

REDESIGNING EU AML POLICY



DOMINIQUE LABOUREIX

Secretary General,
Autorité de Contrôle Prudentiel
et de Résolution (ACPR)

AML-CFT challenges in an era of pandemic and accelerated digitalisation

The last two years have been marked by an upheaval and by the continuation of a deep trend: the upheaval is of course the COVID-19 pandemic, with all its impacts on our daily life, from the way we work to the way we shop; the deep trend is the digitalisation of finance. No need to say that both have a strong impact on multiple aspects of the economy: international interconnectedness, customers and firms behavior, materiality of risks... AML-CFT is no exception.

The pandemic renews the opportunities for all kind of scammers (fake medical material, frauds facilitated by the lockdown, etc.) but also offers specific money laundering opportunities to criminal networks. The freezing of the economic activities created urgent needs of funds once the activity has started again: real estate operations, need for

own funds, firms restructurings, etc. All these operations become more urgent than ever... and with urgency come lesser awareness and diligences regarding the origin of funds. Since the very beginning of the pandemic, FATF, FIUs and Supervisors have alerted the public and the obliged entities on these increased AML-CFT risks. As an example for France, ACPR published on its website (<https://acpr.banque-france.fr/communications-de-lacpr-dans-le-contexte-de-la-pandemie-covid-19>) a series of communications for banks, insurance companies and also for the public. In addition, ACPR intensified its bilateral dialogue with all major obliged entities during this period.

Digitalisation of finance is now an “old” new trend as it started with traditional actors recruiting new clients online. What is new is more the multiplication of status and regimes: traditional banks or insurances companies, electronic money institutions, payment institutions, virtual assets services providers, FinTechs, Big Techs... not all of them being regulated and subject to AML-CFT regulation. The challenge here is to avoid anonymity and to maintain traceability: new technologies could help for both if AML-CFT risks are taken into account from the very beginning in every project. The role of the authorities is therefore to give clear and quick guidance to all actors.

**As money laundering
ignores the borders more
than ever, an appropriate
EU wide solution
is needed.**

Regarding the limitation of anonymity, it is important to develop secure digital identity solutions, which could be easily used by all digital finance actors. To achieve solutions efficient for business and robust from an AML-CFT point of view, it is particularly useful to gather all competencies and stakeholders: Authorities, private sector (traditional and digital economy) and Cybersecurity Agencies. Such a wide range of participants allows to share experiences, to examine AML-CFT obligations before developing technical solutions and to remain technologically neutral.

Regarding the need for traceability, two aspects are of the utmost importance in this sector, where the business models frequently involve dozens of participants: first, the implication in the fight against money laundering and terrorism financing of every participant in the operation or transaction, irrespective of its status or location; and second, the quality and integrity of information collected regarding the operation, its originator and its beneficiary, from its initiation to its conclusion. All actors shall therefore be subject to sufficient AML-CFT obligations to be able to detect suspicious activities. Additionally, the so called “travel rule” is absolutely essential to allow every actor to efficiently conduct its diligences and to give relevant information to the FIUs or Law Enforcement Agencies.

Money laundering of criminal profits ignores the borders and especially with the pandemic and the development of digital finance. AML-CFT regulations shall be established at European or even worldwide level to limit the possibility for criminal networks to make use of their illicit profits. At European level, the future legal framework should ensure a greater harmonization of AML-CFT obligations to ensure level-playing field and to avoid divergences in their practical enforcement. This is particularly true as regards online services and remote onboarding of customers, activities where the freedom to provide services is particularly developed. This future framework shall of course meet all current FATF standards but also proactively inspire the future standards.

The July Commission AML package is an attempt to provide for a global answer to all these challenges. In particular, the launch of a new dedicated authority could be a real leap towards more efficiency if an appropriate balance is found to preserve the existing mechanisms, when proved efficient. For instance, complementarity of permanent off-site and punctual on-site supervision is essential as well as close interaction with the obliged entities for their outreach.



