in order to exploit it
- Creating malware: there is growing concern over 'undetectable malware', password scrappers, etc.
- Cracking passwords: neural networks being established in order to predict passwords and break into systems

Thus AI has become something of an arms race between the normal economy and the criminal fraternity. Passwords are set up to try and stop unauthorised access to systems. Criminal AI then attempts to guess and get through those password protections or scrap them altogether. Captcha

systems are established to try and block automated access. Criminal AI then attempts to guess the captchas. "Real traffic" systems are established to try and differentiate between normal activity and criminal activity. Criminal AI then monitors real traffic to make its attempts at penetration more likely of success.

The AI systems being developed by police forces are not without contention either. Systems used for predictive policing, facial recognition, individual risk assessment and case management, etc., are not centralised, there is little public information available about them, the responsibilities are unclear, and there is little transparency. It is unsurprising that questions have been raised as to their legality. Here, adoption of the principles and requirements of the European Commission High Level Experts Group on AI will be needed to assist in growing trust between the public and private sectors.

7.6 Tools for the alignment of models

Compliance is often seen as all cost with little or no benefit. CEOs invest a lot in ensuring that their business models and compliance functions are properly aligned, effective and efficient. However, it is like fighting the windmills, as new cases may loom around the corner, bringing a bank's management at risk. Some tools can be used to align the different models.

7.6.1 Databases and Ultimate Beneficial Ownership Registers

Progress on improving corporate databases is slow. Standard corporate databases and the information contained in them vary wildly across Europe. Some are quite comprehensive in holding information on directors, shareholders, company accounts, company charges. Others have no publicly accessible data on shareholders, and many have no information on the financial condition of companies, or information which is out of date. In some Member States information stored has decreased in value with loosening of requirements on personal address information, on shareholders and their shareholdings, on dates of birth, all of which make due diligence harder rather than easier. Accessibility and searchability is also an issue, with some databases being free to search, others paid for. Searchability differs between Member States too. It seems curious that steps are being advocated to include ultimate beneficial owners when data quality of even the basic register is often poor. Virtually all such databases are compiled from data submitted by those companies listed, with often no checks as to veracity being carried out by the registry itself. Data filing requirements also differ between incorporation formats such as companies, partnerships, limited partnerships and limited liability partnerships. In some states there can be in excess of twenty different forms of incorporation.

Implementation of this requirement to identify ultimate beneficial owners has been slow and patchy across Europe. Only six Member States implemented by the deadline date. Some Member States have failed to implement the registers at all. Others have put the registers behind a paywall (eight Member States, expected to rise to 10). Two have prevented public searching unless the searcher already knows the tax identification number of the ultimate beneficial owner. Five Member States require searchers to register themselves first before searching.

7.6.2 Outreach

More support of, and liaison with the media is needed. The media is swift to pick up on fines levied against financial institutions, but not so great at picking up incidents of effective law enforcement action. As an example of this, Operation DisrupTor is a very recent joint action carried out by a coalition

of law enforcement agencies across the world supported by Europol and the FBI against criminal actors. Although there was mention of the enforcement action taken, there was no mention of the financial aspects and how the money laundering had been structured. For AML to improve in its effectiveness, publicity is required, as well as feedback to the financial sector. Sensitive operational data clearly should not be revealed, but strategic feedback to the financial sector is most useful in terms of maintenance of the morale of those reporting, as well as their awareness and education.

7.6.3 Peer pressure

The FATF has identified 11 key goals that an effective AML/CFT framework should achieve. These key goals or 'immediate outcomes' are organised by theme. During its mutual evaluations, the FATF assesses the effectiveness of a country's efforts against each of these 11 immediate outcomes. Each country must enforce the 11 immediate outcomes, and ensure that the operational, law enforcement and legal components of an AML/CFT system work together and effectively to deliver results.

