LIFTING THE SPELL OF DIRTY MONEY

EBF blueprint for an effective EU framework to fight money laundering

European Banking Federation

LIFTING THE SPELL OF DIRTY MONEY

EBF blueprint for an effective EU framework to fight money laundering

March 2020

Follow us
#AMLactions
www.ebf.eu

EBF BLUEPRINT FOR AN EFFECTIVE EU FRAMEWORK TO FIGHT MONEY LAUNDERING

FOREWORD

Global integration of the financial system, together with the rise of new technologies, contribute to further sophistication and development of financial crime. To fight against it, a considerable amount of resources is invested by both the public and private sectors. European banks invest huge amounts in security and wider compliance systems, while also filing millions of reports to authorities. Regrettably, this fight has proven unbalanced, with criminals adapting faster than regulation.

The original aim of AML/CFT compliance requirements is to detect and prevent financial crime. Over time, the prescriptive elements of the Anti-money Laundering and Countering the Financing of Terrorism (AML/CFT) regime have created a division between the management of financial crime risk and the management of financial crime compliance risk, with the latter overwhelming the former.

Money laundering is much more than a compliance problem. It is often connected to organised crime gangs and other threats that are extremely harmful for the European society as a whole: human trafficking, illegal drugs' crime and associated street violence, counterfeiting and smuggling, financial fraud, corruption and environmental crime. The ineffectiveness of the current framework means the EU should consider, after 30 years of regulated AML/CFT, a critical review of its AML/CFT regime. This paper is calling for a realignment of the framework to return to founding principles of AML/CFT regulation and maximise its effectiveness: mitigating the risks of facilitating money laundering through the financial system.

Fighting money laundering is different from fighting other crimes, as regulated private sector entities are expected to play a crucial role in detecting it. Among those entities that by law are obliged to report suspicious or unusual transactions, such as notaries or lawyers, banks are the gatekeepers of the financial system i.e. they are the access point to financial and payment services. As such, banks are by far the largest contributors of suspicious activity / transaction reports (SARs / STRs) to public authorities, despite the fact that today many other actors could play a more active role in detecting organized crime and terrorist activities.

In the light of recent money laundering cases, the EBF recognises that some European banks may have not been fully successful in complying consistently with their obligations and in playing a full role as effective gatekeepers of the European financial ecosystem. The banking sector as a whole acknowledges that more effective effort needs to be made, not only because of certain deficiencies observed regarding the required compliance with certain AML/CFT rules, but also because even when complying with the applicable rules, the actual results which come from preventing money laundering can prove disappointing unless supplemented with better targeted efforts to identify and tackle the underlying threats. It is time to address those shortcomings of the framework which have been so far disregarded.

One of the main reasons why the framework has proven to be ineffective in many cases is that it is easier to address financial crime regulations through a tick-the-box rule-based exercise instead of an effective and well informed exercise in risk mitigation and suspicious activity reporting. This needs to change. The existing rules are disproportionate, inflexible and provide neither obliged entities nor supervisors with the appropriate tools, which should be financial crime risk-based

instead of rule-based and should support a more holistic threat picture and intelligence-led prioritisation of efforts.

The banking sector sees itself as being in the forefront of the fight against financial crime. It understands that to be effective this fight cannot remain solely in the hands of the public authorities or solely in the hands of the industry. It has mobilised itself to support legislative and policy reforms in a number of jurisdictions as well as at European level. Banks are part of the solution and must be considered as such.

The EBF, as the voice of European banks, aims to be at the forefront of the fight against financial crime, calling for a change in the current AML/CFT framework and proposing concrete amendments for improvement. This AML/CFT Blueprint is aimed at identifying the main challenges faced by banks and suggesting solutions for enhancing the European AML/CFT rulebook.

"The banking sector sees itself as being in the forefront of the fight against financial crime. It understands that to be effective this fight cannot remain solely in the hands of the public authorities or solely in the hands of the industry."

Wim Mijs
CEO of European Banking Federation

MONEY LAUNDERING WHAT IS AT STAKE?

- Transforming the proceeds of crime into ostensibly legitimate assets;
- Much more than white collars' crime;
- Connection to organised crime gangs and extremely harmful threats.