MARTIN MERLIN

Director, Banking, Insurance and Financial Crime,
DG for Financial Stability,
Financial Services and Capital
Markets Union, European
Commission

AML – institutional heart of the new European AML/ CFT framework

The EU-level AML/CFT Authority (AMLA) is the embodiment of the institutional reform of the Union AML/CFT framework in the areas of supervision and work of financial intelligence units.

AML/CFT supervision within the EU is currently Member State-based. Its quality and effectiveness are uneven, due to significant variations in resources and practices across Member States. As recent cases of alleged money laundering involving EU credit institutions show, the approaches to cross-border situations are not consistent.

AMLA will become the centre of the new integrated Union AML/CFT supervisory system. This system will be stronger and more effective than the sum of its current parts – individual national supervisory authorities without the coordinating centre.

The Authority will have direct and indirect supervisory powers in the financial sector and indirect oversight tasks in the non-financial sector.

AMLA will directly supervise some of the riskiest financial sector entities. In the spirit of the system-based approach, supervision will be carried out by Joint Supervisory Teams – including staff of AMLA and supervisors from relevant national authorities. AMLA staff and national JST members will work together on the ground, and propose common decisions to be taken and enforced by the independent Executive Board of AMLA. The decisions and enforcement tools will be just as comprehensive as they are at national level, with the possibility to address binding decisions and to impose significant sanctions in cases of non-compliance with Union requirements.

It is important to keep in mind that AMLA is not meant to replace national supervision for all high-risk financial sector entities, and indeed many risky ones will remain supervised at national level – simply because in most cases national supervision is adequate. However, the single supervisory system is about more than just direct supervision and joint supervisory teams. This system will be underpinned by common supervisory methodologies and convergent practices, as well as centrally enabled and coordinated knowledge and information-sharing. The legislative proposal envisages mechanisms of mutual assistance, including the exchange of staff, expertise and best practices, as well as some joint supervisory exercises.

**AML/CFT supervisors
& FIUs need a single
support centre, the heart
of the system – it will
be AMLA.**

We aim at better supervision across the Union, also at national level. Therefore, regulatory, convergence and indirect supervision tasks are all equally important to ensure the success of the new AML/CFT supervisory system.

The improvement in the exchange of information and cooperation between FIUs is an equally critical rationale for the institutional reform. All recent major money laundering cases reported in the EU had a cross-border dimension. The absence of a common structure to underpin cooperation between FIUs leads to situations where necessary

joint analyses are not performed for lack of common tools or resources. These divergences reduce the capacity to detect money laundering and terrorism financing early and effectively, resulting in a fragmented approach that is exposed to misuse for money laundering and terrorism financing.

For FIUs across the Union, AMLA will become an enabler for more effective and efficient execution of FIUs' strategic and operational tasks. It will provide stable hosting of the communications network FIU.net and will ensure organisation and conduct of joint analyses of suspicious cross-border transactions and activities. AMLA will also be the centre of mutual assistance and the guardian of convergence of practices among all EU FIUs.

Timely identification of trends and typologies at Union level and facilitation of joint analyses of suspicious activities and reports will directly contribute to the prevention of incidents of money laundering and terrorism financing in the Union.

In both capacities, AMLA will be empowered and mandated to cooperate closely with all other relevant Union bodies and entities, as well as relevant national authorities, such as prudential supervisors. AMLA will also be entrusted with a leading role in interactions with third country authorities for matters with a cross-border dimension and falling within the remit of its tasks.

Both AML/CFT supervisors and FIUs need a single support centre, the heart of the system – it will be AMLA.



FRANÇOIS- LOUIS MICHAUD

Executive Director,
European Banking
Authority (EBA)

Fighting ML/TF in the age of digitalisation: the importance of a tech-led fight

The use of technology in financial services is not new.

The industry has always been evolving to look for better, faster, and more efficient ways of conducting its business. What is new is the pace at which technology develops, and the pace at which it transforms lives.