Table 4. Rating of FATF Immediate Outcomes

Country	Date	1	2	3	4	5	6	7	8	9	10	11
Austria	Nov/18	ME	SE	ME	ME	ME	LE	LE	ME	SE	ME	SE
Belgium	Sep/18	SE	SE	ME	ME	ME	SE	ME	ME	SE	ME	ME
Bulgaria												
Croatia												
Cyprus	Dec/19	SE	SE	ME	ME	ME	ME	ME	ME	SE	ME	ME
Czech Republic	Sep/20	ME	SE	ME	ME	ME	ME	ME	SE	SE	ME	ME
Denmark	Nov/19	ME	SE	LE	LE	ME	ME	ME	ME	SE	ME	SE
Estonia												
Finland	Apr/19	SE	HE	LE	ME	ME	SE	SE	ME	ME	ME	ME
France												
Germany												
Greece	Sep/19	SE	SE	ME	ME	ME	SE	ME	ME	SE	ME	SE
Hungary	Dec/19	LE	SE	ME	ME	LE	SE	LE	LE	ME	ME	ME
Ireland	Nov/19	SE	SE	SE	ME	ME	SE	ME	ME	ME	ME	SE
Italy	Mar/19	SE	SE	ME	ME	SE	SE	SE	SE	SE	ME	SE
Latvia	Dec/19	ME	SE	ME	ME	LE	ME	ME	ME	ME	ME	LE
Lithuania	Sep/20	ME	SE	ME	ME	ME	ME	ME	ME	ME	ME	ME
Luxembourg												
Malta	Jul/19	ME	SE	LE	ME	ME	ME	LE	LE	ME	ME	SE
Netherlands												
Poland												
Portugal	Dec/17	SE	SE	ME	ME	ME	ME	SE	ME	SE	SE	SE
Romania												
Slovakia	Sep/20	ME	SE	ME	ME	ME	ME	ME	LE	ME	ME	ME
Slovenia	Dec/18	ME	SE	ME	ME	ME	ME	ME	ME	ME	ME	ME
Spain	Dec/19	SE	SE	SE	SE	SE	HE	SE	SE	SE	ME	SE
Sweden	Sep/20	ME	HE	ME	ME	ME	ME	SE	SE	SE	ME	SE
UK	Dec/18	HE	SE	ME	ME	SE	ME	SE	SE	HE	HE	HE

HE: *High Level of Effectiveness. Minor improvements needed (7)*
SE: *Substantial Level of Effectiveness. Moderate improvements needed (75)*
ME: *Moderate Level of Effectiveness. Major improvements needed (113)*
LE: *Low Level of Effectiveness. Fundamental improvements needed (14)*

Source: FATF Website as updated to 23 Dec 2020, http://www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf.

Table 4 gives an overview of the rating of the FATF immediate outcomes for the EU. Nine of the EU Member States are not scored. Of the 19 that were, there would be 209 measures, and the number of these per level is included in brackets below the Table 4. Naturally, the position in certain member states may be better than indicated as only four member states have been assessed in 2020 so far, and there may have been improvement in the intervening period. However, it is noticeable that of the 209 scores, only 7 are judged to be of a high level of effectiveness. Some 61% of outcomes across the EU are thought to require major or fundamental improvements.

8. The way forward: a step-by-step approach

At the regulatory level:

1. Have a proper impact assessment of the effectiveness of the AML directives and the measures that have thus far been introduced by the member states;
2. Turn (parts of) the directive into a regulation. This is no panacea. It requires careful drafting and a well-managed decision-making process. Ensure alignment of EU rules with international standards;
3. Ensure whistle-blower protection. The EU adopted a directive in 2019, which has to be implemented by 2021;
4. Create common templates for reporting (STRs and SARs) to FIUs;
5. Mandate disclosure and feedback on reports filed;
6. Conclude a European pact effectively to combat tax fraud, avoidance and evasion and money laundering. This is one of the main proposals of a recent European Economic and Social Committee) opinion, as civil society should be more involved in building momentum against money laundering and tax avoidance;
7. Expand use, upgrade data quality, increase access and enhance transparency of public registries of corporates, UBOs and LEIs;
8. Ensure clear objectives and key results of regulation, set useful and realistic KPIs;
9. Address overall AML architecture to ensure effectiveness and efficiency of operation;
10. Accelerate policy to implementation process to keep abreast of technological and criminal advancements;

At the supervisory level:

1. Upgrade the role of EBA with over time a separate governance structure for AML;
2. Integrate FIUs toward the creation of a centralized intelligence unit. An EU intelligence unit would also be an effective way to aggregate data across the EU, connecting the dots, which individual banks are not in a position to do;
3. The EU needs a single voice in international fora. Today, its international representation lacks streamlining. Fourteen EU countries are members of the FATF, while the other thirteen are

members of Moneyval. This causes fragmentation and generates artificial boundaries in the fight against money laundering and financial crime in general;