Human trafficking

Illegal drugs crime

Corruption

Terrorism

Environmental crime

Counterfeiting and smuggling

Financial fraud

FACTS & FIGURES*

Millions
of STRs and SARs from banks to FIUs annually

Barely 1%
of the cases are prosecuted

Barely 1%
of criminal proceeds in the EU are confiscated by the authorities

The European financial sector spends about

€100 billion
on compliance annually

10% of banks' staff
are dedicated to compliance tasks

EXECUTIVE SUMMARY

The EBF has made its own assessment of how to deliver on the promise of a more effective way of fighting financial crime in the EU, and has identified four priority areas that need to be addressed, resulting in 20 concrete EU policy recommendations. These priorities are outlined in further detail in this Blueprint and summarised hereinafter. In concrete terms, the EBF suggestions are to:

- **HARMONISE the EU AML/CFT framework and strengthen its risk-based nature;**
- **EMPOWER EU supervision and law enforcement by strengthening the institutional architecture and the framework for public-private collaboration;**
- **Enable all interested parties to effectively COOPERATE and share information;**
- **BE SMARTER: Leverage new tools and technologies.**

Our recommendations are mainly based on lessons learned from EU and international best practice, including recent reports of the EU Commission, EU Parliament, FATF and the Wolfsberg Group. The legislative recommendations focus mainly on the EU's Anti-Money Laundering Directive (AMLD) framework, the EU's main piece of legislation on this issue. However, the EBF equally recognises the importance of EU legislation such as the Funds Transfer Regulation and the Directive on combating money laundering by criminal law.

Financial crime is a complex issue that requires a detailed analysis and assessment. This Blueprint aims to present some of the main issues for the financial services sector and to contribute to a meaningful discussion on the fight against money laundering and terrorism financing. The EBF looks forward to constructively engaging with EU policymakers and other stakeholders in the coming years.

*Sources: Europol, Global Coalition against Financial Crime, Bloomberg and European Banking Federation

EU POLICY RECOMMENDATIONS

In concrete terms, the tables below outline the EBF policy recommendations for a robust future AML/CFT regulatory framework, which, ideally, would address policy and institutional fragmentation. Several of these recommendations are also being developed by the EBF in separate position papers.

Priority 1
HARMONISE

Recommendations:

1/ Turn AML Directives to the extent possible into directly applicable Regulation
2/ Minimise discretionary powers for Member States to defined instances where their national specificities need to be taken into account
3/ Clarify the risk-based approach (RBA)
4/ Modernise and standardise the know-your-customer (KYC) policy
5/ Exploit synergies with other legal and regulatory frameworks as appropriate and promote a global level playing field
6/ Anticipate the potential impact of technology on the AML/CFT framework

Priority 2
EMPOWER

Recommendations:

7/ Enhance the role of the European Banking Authority (EBA) as rule-setter with a view to providing fully harmonised standards
8/ Reinforce the AML/CFT role of supervisors, enhance supervisory convergence focusing on risks and ensure effective EU/EAA and cross-border coordination of AML/CFT supervisors
9/ Harmonise and strengthen the Financial Intelligence Unit (FIU) functions across the EU/EEA
10/ Empower existing EU law enforcement bodies
11/ Provide EU institutions and agencies with adequate resources to fight financial crime

Priority 3
COOPERATE

Recommendations:

12/ Adopt a coherent approach for information sharing, balancing data protection and financial crime prevention
13/ Adopt an EU/EEA-wide GDPR AML/CFT Guidance
14/ Facilitate enterprise-wide reporting of suspicious transactions /activities
15/ Facilitate bank-to-bank information sharing e.g. by removing legal obstacles to the use of shared utilities, while being respectful with the GDPR principles
16/ Stimulate public-private information sharing and broaden the conditions under which operational data could be shared
17/ Support at EU level the Europol Financial Intelligence Public Private Partnership (EFIPPP)
18/ Improve cooperation between public authorities

Priority 4
BE SMARTER

Recommendations:

19/ Ensure beneficial ownership transparency based on better designed UBO registers, checked by public authorities and useable for obliged entities
20/ Encourage the use of enhanced analytics and machine learning tools for KYC purposes which are respectful of privacy rights

Priority 1
HARMONISE

Legal requirements for AML/CFT currently vary across the EU, with uneven implementation of EU Directives as well as inconsistencies in how national legislation implement these Directives. While the EU legislative framework has significantly improved in recent years, it has been constructed in silos, developed in successive layers and has followed a minimum harmonisation approach. The resulting fragmentation hinders the roll-out of common and consistent EU-wide AML/CFT risk management frameworks, while regulatory weaknesses and inconsistencies between jurisdictions are easily exploited by criminals.

National divergences in the AML/CFT rules and implementations include:

- Divergences of the implementation of know your customer (KYC) rules
- Divergences in the definition of certain predicate offences
- Divergent rules around filing suspicious activity / transaction reports (SARs / STRs)
- Divergent thresholds for activating the SARs / STRs mechanism

1/ Turn AML Directives to the extent possible into directly applicable Regulation

The EU AML/CFT framework is based on Directives (the AMLDs) which provide for minimum harmonisation of the legal framework. This has led to quite significant differences in the implementation and interpretation of the framework across the EU Member States, complicating the work of regulators, law enforcement and multinational banking Groups. Cross-border crime should be met with harmonised rules that apply consistently across EU jurisdictions and can help create a level playing field in terms of common approaches and interpretations of key terms. To the extent possible, the EBF would therefore support transforming applicable parts of the AMLDs into a directly applicable EU Regulation.