Like in other areas, technology has the potential to reshape what effective anti-money laundering and counter-terrorist financing (AML/CFT) measures look like: it can be a game changer for institutions, who can take a commercial advantage of more effective and efficient compliance systems and processes; it can be a game-changer for supervisors, who can transform their money laundering and terrorist financing (ML/TF) risk assessment processes using a dynamic data-led approach; and it can be a game-changer for consumers, as long as due to the implementation of such measures they can benefit from better and more secure access to financial services. And

still, the use of the most innovative technologies to fight ML/TF is not as widespread as desirable.

The challenge for regulators is to ensure that the new digital tools and processes to fight ML/TF are used in a way that harnesses the benefits innovative technology offers, while keeping the risks associated with them under control.

In the area of AML/CFT, this means:

Firstly, putting in place a legal and regulatory framework that is technology neutral and supports the continuous development and implementation of new approaches to tackling ML/TF in Member States and across borders. The European Commission's move towards greater harmonisation of Customer Due Diligence (CDD) requirements constitutes an important first step in this regard and needs to be complemented by clear rules on data pooling, data sharing and data processing.

Secondly, creating a supervisory culture where technology and innovation is understood and embraced, rather than viewed with suspicion. The EBA has put in place cooperation platforms such as the FinTech Knowledge Hub, that bring together institutions, technology providers, supervisors, and many other relevant stakeholders, to raise awareness of innovative technologies, share information on relevant regulatory developments and close knowledge gaps that may hamper the scaling up of financial innovation.

**Digitalisation is a game
changer to fight ML/TF -
but some associated
risks need proper
mitigation.**

Thirdly, developing a common understanding of the risks associated with the use of new and emerging innovative technologies such as data privacy requirements and user friendliness to all categories of consumers and how to address them to ensure the responsible use of innovation for AML/CFT compliance purposes. The EBA has been leading the debate in this field since 2018 with guidance on the use of innovative solutions in the CDD context and regular updates on market developments, vulnerabilities, and threats.

The EBA's 2021 stocktake on the use of RegTech in the EU Financial Sector shows that this for AML/CFT that such

solutions are by far the most frequently used. Yet, risks exist that relate inter alia to the over-reliance on the same AML/CFT compliance solutions in and uneven awareness of the limitations of RegTech in the AML/CFT compliance space. Technology enhances, but cannot replace, human skills and expertise in the fight against financial crime.

The EBA works to facilitate the safe and sound uptake of technological innovation and remains committed to leading, coordinating and monitoring the EU financial sector's transition towards a better and more effective, technology-led fight against financial crime.



JESPER BERG

Director General,
Danish Financial Supervisory
Authority (Finanstilsynet)

Efficient use of technology and data is key in fighting financial crime

To my mind, there is no doubt that technology and data must be leveraged more efficiently if we are to succeed in the fight against financial crime.

A recent report by the Danish Financial Supervisory Authority (DFSA) highlights exactly this.^[1] Technology can support increased automation of static and manual procedures, thereby allowing resources to be allocated where the risk of money laundering is highest. It can also help increase the accuracy of risk assessments and classifications of customers as well as transaction monitoring.

The feedback on the report, internally known as project AML/TEK, has mainly been supportive of the initiatives analyzed in the report, inter alia:

Create (or enhance) national electronic IDs to verify customer identity. eIDs can ease the onboarding of most customers, as banks would no longer need copies of passports and other documents. It would also reduce hassle for the customers.

Build digital data registers to verify business identity. Registers should be

able to provide high-quality information (e.g. certified by lawyers or auditors) that banks can use when onboarding businesses.

Encourage banks to build shared KYC utilities. The banking sector would greatly benefit from a centralized database of customer information that can also be fed by to public registers – and customers with several banking partners would also benefit.