4. More transparency (at the aggregate level) is needed for performance indicators used in AML: create a robust and uniform, EU-wide framework for relevant statistics (STRs, SARs, FIU investigations, prosecutions);
5. Improve public private partnerships, feedback loops and media liaison;
6. Improve training effectiveness for those involved in the law enforcement, judicial process, and data exchange;
7. Provide effective inalienable budgets for law enforcement and judiciary capability and concomitant necessary support such as sufficient IT and staff;
8. Shy away from micro management and enable obliged entities to develop effective AML risk management models;
9. Assess boundaries with the economy and ensure fair access to financial markets, safe, fast and appropriate data exchange, proper competition, and reduce financial exclusion;
10. Ensure both public and private sectors produce annual reports on progress.

At the public policy level:

1. Support informative campaigns and seminars to discuss more thoroughly the positive effects of strong AML practice in both the private and public sectors.

Between the public and private sector:

1. Public/private partnerships offer the potential to improve AML monitoring, but further work is required. While there are examples of good practice available, there needs to be guidance or a framework for establishing such partnerships and getting the most out of them.

It is unrealistic to expect all the recommendations in this report to be carried out at the same time, even though all would result in improving the effectiveness of AML. There should thus be prioritisation. Recommendations that act as 'kingpins' (that solve more than one issue at the same time or have a greater impact) should be implemented first. Annex I of the Europol Regulation lists the forms of crime that fall under its mandate. Many of these are similar, and some rationalisation could be helpful, as well as sorting out which need combating most immediately. The Task Force would also urge that the recommendations be carried out concurrently rather than consecutively. There is no reason why a workstream looking at technological developments cannot operate at the same time as one looking at regulatory impact analysis, development of OKRs and KPIs, or improved training and the furnishing of more resources for law enforcement.

Table 5. Supranational risk assessment of money laundering threats and vulnerabilities by product/activity

Product/Activity	Money laundering threat	Money laundering vulnerability
Cash couriers	Very significant (4)	Significant/very significant (3/4)
Cash-intensive business	Very significant (4)	Very significant (4)
High-value banknotes	Very significant (4)	Very significant (4)
Payments in cash	Very significant (4)	Very significant (4)
Privately owned ATMs	Very significant (4)	Significant (3)
Deposits on accounts	Very significant (4)	Significant (3)
Institutional investment sector — Banking	Very significant (4)	Significant/very significant (3/4)
Institutional investment sector — Brokers	Very significant (4)	Significant (3)
Corporate banking sector	Very significant (4)	Significant (3)
Private banking sector	Very significant (4)	Significant/very significant (3/4)
Crowd-funding	Very significant (4)	Significant (3)
Currency exchange	Very significant (4)	Moderately significant (2)
Transfers of funds	Significant/very significant (3/4)	Significant/very significant (3/4)
Illegal transfers of funds — Hawala	Significant/very significant (3/4)	Significant/very significant (3/4)
Payment services	Significant/very significant (3/4)	Significant (3)
Virtual currencies and other virtual assets	Significant/very significant (3/4)	Very significant (4)
Business loans	Significant (3)	Very significant (4)
Consumer credit and low-value loans	Significant (3)	Moderately significant/significant (2/3)
Mortgage credit and high-value asset-backed credits	Significant (3)	Significant (3)
Life insurance	Significant (3)	Moderately significant/significant (2/3)
Non-life insurance	Significant (3)	Significant (3)
Safe custody services	Significant (3)	Moderately significant/significant (2/3)
Creation of legal entities and legal arrangements	Significant (3)	Significant (3)
Business activity of legal entities and legal arrangements	Significant (3)	Significant/very significant (3/4)
Termination of business activity of legal entities and legal arrangements	Significant (3)	Moderately significant/significant (2/3)
High-value goods – Artefacts and antiquities	Significant (3)	Very significant (4)
High-value assets – Precious metals and precious stones	Significant (3)	Very significant (4)