Such harmonisation would enable European banks that operate cross-border, but also other obliged entities, to develop more effective group-wide AML/CFT policies and processes, create synergies and facilitate effective cross-border supervision and public-private cooperation.

The adoption of an EU AML Regulation which would take back the core principles of the AMLDs would create a level playing field across the EU Member States. It may also reduce the scope for regulatory arbitrage, when criminals exploit weakness in one jurisdiction to launder funds and move these around financial markets. It would also be a unique opportunity to clarify the grey zones in the existing rulebook, e.g. by providing a detailed typology of crime and by harmonising and eventually centralising beneficial ownership registers and other reporting requirements. Such a Regulation should address variables such as the national penal codes, the role of local FIUs and investigations, and should be developed in close cooperation with the industry.

2/ Minimise discretionary powers for Member States to defined instances where their national specificities need to be taken into account

The AMLDs have allowed for significant Member States' discretion in choosing policy options. At a minimum, the resulting divergencies between national regimes have added unnecessary bank compliance costs and customer delays, preventing obliged entities from purely focusing on risks, without improving the overall control environment. These divergences lead criminals to move activity to or through jurisdictions with the 'weakest' rules making them the Achilles' heel of the EU AML/CFT framework. Therefore, the EU rules should be characterised by the principle of as much harmonization as possible, including both standard requirements and the criteria for enhanced or simplified due diligence in line with the risk-based approach (RBA). This approach to harmonisation could mandate the existing European Banking Authority (EBA) Guidelines on AML/CFT Risk Factors, simplifying and standardising the rulebook on how cross-EU banking groups manage risk and leave options and discretions to Member States only in very defined instances, for example, when their particularities need to be taken into account.

3/ Clarify the risk-based approach (RBA)

Supervisors still tend to supervise banks for AML/CFT rules through the prism of technical compliance, rather than focusing on the practical prevention and disruption of financial crime. This does not support an efficient allocation of specialist bank compliance resources or more innovative approaches to tackling complex threats such as human trafficking and trade-based money laundering.

Enhanced due diligence in correspondent banking relationships

An example of focussing on risks rather than just "ticking a box" would be the following. Banks should remain free to classify their correspondent banks as low, regular or high-risk correspondents in accordance with their own risk assessment and apply a RBA to the degree of mandatory enhanced due diligence required for non-EU/EAA respondents (application of proportionality principle supported by FATF).

In some cases, a rule-based approach to supervision can drive de-risking i.e. the phenomenon of banks terminating or restricting business relationships with higher risk categories of clients, which could result in financial exclusion. An over-emphasis on a rule-based approach to AML/CFT can have the unintended effect of obstructing financial inclusion. This problem needs to be addressed at EU level in a close cooperation between the public and private sectors.

The strengthening of the RBA is central to the implementation of the FATF Recommendations including both technical compliance and

RBA in High-Risk Third Countries relationship or transactions

Banks should remain free to apply customer due diligence in accordance with a RBA and taking into account the specific circumstances of a business relationship or transactions.

effectiveness of the overall regime. As set out in the existing EBA Guidelines, the RBA means that countries, competent authorities and banks identify, assess and understand the money laundering and terrorist financing risks to which they are exposed, and take the appropriate mitigation measures in accordance with the level of risk. This flexibility allows for a more efficient use of resources and enables obliged entities and competent authorities to:

- focus their resources and take applicable enhanced measures in situations where the risks are higher;
- apply simplified measures where the risks are lower;
- exempt low-risk activities from routine requirements, such as for low-value non-rechargeable gift cards; and
- ensure financial inclusion is maintained through precise, risk-based decision-making.

This necessary flexibility is not allowed for by overly prescriptive requirements, such as that relating to mandatory EDD for non-EEA correspondent banking relationships and relating to High-Risk Third Countries. Conversely, AML/CFT requirements that do not apply to all activities presenting ML/FT risks and to all entities engaged in financial transactions, such as virtual asset services providers, do not support an effective AML/CFT regime. A proportionate and robust RBA to AML/CFT assessments should be put forward in the EU, allowing all parties involved in AML/CFT prevention, including obliged entities, FIUs, law enforcement, prudential and AML/CFT supervisors to collaborate and determine the types of business relationships and transactions to be considered a priority. That said, the RBA by default leaves to the discretion of each firm to determine and apply their own risk appetite, aligned to their business model. This requires stepping away from an AML/CFT rule-based approach towards an AML/CFT RBA.