Allow banks to share risk flags. Money launderers often use multiple banks, making it difficult for any one of them to identify suspicious transactions. Being able to share data will give everyone a fuller picture of a customer's banking activity. It would also prevent those who are barred from one bank for suspicious activity from simply moving to another bank across the street.

Make it easier to screen for politically exposed people. Governments often have information on individuals, which can be used to identify relatives and close associates of politically exposed persons (PEPs). Making this information available for bank queries would improve the PEP-screening process while at the same time ensuring data minimization.

Give banks access to other relevant data. Public authorities hold all kinds of information that could be useful for banks trying to prevent laundering. Police could also share what they know about how criminals behave to help banks identify suspicious transactions.

Technology and data must be leveraged better to succeed in the fight against financial crime.

Unfortunately, there is no such thing as a free lunch. Increased data-sharing raises important questions about privacy and legal rights. For example, granting increased access to authorities' data and allowing banks to share risk flags could conflict with data protection regulations (in the EU the GDPR), anti-money laundering legislation (in the EU the AMLD) and even banking secrecy norms. Sharing data also creates a risk that an individual or a business becomes non-bankable without being able to challenge this. We need a public, transparent debate on the issues to ensure that we reach the right balance of this trade-off.

It is also necessary to ensure that the regulatory framework allows for the

use of technology, which presupposes increased harmonization and guidance.

There is a natural barrier to being a first mover in applying new and advanced technologies. For example, it can be costly to implement and adapt new technologies, while the reputational costs can be huge if unsuccessful and the regulatory response can be uncertain. It can be also difficult to predict all new risks associated with new technologies, and the efficient use of new technologies for some tasks requires that consensus is reached on e.g. data harmonization. Regulators thus need to set out clear regulatory expectations.

Denmark is a highly digitized society with a strong tradition for public-private cooperation, which is the perfect environment for a move towards increased use of technology. Hence, the DFSA believes that some of the less complex initiatives presented in project AML/TEK can be implemented within a couple of years. However, the DFSA is also of the view that the full potential of technology cannot be achieved without more collaboration, both nationally and internationally. This includes developing public-private partnerships, providing guidance on the right use of technologies, as well as increasing the room for data sharing.

Financial crime is a societal problem, and criminals use advanced methods that often put them one step ahead of those trying to stop them. To be successful in this pivotal fight – and we have to succeed – we need to make the right tools available – and for obliged entities and authorities stand together, as no chain is stronger than its weakest link. This will give us a much greater chance of succeeding than the continuous tweaking of rules and governance arrangements that seems to be e.g. the EU's answer to any problem, including this.

[1] See An analysis on developing the digital infrastructure and strengthening the "Know Your Customer"-procedures (dfs.dk).



RIMANTAS ŠADŽIUS

Member,
European Court
of Auditors (ECA)

Expectations for the EU's AML Authority – The auditors' view

As the EU's independent external auditor, the European Court of Auditors (ECA) not only assesses implementation of the EU budget, but also the performance of EU institutions and bodies in reaching their objectives. We evaluate actions of the European Commission, the European Supervisory Authorities (ESAs), ECB Banking Supervision, and the Single Resolution Board.

Our recent audit of the EU's efforts to fight money laundering in the banking sector highlighted several weaknesses. First, the sharing of information relating to money laundering was often delayed between different AML authorities and even within the same authority, especially in the context of cross-border cases. Second, shared data was frequently of mixed quality, differed in scope and was not consistent between authorities. Third, due to limited harmonisation and differing risk methodologies, national AML supervisors took different approaches, which negatively affected the consistent factoring of AML risks in the context of prudential supervision. The EU level lacks powers to follow up on actions of national AML authorities.

We recommended that EU bodies should address the above issues through updated guidelines and more efficient information sharing practices. We also had findings and recommendations relating to late transposition of EU AML directives by Member States, how the Commission identifies money laundering risk, as well as governance issues at the EBA.