High-value assets – Other than precious metals and stones	Significant (3)	Significant (3)
Couriers in precious metals and stones	Significant (3)	Significant (3)
Investment real estate	Significant (3)	Significant (3)
Services provided by accountants, auditors, tax advisors	Significant (3)	Very significant (4)
Legal services from notaries and other independent legal professionals	Moderately significant/significant (2/3)	Moderately significant (2)
Betting	Moderately significant (2)	Moderately significant (2)
Bingo	Moderately significant (2)	Moderately significant (2)
Casinos	Moderately significant (2)	Moderately significant (2)
Gaming machines (outside casinos)	Moderately significant (2)	Significant (3)
Lotteries	Moderately significant (2)	Low/moderate significance (1-2)
Poker	Moderately significant (2)	Moderately significant (2)
Online gambling	Moderately significant (2)	Moderately significant (2)
Collection and transfers of funds through a non-profit organisation	Moderately significant (2)	Moderately significant (2)
Collection and transfers of funds through a non-profit organisation receiving institutional funding	Low/moderate significance (1-2)	Moderately significant (2)
Investments in professional football and transfer agreements relating to professional football players	Low significance (1)	Low significance (1)
Free ports	Low significance (1)	Low significance (1)
Citizenship investment programmes and investor residence schemes	Low significance (1)	Low significance (1)
E-money sector	Unknown	No assessment for illegal activities

Source: EU Commission report (2019).

Table 6. Financial Supervisory Authorities for AML and FIUs in the member states (EU and EEA)

Country	Name of the Authority	Abbreviations*	Financial Intelligence Unit (FIU)	Department of FIUs
Austria	Finanzmarktaufsicht (FMA)	FSA	Bundeskriminalamt	Ministry of Interior
Belgium	National Bank of Belgium (NBB)	CB	Belgian Financial Intelligence Processing Unit	Ministry of Justice and Ministry of Finance
	Financial Services and Markets Authority (FSMA)	FSA		
Bulgaria	Bulgarian National Bank (Българска народна банка)	CB	State Agency for National Security FID SANS	State Agency for National Security
	Financial Supervision Commission (Комисия за финансов надзор)	FSA		
	FID SANS (FIU)	FIU		
Cyprus	Insurance Companies Control Service (ICCS)	SI	Unit for Combating Money Laundering (MOKAS)	Ministry of Justice (Attorney General)
	Cyprus Securities and Exchange Commission	FCMC		
	Central Bank of Cyprus (Κεντρική Τράπεζα της Κύπρου)	CB		
Czech Republic	Czech National Bank (Česká Národní Banka)	CB	Financial Analytical Unit (FAU-CR)	Ministry of Finance
	Financial Analytical Office of the Czech Republic	FSA		
Germany	Federal Financial Supervisory Authority, BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht)	FSA	Zentralstelle für Finanztransaktionsuntersuchungen	Customs authority
Denmark	Danish Financial Supervisory Authority (Finanstilsynet)	FSA	State Prosecutor for Serious Economic Crime / Money Laundering Secretariat	Ministry of Justice
Estonia	Financial Supervision Authority (Finantsinspektsioon)	FSA	Money Laundering Information Bureau	Customs administration
Spain	SEPBLAC, in cooperation with Banco de España, CNMV and DGSFP		Executive Service of the Commission for the Prevention of Money Laundering and Monetary Infractions	Bank of Spain
Finland	FIN-FSA (Financial Supervisory Authority)	FSA	National Bureau of Investigation Financial Intelligence Unit (RAP)	Independent entity cooperation with Bank of Finland
	The Regional State Administrative Agency for Southern Finland			