To complement this, the EBF suggests the European Commission and the EBA, in close cooperation with law enforcement, to provide further guidance on the national and supranational risk assessments to support a consistent basis for enhanced and simplified due diligence requirements, and, in particular, on the level of transaction monitoring expected.

4/ Modernise and standardise the know-your-customer (KYC) policy

Implementation of know-your-customer (KYC) rules according to the AMLD4 and AMLD5 differs significantly across the Member States. An example of this would be the differing requirements placed on obliged entities when verifying the information on beneficial owners and the intensity and time allowed to review, periodically, customer information and documents.

An AML Regulation should set out clear and uniform rules for harmonising the KYC policy across the EU and align it with international standards and the FATF's Guidance. In addition, such rules need to be followed up with clear guidance on how to implement specific provisions and include risk-based KYC requirements for specific topics. A document-based approach to KYC is rapidly becoming unsustainable in an ever-increasing digital world.

The EBF supports the use of KYC tools such as the Wolfsberg Group Correspondent Banking

Electronic identification (e-ID) challenges

E-ID measures should not understate the risks arising from vulnerabilities in the unregulated sector (e.g. providers of digital ID systems) and inconsistencies in national and regional guidelines. Both issues make it more challenging for banks to assess the adequacy of digital ID systems.

Due Diligence Questionnaire which has the potential to become the standard instrument for KYC self-certification for more efficiency and consistency in the KYC process, in order to avoid the issuance of individual KYC documents by banks. The KYC policy should be modernised, by clarifying and facilitating e-identification and the use of shared utilities. The EU AMLR should be more specific in terms of information to be collected and used (i.e. by illustrating different ways in which the KYC requirements based on the type of entity the obliged entities deal with; a long-established example is the Guidelines issued by the Joint Money Laundering Steering Group / JMLSGin the UK). Basic customer data which are defined under clear and comprehensive rules should be collected in line with the RBA, including simplified due diligence flexibility on timing and means where appropriate or supplemented by additional risk-based measures.

5/ Exploit synergies with other legal and regulatory frameworks as appropriate and promote a global level playing field

Overall, synergies could be exploited with other EU legal frameworks and a global level playing field should be promoted, including through better alignment with FATF requirements and other applicable international standards (such as OECD). A global approach would also help mitigate cross-border risks and address the challenge of de-risking which in some cases may result from too prescriptive measures. With better alignment between AML/CFT and due diligence requirements under the OECD's Common Reporting Standard (CRS) and the Directive on Administrative Cooperation (DAC2), synergies could be exploited. Essentially, the AML/CFT concept of beneficial owners and the fiscal concept of controlling persons of a passive non-financial entity should be harmonised. The OECD will undertake a review of the CRS in 2020 and should be encouraged in this context to align it on AML/CFT standards.

6/ Anticipate the potential impact of technology on the AML/CFT framework

A clear and consistent AML/CFT rulebook could also support a technology neutral approach for delimiting the scope and application of the AML/CFT rules. The current approach, based on descriptively defining obliged entities, can lag behind developments in new technologies and delay clarification of the scope and application of AML/CFT requirements. On the other hand, technological neutrality could at one stroke remove the arguments about who is or not caught by the AML/CFT requirements. It would also future proof the framework against new and evolving technologies/ payment systems, for example, the tech firms.

A principle-based approach, where all entities authorised to engage in financial transactions and other relevant activities are covered unless they are specifically exempted, could be a way forward in order to ensure that the scope of obliged entities is technology neutral, hence avoiding regulatory gaps, particularly in light of the emergence of virtual assets. The second EU Payment Services Directive (PSD2), which regulates an area equally subject to rapid technological change, namely payments, also uses this approach in its coverage of all legal persons authorised to provide payment services.

Virtual assets

While the AMLD5 captures wallet providers and providers of exchange services, FATF Guidance of June 2019 goes further and recommends jurisdictions to include other crypto-related services, such as crypto-to-crypto exchanges and crypto issuers. The EBF would support this FATF Guidance to be converted into EU law. However, with the current approach to the scope of the AMLD, it will take a few years, at least, for this to materialise in practice. This mechanism can allow serious risks of regulatory gap in times of rapid technological change.

Priority 2
EMPOWER

Despite many efforts, the EU's institutional framework on AML/CFT remains fragmented. Hence, weaknesses in the EU AML/CFT setup represent a risk to the integrity and resilience of the European banking sector and to the overall regulatory and supervisory effectiveness of the European Union. Institutional and functional fragmentation renders the fight against financial crime more difficult. Since financial activities as well as criminal activities are cross-border, it is ineffective to set regulatory borders. Coordination at European level, and with key third country regulators and supervisors, can also help national competent authorities to deploy resources more effectively, in particular, where the risks are more significant.