The Commission's July 2021 proposal foresees the establishment of a new EU AML Authority with supervisory powers and a new Single Rulebook on AML. However to be effective, the new EU body has to be set up properly, to be adequately resourced and to enjoy appropriate powers and responsibilities. As it will be the centerpiece of an integrated EU AML supervisory system, the governance arrangements need to be effective. The scope of its powers and its rights to access information need to be clearly defined.

The Authority has to be incentivised to impose effective sanctions when AML breaches are identified.

Our comprehensive audit experience shows that the setting-up of new agencies from scratch can be challenging. Key issues include the effective and timely recruitment of numerous staff starting from limited human and financial resources. It will be essential, once the co-legislators have approved the set-up of the new EU AML Authority, that the Commission provides sufficient skilled staff to the new agency on a temporary basis to ensure rapid, large-scale recruitment and efficient procurement. Numerous internal policies, IT solutions and the Single Rulebook will need to be established. Thus, any slow growth in staff numbers risks to cause delays in launching actual full-scale AML supervision and convergence work. Given the pressing issues at hand, we clearly cannot afford any such delays if caused by organisational hurdles.

The lessons learned from the setting up of the ESAs, the Single Supervisory Mechanism and the Single Resolution Mechanism should be taken into account. In this regard, for direct AML supervision, the model used by the SSM for resourcing its Joint Supervisory Teams could act as a good example.

As we observed in our reports in recent years, the ESAs face governance issues,

which hamper their effectiveness. Therefore, the Commission's proposal rightly suggests differing governance arrangements. They need to allow for efficient decision making while ensuring independence of the EU AML Authority in executing its tasks. This can be facilitated by clear rules that the members of the board act solely in favour of the EU's interests as a whole. The Authority has to be incentivised to impose effective sanctions when AML breaches are identified.

The proposed EU AML Authority would have direct supervisory powers over the most risky financial operators. For effective supervision, an appropriate risk model needs to capture the most risky entities and mitigate the loopholes identified, especially in cross-border supervision. It needs to be equipped to perform off-site supervision but also on-site inspections.

A clear co-operation mechanism to ensure efficient data sharing, both for the AML national authorities and the financial intelligence units, will be key for the EU AML authority to perform effective oversight and managing cross-border issues. This will be the foundation for consistent, high-quality supervision. The EU AML authority will also require a strong co-operation framework with prudential bank supervisors, including the ECB, in order to ensure efficient data exchange and improve cross-sectoral supervision and co-operation.

The ECA will continue to report on the EU's efforts to ensure sound financial markets. We intend to publish a report on the Single Market for investment funds in early 2022. In addition, we have recently started an audit to assess the ECB's supervision of non-performing loans in the banking sector.



MARCUS PLEYER

Deputy Director General,
International Financial Markets,
Digitization, Anti-Money
Laundering & Counter Terrorist
Financing, Federal Ministry of
Finance, Germany

Why the uniform application of anti-money laundering law throughout the EU is so important to combat illicit financial flows

In the absence of a single rulebook, the diverging implementations of the existing Anti-Money Laundering Directive by the Member States have led to a lack of a level playing field - and sometimes even to a race to the bottom. Not only does this make life easier for money launderers, it also endangers the entire internal market and distorts fair competition. The Commission is addressing these weaknesses in the current system with its legislative package, which also includes a proposal for the extensive transfer of provisions from the Directive to a directly applicable Regulation.

However, it must be borne in mind that harmonisation alone is only one piece

of the puzzle: even the most ambitious single rulebook will prove inadequate if it is not applied uniformly.

The planned establishment of a European anti-money laundering supervisory authority - known as the AMLA - will play a significant role in this regard.

The AMLA's first task will be to define its approach to risk-based supervision, especially by developing a common and EU-wide risk matrix. It will only be possible to apply the legislation uniformly if there is a shared awareness of money laundering risks throughout the Union.