France	Financial Markets' Authority (Autorité des marchés financiers)	FCMC	Unit for Processing Intelligence and Action against Illicit Financial Networks (TRACFIN)	Ministry of the Economy, Finance and Economic Recovery
	Prudential Supervisory and Resolution Authority (Autorité de Contrôle Prudentiel et de Résolution)	CB		
Greece	Hellenic Capital Market Commission (Επιτροπή Κεφαλαιαγοράς)	FCMC	Hellenic Anti–Money Laundering and Anti-Terrorism Financing Commission (HAMLC)	Several ministries: see link
	Bank of Greece (Τράπεζα της Ελλάδος)	CB		
Croatia	Croatian Financial Services Supervisory Agency (Hrvatska Agencija za Nadzor Financijskih Usluga)	FSA	Anti–Money Laundering Office	Ministry of Finance
	Croatian National Bank (Hrvatska Narodna Banka)	CB		
	Ministry of Finance, Financial Inspectorate	MoF		
Hungary	Central Bank of Hungary (Magyar Nemzeti Bank)	CB	Central Criminal Investigations Bureau of the Customs and Finance Guard	National Tax and Customs Administration
Iceland	Financial Supervisory Authority (Fjármálaeftirlitid)	FSA	The District Prosecutor	Ministry of Justice
Ireland	Central Bank of Ireland	CB	Bureau of Fraud Investigation (MLIU)	Ministry of Justice
Italy	Bank of Italy (Banca d'Italia)	CB	Financial Intelligence Unit (UIF)	Bank of Italy
	"IVASS" - Institute for Insurance Supervision	SI		
	OAM (Organismo degli Agenti e dei Mediatori)			
Latvia	Consumer Rights Protection Centre of Latvia		Control Service - Office for Prevention of Laundering of Proceeds Derived from Criminal Activity	Ministry of Finance
	Bank of Latvia (Latvijas Banka)	CB		
	Financial and Capital Market Commission (Finanšu un Kapitāla Tirgus Komisija)	FCMC		
Lithuania	Financial Market Authority (Finanzmarktaufsicht)	FSA	Financial Crime Investigation Service Under the Ministry of the Interior of the Republic of Lithuania (FCIS)	Ministry of Interior
	Bank of Lithuania (Lietuvos Bankas)	CB		
Luxembourg	Commission for the Supervision of Financial Sector (Commission de Surveillance du Secteur Financier)	FCMC	Financial intelligence Unit (FIU – LUX)	Ministry of Justice
	Commissariat aux Assurances (CAA)	SI		

Malta	Malta Financial Services Authority	FSA	Financial Intelligence Analysis Unit (FIAU)	Ministry of Finance
Netherlands	The Dutch Authority for the Financial Markets (AFM)	FCMC	Financial Intelligence Unit — Nederland	Independent government body
	Dutch Central Bank (De Nederlandsche Bank)	CB		
Norway	Financial Supervisory Authority (Finanstilsynet)	FSA		Økokrim
Poland	FIU Poland (Generalny Inspektor Informacji Finansowej)	FIU	FIU Poland (Generalny Inspektor Informacji Finansowej)	Ministry of Finance
	FSA Poland (Komisja Nadzoru Finansowego)	FSA		
Portugal	Bank of Portugal (Banco de Portugal)	CB	Financial Information Unit (UIF)	Ministry of Finance
	ASF (Autoridade de Supervisão de Seguros e Fundos de Pensões)	FSA		
	CMVM - Comissão do Mercado de Valores Mobiliários	FCMC		
Romania	Financial Supervisory Authority (Autoritatea de Supraveghere Financiara)	FSA	National Office for the Prevention and Control of Money Laundering (ONPCSB)	Ministry of Justice
	National Bank of Romania (Banca Naţională a României)	CB		
	National Office for Prevention and Control of Money Laundering (NOPCML)			
Slovakia	National Bank of Slovakia (Národná Banka Slovenska)	CB	Financial Intelligence Unit of the Bureau of Organised Crime (SJFP UBPOK)	Ministry of Interior
	FIU (Finančná spravodajská jednotka)	FIU		
Slovenia	Securities Market Agency	FCMC	Office for Money Laundering Prevention (OMLP)	Ministry of Finance
	Bank of Slovenia (Banka Slovenije)	CB		
	Insurance Supervision Agency (AZN)	SI		
	Office for Money Laundering Prevention	FIU		
Sweden	Finansinspektionen (Sweden)	FSA	National Criminal Intelligence Service, Financial Unit (NFIS)	National Police Force
UK	Prudential Regulatory Authority (PRA)	CB	National Crime Agency (NCA)	Home Office
	Financial Conduct Authority (FCA)	FSA		

*FSA = Financial Supervisory Authority; CB = Central Bank; FIU = Financial Intelligence Unit; MoF - Ministry of Finance;
FCMC = Financial Capital Market Commission; SI = Superintendent of Insurance
Source: updated from EBA and FIU.net