The EU has already taken steps to strengthen the institutional architecture

8 May 2018: EC (First Vice-President Frans Timmermans, Vice-President Valdis Dombrovskis and Commissioner Vera Jourova) sent a letter to the European Central Bank (ECB) and the European Supervisory Authorities (ESAs) to initiate a collective reflection on how to improve the framework for cooperation between AML/CFT and prudential supervision. A joint working group was set up bringing together the EC, the ECB and the ESAs.

12 September 2018: EC Communication on on-going work to put forward proposals that would give the European Banking Authority greater enforcement powers and more resources to investigate the activities of banks involved in illicit financing.

September 2018: EC Communication on strengthening the AML/CFT and prudential frameworks and new rules to strengthen the role of the European Banking Authority. This led to the reinforcement of the AML/CFT dimension in prudential banking legislation through the adoption of the fifth Capital Requirements Directive in December 2018.

8 November 2018: ESAs' Draft joint guidelines on the cooperation and information exchange between prudential and AML/CFT competent authorities for the purposes of AML/CFT supervision.

21 March 2019: Council and Parliament reached provisional deal on supervisory framework for European banks.

7/ Enhance the role of the European Banking Authority (EBA) as rule-setter, providing fully harmonised standards

According to the new article 9a of Regulation (EU) 1093/2010 ("Special tasks related to preventing and countering money laundering and terrorist financing"), the EBA will notably dispose of new AML/CFT powers, which shall remedy the shortcomings spotted by the European Commission in terms of information sharing among authorities, as well as providing guidance and assistance to tackle the AML/CFT weaknesses within the EU.

Consequently, the EBA will benefit from enhanced prerogatives to develop common guidance and standards, effectively, to prevent and counter ML/TF and promote their consistent implementation within the EU, through the information collected from national authorities, by issuing technical regulatory standards. This is a positive first step to improving the structural issues relating to AML/CFT supervision. The EBF supports a better use of the ESAs' powers and enhanced role for the EBA as a rule setter, which is its DNA.

However, the financial stability implications of money laundering are so large that it should not be the only measure.

8/ Reinforce the AML/CFT role of supervisors, enhance supervisory convergence focusing on risks and ensure efficient EU/EEA and cross-border coordination of AML/CFT supervisors

The EBF supports the idea of ensuring high quality and consistent risk-based AML/CFT supervision, seamless information exchange and optimal cooperation between all financial supervisory authorities, as highlighted by the European Commission in its reports on shortcomings in the fight against money laundering/ terrorist financing, released on 24 July 2019, and also recalled in the Council conclusions of 5 December 2019. There is a crucial need to improve AML/CFT supervision focusing as a first step on the following aspects:

- **AML/CFT considerations must be better integrated into prudential supervision.** In the wave of the money laundering cases uncovered, it has become apparent that AML/CFT issues can quickly become major prudential issues affecting individual banks' viability and the stability of the banking sector as a whole. In concrete terms, the new rules should resolve the issue of the misalignment between prudential and AML/CFT supervision. A **reinforcement of the AML/CFT role of supervisors** is required, together

with a better use of the ESAs' powers and an enhanced role for the EBA.

- The European Commission has highlighted in its post-mortem report of July 2019 that supervision differs between Member States. Supervisory fragmentation is a major challenge that must be addressed. Transforming applicable parts of the current AMLDs into an AML Regulation directly applicable to all EU Member States will be a beneficial next step towards **supervisory convergence,** and one which will strengthen the EU AML/CFT rulebook, while providing clear regulatory guidance. In this context, supervision should **focus on managing the AML/CFT risks** rather than on inflexible rules-based compliance.

- While financial crime is cross-border and criminals seek to exploit the weakest links, the lack of centralisation, coordination and oversight of AML/CFT supervisory powers has so far obstructed cross-border cases. The AML/CFT supervisory Colleges put in place by the EBA are welcome but should be complemented by further measures to support **efficient EU/EEA coordination of national AML/CFT supervisors.** These further measures should leverage the experience and expertise of national supervisors in this field, while supporting coordination with key third country supervisors and ensuring that the EU is a credible counterpart in international cooperation, in particular towards the US. This cross-border coordination would help to achieve harmonisation and avoid fragmentation of the legal framework, leveraging the positive effects of the harmonisation of the AML/CFT rules at EU level. In this regard, cooperation with the EBA in its enhanced mandate will be fundamental.

If this coordination is materialised through a centralisation of supervisory powers, then the mandate should be clarified as from the start. Any oversight responsibilities as well as the relationships with local supervisors and banks should be clearly defined.