As well as establishing this common risk orientation, the AMLA will be able to set common standards for supervisors and - through AML colleges as well as thematic and peer reviews of supervisory practices - ensure that these standards are uniformly enforced. For obliged entities with intensive cross-border activities and particularly distinctive risk profiles, the AMLA will be able to supervise such entities directly and, where national supervision is not sufficient, take over supervision from national supervisors in individual cases.

A single rulebook must go hand in hand with EU-wide uniform enforcement of such a rulebook in order to effectively combat money laundering.

Although uniform enforcement and supervision of anti-money laundering provisions in both the financial and non-financial sectors is desirable at the EU level, we must also take the reality of implementing these ambitious plans into considerations. A far higher degree of harmonisation exists in the financial sector than in the non-financial sector, so that European coordination and supervision practices can be implemented here more swiftly.

The very heterogeneously structured non-financial sector - which is still subject to less harmonised rules and encompasses a vast number of obliged entities - can therefore only be tackled in a second step.

This will also reduce the burden on the AMLA, which like any EU agency will

probably have to deal with teething problems to begin with. Once AMLA is set up and running for the financial sector, we can turn our attention to the non-financial sector.



AGATA STROZYNSKA

RVP, Head of Compliance
Europe - Western Union
Payment Services Ireland
Limited

Anti-moneylaundering: combining pragmatism with results

Compliance with anti-money laundering and anti-terrorism financing requirements (AML) is one of the single largest cost factors for Western Union. Over twenty percent of all our staff is working directly or indirectly on this important compliance issue. We have invested heavily in technology-based solutions to track AML risks.

While some might believe that the remittance business of transferring cash or electronic money at short notice from one part of the globe to another is inherently high-risk from an AML perspective, the sophistication demonstrated by Western Union actually speaks to the exact opposite.

Western Union is a strong supporter of the legislative package presented by the European Commission in July to strengthen the EU's AML regime. At the centre of the proposals is more harmonization of the rules, reporting standards but also day-to-day supervision. Common rules allow

companies to streamline their processes and invest in single IT solutions while at the same time improving AML compliance.

Let me give you a few examples how small changes in the rules will have a big impact. At present, each Member State has its own template for the reporting of suspicious transactions. A single template will increase cross-border comparability and allow companies to introduce a single EU-wide reporting framework. Similarly, proposals to align customer due diligence requirements across the EU will bring more safety to the financial system and allow companies to streamline their on-boarding process. We welcome also combining this with an EU-wide e-ID system. If a customer could carry their information with them this would mean no additional customer due diligence is required when entering a new commercial relationship, allowing customers to switch between providers and increase competition in the European market.

Western Union also welcomes plans to create an EU AML authority and to reinforce the cooperation between Financial Intelligence Units. Today the uncertainty of what information can be shared with whom in a cross-border context means not all the valuable information provided by the industry is being acted upon.

**It should be possible
for a company to
voluntarily opt into EU-
wide supervision if it
wishes to streamline its
AML compliance within
the EU.**

Improved EU-wide AML supervision should give all parties along a payment chain comfort about their counterparties. The remittance industry has suffered from decisions by banks to terminate their commercial relationships with this sector. AML related de-risking by the banking sector has similarly affected correspondence banking relationships and the entry to market for many FinTech start-ups. While many of these concerns are generally unfounded, a harmonised approach to AML rules and supervision would nonetheless give banks more certainty.

Additionally, giving the AML authority the power of direct supervision could be a real improvement if it genuinely

replaces the existing obligations in the 27 Member States. At the same time, we remain concerned about the designation process. The Commission's proposal bases the decision of direct supervision on two criteria: the perceived level of risk of the business model and the cross-border nature of the business. We believe the designation process needs to be objective. It should balance the risk of the business model with the level and sophistication of the compliance mechanisms already in place. Moreover, it needs to reflect that by their very nature payment services are cross-border services. Any decision on direct supervision should therefore be carefully considered.

At present, the proposal does not consider one other important possibility. It should be possible for a company to voluntarily opt into EU-wide supervision if it wishes to streamline its AML compliance within the EU.