Table 7. EU FIUs websites, annual reports and number of SARs

Country	FIU	Website	Annual report	SARs latest
Austria	Austrian FIU (A-FIU)	None	None	No data
Belgium	Belgian Financial Intelligence Processing Unit Cel voor Financiële Informatieverwerking - Cellule de Traitement de Informations Financieres	www.ctif-cfi.be	2019	25,991
Bulgaria	FID-SANS Financial Intelligence Directorate State Agency for National Security	www.dans.bg	2019	2,894
Croatia	Anti-Money Laundering Office	https://mfin.gov.hr/highlights-2848/anti-money-laundering-office/2875	2011	No data
Cyprus	Unit for Combating Money Laundering MOKAS	http://www.law.gov.cy/law/mokas/mokas.nsf/index_en	None	No data
Czech Republic	FAU-CR Financial Analytical Unit Financní analytický útvar	https://www.financnianalytickyurad.cz/zpravy-o-cinnosti.html	2019	3,954
Denmark	HVIDVASK - Hvidvasksekretariatet Stadsadvokaten for Særlig Økonomisk Kriminalitet	https://hvidvask.politi.dk/Home	NRA 2018	24,911 (2017)
Estonia	Rahapesu Andmeburoo	https://www.politsei.ee/en/financial-intelligence-unit	2019	6,164
Finland	RAP Keskusrikospoliisi-Rahanpesun selvittelykeskus	https://www.poliisi.fi/crimes/financial_intelligence_unit	None	No data
France	TRACFIN - Traitement du renseignement et action contre les circuits financiers clandestins	www.economie.gouv.fr/tracfin Only available in French	2019	99,527
Germany	Financial Intelligence Unit (FIU)	www.fiu.bund.de	2019	114,914
Greece	HAMLC - Hellenic Anti-Money Laundering and Anti-Terrorism Financing Commission	www.hellenic-fiu.gr	2018	6,450
Hungary	Central Criminal Investigations Bureau of the Hungarian Customs and Finance Guard Hungarian Financial Intelligence Unit	https://en.nav.gov.hu/anti_money_laundering/Hungarian_Financial_Intelligence_Unit	2017	8,585

Ireland	MLIU - An Garda Síochána, Garda National Economic Crime Bureau	www.garda.ie	2018	23,939
Italy	UIF - Banca d'Italia - Unità di Informazione Finanziaria	http://www.bancaditalia.it/chi-siamo/organizzazione/uif/index.html	2020	105,789
Latvia	Kontroles dienests - Noziedîgi iegûto lîdzeklu legalizâcijas novçrsanas dienests	https://www.fid.gov.lv/index.php/en/	July 2020	2,289 (first 6 months)
Lithuania	FCIS - Finansiniu Nusikaltimu Tyrimo Tarnyba Prie Lietuvos Respublikos Vidaus Reikalu Ministerijos Pinigu Plovimo Prevencijos Skyrius	www.fntt.lt/en	2020	1,501
Luxembourg	Cellule de Renseignement Financier	www.crf.lu Only available in French	2020	52,374
Malta	FIAU - Financial Intelligence Analysis Unit	www.fiumalta.org	2019	2,778
Netherlands	FIU - Netherlands	http://en.fiu-nederland.nl/	2019	39,544
Poland	Generalyny Inspektor Informacji Finansowej	https://www.gov.pl/web/finance/aml-cft	None	No data
Portugal	UIF - Unidade de Informação Financeira	None	None	No data
Romania	ONPCSB - Oficiul Nacional de Prevenire si Combatere a Spalarii Banilor	www.onpcsb.ro	2011	4,116
Slovak Republic	SJFP UBPOK - Spravodajská jednotka financnej polície Úradu boja proti organizovanej kriminalite	www.minv.sk	None	No data
Slovenia	OMLP - Urad RS za Preprecevanje Pranja Denarja Ministrstvo za Finance	None	None	No data
Spain	SEPBLAC - Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias Banco de Espana	www.sepblac.es	2019	7,354
Sweden	FIU - Sweden FIPO Finanspolisen Rikskriminalpolisen	None	None	No data
United Kingdom	NCA - National Crime Agency	www.nationalcrimeagency.gov.uk	2020	573,085

Task Force participants*

Chair

Eero Heinäluoma, Member of the European Parliament; former Minister of Finance, Finland

Rapporteurs

Karel Lannoo, CEPS & ECRI

Richard Parlour, Principal of Financial Markets Law International

Members

BAE Systems Applied Intelligence	Philippe Hieronimus Gary Kalish
BNP Paribas	Cédric Perruchot
BNY Mellon	Severine Anciberro
Den Danske Bank	Satnam Lehal
Deloitte	Chris Bostock Rob Wainwright
Deutsches Aktieninstitut	Maximilian Lück
Afore Consulting - EPIF	Constantine Arvanitis Paloma García Nickolas Reinhardt Inmaculada Perez Ruiz
Exiger	Jason Holt
EY	Debbie Ward Elizabeth Krahulecz
Finance Finland	Mika Linna

* The contents of this Task Force convey the general tone and direction of the discussions, but its recommendations do not necessarily reflect a common position reached by all members of the Task Force. Nor do they represent the views of the institutions to which the members, the Chairman or the rapporteurs belong.