If this coordination is materialised through a mandate provided for direct supervisory powers over banks, duplicate supervision must be avoided and a broad scope including all Member States and all obliged entities (beyond the financial sector) must be considered. When the political discussion on such centralisation has matured, the industry should be consulted. The EBF will consider the options that will be put on the on the table and will provide further comments and recommendations.

State of play of the integration of AML/CFT considerations into prudential supervision

- The ECB identified conduct risk (AML/CFT being seen more as a conduct issue than a prudential issue) as one of the key areas of risk for the banking system (annual Supervisory Review and Evaluation Process - SREP).
- The SSM Regulation does not allocate responsibility for the supervision and enforcement for AML/ CTF, which lies with national AML/CFT supervisors.
- The ECB has a duty to cooperate with AML/CFT supervisors, but this has been limited, so far, by a number of obstacles (e.g. data protection, lack of harmonisation).
- As required under the AMLD5, the ECB concluded a multilateral memorandum of understanding on the exchange of information with AML/CFT supervisors in January 2019.
- Banks outside the scope of the SSM supervision are subject to national prudential authority supervision which is not always within the same organisation as that of the AML/CTF supervisor (often the conduct regulator), or the Financial Intelligence Unit (FIU).
- As noted by the European Commission, national prudential supervisors should clarify the practical arrangements for the incorporation of AML-related aspects into their prudential supervision.
- The EBA has undertaken a 'stock taking exercise' to identify the various AML/CFT issues relevant to a prudential perspective and deficiencies in current supervisory practices, and to adopt guidance.
- Capital Requirements Directive (CRD): the EC has proposed an amendment to the CRD so that all authorities receiving information relating to AML/CFT should be explicitly covered by confidentiality waivers.

9/ Harmonise and strengthen the Financial Intelligence Unit (FIU) functions across the EU/EEA

The main function of an FIU is that it investigates suspicious or unusual activity reports (i.e. SARs / STRs) provided by obliged entities. SARs / STRs will not improve if banks do not receive operational police data, i.e. in the fore field of a suspicion. Such data cannot be provided by all the supervisors or by FIUs in each Member State. While organised crime is very often connected throughout cross-border networks, tip offs from the local police authorities have often helped banks to rule out or confirm a suspicion. Consequently, the EBF firmly believes that both perspectives (cross-border and local) need to be taken into account when improving the FIUs' role.

First, the EBF suggests that the function of national FIUs be harmonised and clarified so that they can provide and receive operational data on a clear legal basis.
As a second step, those FIUs should be interconnected to avoid duplication. A European FIU function could incorporate the existing Europol structure of the FIU.net and replace the European Commission's Financial Intelligence Unit platform structure, serving as a central node in the system of existing FIUs. It could potentially focus on cross-border SARs / STRs and would be able to coordinate the exchange of data required between national FIUs by AMLD5. In line with the reasoning on supervision, this European FIU function would reduce the risk of criminals exploiting weaknesses across jurisdictions, while it would also mirror the cross-border nature of financial crime. With this function, the EU would also be able to express a strong EU united voice in the Egmont Group, which brings together FIUs from around the world. This would strengthen the EU's ability to position itself as a strong block in supporting and cooperating with other jurisdictions, and to put pressure on third countries' FIUs, where appropriate.

10/ Empower existing EU law enforcement bodies

Existing EU law enforcement bodies could be strengthened in their AML/CFT functions.
The EBF strongly supports the role of Europol and Eurojust in providing the necessary cooperation between law enforcement and prosecutors across jurisdictions. In particular, the EBF supports the recent calls, including from the European Parliament, to reform Europol, transforming it into a stronger European agency with executive powers. If such an idea were to be pursued, the fight against financial crime should certainly be one of the top priorities of the new approach, and part of the overall mandate to tackle cross-border organised crime and terrorism.

The setting-up of the European Public Prosecutor's Office (EPPO) by 22 EU Member States is also a potential way forward to explore in the context of AML. Although the initial focus of the EPPO will be on cross-border crime against the EU budget (i.e. fraud, corruption, or serious cross-border VAT fraud), European policymakers could mandate the European Commission to explore the potential for the EPPO to prosecute financial crime with an European dimension extended to all Member States of the EU and the European Economic Area (EEA).

11/ Provide EU institutions with adequate resources to fight financial crime

On top of stronger mandates, all relevant public authorities should be provided with adequate resources to allow them to perform their law enforcement activities, effectively, and on a continuous basis.

Priority 3
COOPERATE

Effectively combating money laundering and terrorist financing requires a coordinated approach from legislators, supervisors, law enforcement agencies, judicial authorities, FIUs, banks and other public and private participants in the AML/CFT ecosystem. Nevertheless, cooperation between these actors has often been ineffective. Communication channels are cumbersome and lack agility, especially across borders, which may partially be caused by legal restrictions or insufficient knowledge about legal remedies that could allow information sharing. Impediments to information sharing impact the ability of both the private and the public sector to detect malicious activity, effectively, creating potential systemic risks and eventually threatening financial stability.

12/ Adopt a coherent approach for information sharing, balancing data protection and financial crime prevention

Data protection and anti-money laundering share, each in its own way, the objective of protecting European citizens. However, there can be tension between the two, hence the need to ensure proportionality and coherence.
The reassessment of EU AML/CFT rules provides an opportunity to review the proportionality of the AML/CFT requirements and identify areas where the RBA could be strengthened. This would enhance the protection of personal data in the EU. The new rules should also seek to identify and address areas where AMLD4 rules could be better aligned with the GDPR framework. For instance, it is noted that the interpretation of the AMLD4 retention periods is diverse in different Member States. Interactions between the AML/CFT data retention periods and domestic laws should be considered carefully in order to avoid any unintended consequences or inconsistencies. In addition to GDPR, national bank secrecy / confidentiality regimes should also be reviewed and amended as required by FATF standards.

13/ Adopt an EU/EEA-wide GDPR AML/CFT Guidance

In light of the above, the EBF takes the view that an EU-wide approach to the question of effective information sharing could bring forward better outcomes. The European Data Protection Board (EDPB), established by the GDPR brings together national data protection supervisors and should play a key role in setting up a data driven compliance-by-design. An inclusive and pragmatic guidance on how to interpret the GDPR in an AML/CFT context should be developed in cooperation with the EBA, to ensure the trade-off between data protection and AML/CFT enforcement is balanced. The industry should also be consulted, to make sure the core challenges faced by banks in their every-day business are effectively and proportionately addressed.

Resolving issues stemming from GDPR interpretation

The general need for clarification of the AML/CFT regime should look at how this fits in with existing data protection and privacy rules. Hence, a new AMLR should certainly consider how the AML/CFT framework interacts with privacy rules.

In particular, Article 5(1)(e) of GDPR allows firms to retain personal data for as long as necessary in order to achieve a legitimate purpose and allows firms to hold the same data for multiple purposes. As such, data need to be erased once it is no longer needed for any legitimate and lawful purpose. In contrast, Article 40 of AMLD4 requires records to be deleted after the relevant AML/CFT retention period has expired, with ongoing retention only permitted in narrowly defined circumstances. AMLD4 does not, therefore, anticipate that AML/CFT data be also relevant for other legitimate purposes, such as when there is a risk of litigation or when the firm has a third country obligation to retain the data.

In addition, there are situations in which the processing of personal data could be highly beneficial for AML/CFT purposes, either because the sector sees it necessary when taking responsibility as a gatekeeper, or because it is expected from competent authorities and regulators.

However, it is unclear how to apply the rules of the GDPR which is risk-based. In particular, where certain processing would be helpful for the detection and prevention of money laundering but is not strictly required by legal obligations, it is unclear what would be permitted under GDPR. For example, it is unclear the degree to which firms can rely on 'legitimate interests' (GDPR Article 6(1)(f)) to share AML/CFT intelligence. Consistency and harmonisation on the interpretation of the GDPR in the context of ML/TF is key. At this moment, there is a lack of clarity and harmonisation across the EU on what would be the most adequate legitimate ground to base certain data processing in the context of AML/CFT and to which extent local laws should be amended to achieve coherence throughout the EU. It should be borne in mind that to the extent certain data could be close to qualify as data relating to a criminal offence, these fall under the regime of the different member states. The conditions under which such criminal offence data may be processed or shared is also not harmonised in the GDPR. This has been left out to the Member States (see article 10 GDPR).

14 Facilitate enterprise-wide reporting of suspicious transactions/activities

Barriers to information sharing have started to be addressed for competent authorities but still inhibit public-private cooperation and sharing of AML/CFT intelligence between and within EU-wide banking Groups. Even though the AMLD and the Directive on combating money laundering by criminal law harmonised to a significant extent the EU AML/CFT framework, this remains strongly connected to the national rulebooks, particularly to the criminal law of individual Member States and the crimes defined therein, which differ considerably.

Good quality SARs / STRs are vital in the fight against money laundering and they constitute the only means for regulated entities to identify an unusual or "suspicious" transaction. The EBF believes that policymakers should explore the legal possibilities and gateways to harmonise the framework for sharing information.
Currently, European banks that do business cross-border need to break down their information sharing level as follows:

i) between Member States,
ii) between Member States and countries with equivalent requirements,
iii) between Members States and countries with non-equivalent legal frameworks. Some national laws may authorise the sharing with the head office only, especially when the head office is not located in the same country as the local entity which provides the information. In most EU Member States the law does not make any difference as to whether the sharing is to the benefit of the head office or the subsidiaries.In the current EU AML/CFT framework, differences in the transposition may lead to discrepancies between domestic regulations. For instance, between two Member States, the stricter AML/CFT (or data protection) law is the one applicable, as long as the sharing of information is possible. Such divergences pose serious issues to European banks that operate cross-border, in particular, in non-EU jurisdictions.