Fleishman Hillard	Guillaume Lenglet Bertie Huet
HSBC	William Morgan Mark Turkington
ING	Koen Holtring
Isle of Man	Paul Heckles Karen Ramsay Mike Vercnocke
JP Morgan	Richard Wild
Mastercard	Isabel Simon
Natixis	Paul Rothwell Antony Whitehouse
Nordic Financial Union	Morten Clausen Vasilka Lalevska
Rabobank	Nieke Martens
REFINITIV	Vivienne Artz Che Sidanius
Schufa	Axel Bysikiewicz Urte von Raczeck
Teneo	Tomasz Krawczyk

Observers

ECB	Roberta Cossu Joachim Eule Wojciech Golecki Steven de Vries
EESC	Javier Doz Orrit Stefano Palmieri Mihai Ivascu (EESC member until 18.9.2020)
Eurasian Economic Union	Arman Khachaturyan
European Commission - DG FISMA	Raluca Pruna Chiara Bacci Gabriel Hugonnot

Europol	
Latvian FIU	Ilze Znotina
Office of MEP Javier Nart	Norma Caballero
S&D Group	Miguel Carapeto
RUSI	Isabella Chase

Invited speakers

Danish Financial Supervisor	Jasper Berg
EBA	Carolin Gardner
European Data Protection Supervisor	Anna Buchta
European Commission-DG FISMA	Tobias Mackie
Europol	Igor Angelini
HSBC	Tracy Paradise
LEI	Clare Rowley
Nordea	Richard Daniels

Further reading

Recent official documents

Government offices of Sweden gives an excellent succinct overview of the complexity of the structure of Combating money laundering and terrorist financing (2019), with links to all official international documents, and the different country's risk assessments

EU Council of Ministers (2020), Conclusions on anti-money laundering and countering the financing of terrorism, 5 November.

European Commission (2020), Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing, 7 May.

European Commission (2019) Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework, 27 July.

European Commission (2019), On the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, 27 July.

European Commission (2019), European Commission staff working document accompanying the document (annex), Report from the European Commission on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, 27 July.

European Commission (2019), On the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts.

European Commission (2019), On the assessment of recent alleged money laundering cases involving EU credit institutions, 27 July.

European Commission (2019), Assessing the framework for cooperation between Financial Intelligence Units, 27 July.

Recent reports and research

Borlini, Leonardo and Francesco Montanaro (2017), "The Evolution of the EU Law against Criminal Finance: The "Hardening" of FATF Standards within the EU", SSRN Scholarly Paper ID 3010099, Social Science Research Network (https://papers.ssrn.com/abstract=3010099).

Kirschenbaum, Joshua, Nicolas Véron and Giuseppe Porcaro (2018), "A Better European Union Architecture to Fight Money Laundering", Bruegel Policy Contribution (https://www.bruegel.org/wp-content/uploads/2018/10/PC-19_2018-241018_.pdf).

LexisNexis (2017), "The True Cost of AML Compliance — European Survey" (https://bit.ly/38fGkQQ).

Mitsilegas, Valsamis and Niovi Vavoula (2016), "The evolving EU anti-money laundering regime, Challenges for Fundamental Rights and the Rule of Law" (https://qmro.qmul.ac.uk/xmlui/bitstream/handle/123456789/13702/Mitsilegas%20The%20Evolving%20EU%20Anti-Money%202016%20Published.pdf?sequence=1&isAllowed=y).

Pol, Ronald F. (2020), "Anti-Money Laundering: The World's Least Effective Policy Experiment? Together, We Can Fix It", *Policy Design and Practice,* 3(1): 73-94. https://www.tandfonline.com/doi/full/10.1080/25741292.2020.1725366.

Unger, Brigitte (2020), "Improving Anti-Money Laundering Policy, European Parliament", May (https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2020)648789).