Intelligence sharing of clients exiting for financial crime reasons

Banks would welcome being able to share between regulated entities, at a minimum within Europe, a list of clients with whom relationships have been terminated or who have been refused banking services based on specific financial crime reasons, as identified through KYC and wide CDD controls. This list would serve for banks to warn each other about risks and improve their CDD checks. The same applies to the area of sanctions screening. The EBF recommends EU policymakers to clarify that the GDPR allows for such lists to be developed under appropriately stringent and clear conditions and provided that they are proportionate.

15/ Facilitate bank-to-bank information sharing e.g. by removing legal obstacles to the use of shared utilities, while being respectful with the GDPR principles

Combining efforts and collecting alerts from different institutions may enhance the effectiveness of reporting and may also develop intelligence patterns which can provide banks with the ability to prevent future crimes. In essence, one additional alert may offer a more complete picture of another, thereby identifying criminal behaviour.

However, the current EU data protection framework provides limited mechanisms for sharing AML/CFT information outside the organisation (bank-to-bank). Third party information sharing, e.g. via a shared utility, is also generally limited. Some jurisdictions are exploring this idea within the legal boundaries and may have to modify their existing laws. Different national initiatives of financial fraud intelligence sharing demonstrate that more can still be done to help protect customers and disrupt organised crime gangs.
The new AML/CFT rules should allow a centralisation of the transaction data collected by banks. Secure platforms hosted by trusted third parties and supported by governments under a robust legal framework may offer banks the capability to match KYC information stemming from different databases, without each bank having access to the other's datasets. An AML/CFT Regulation could set up this framework and provide clarifications at EU level, e.g. by explicitly allowing outsourcing of transaction monitoring under strict conditions (notably that the obliged entity does not outsource its liability/responsibility).
The EBF fully supports the principles of data protection and privacy that safeguard the protection of customer data, therefore ensuring trust towards regulated financial entities. Against this background, it remains important that banks can rely on EU-wide clarity on the interaction between the GDPR and AML/CFT requirements also in the area of bank-to-bank information sharing. Finding the right balance between data protection and the fight against financial crime, is key, also in the design of public-private and private-private partnerships.

Transaction Monitoring Netherlands (TMNL)

Criminals may use different banks to make transactions. To better identify patterns in these transactions obliged entities should share transaction data between themselves in a trusted network.

In the Netherlands, the biggest banks with the support, and in coordination with the national competent authorities, joined forces for the creation of the first shared transaction monitoring utility on payment data. This mechanism, which is still in pilot mode, aims to cross-check transaction data between the different databases of the participant banks, identifying criminal patterns, without organisations having access to the others' client data. As a first step, the TMNL will be operating in addition to each bank's KYC reporting systems. The public and private sectors are in constant dialogue for the alleviation of any operational/ legal challenges that may impede the well-functioning of the mechanism.

16/ Stimulate public-private information sharing and broaden the conditions under which operational data could be shared

While there are some positive examples of formal public/private cooperation in the field of counterterrorism and cybersecurity, the AML/CFT framework has so far focused narrowly on the administrative requirements imposed on banks and other regulated entities. The outcome of this rule-based approach is a massive flow of information to the competent authorities, which is typically unguided by feedback and limited by individual banks' limited intelligence picture. In addition, such a concept seems to contradict, essentially, the very basic privacy principles of proportionality and subsidiarity.
When filing a SAR / STR to their national FIUs, it is vital for banks to receive feedback on their reporting. Such two-fold information streams would facilitate the efforts of banks to identify more clearly, prevent and mitigate the risks of ML/TF, while also decreasing the need for further data processing of those who are not involved in such criminal activities. Nevertheless, as also stated in the European Commission's AML/CFT Package, FIUs, often understaffed, find it difficult to select the data, with an added value, out of all the volume of the data they receive. This rule-based approach results in inefficiency and, ultimately, deviation from the overall objective of detecting suspicious criminal activity. An agreement on typologies and the information that is necessary to be shared between the private and the public sector for the identification unusual/suspicious activities would improve the quality of the reporting and contribute to the efficiency of the process.
Another issue that banks and other obliged entities face, with regard to reporting, relates to the competences within jurisdictions. Currently, exchange of information from banks to national competent authorities is possible within the home country jurisdiction. However, banks find it extremely difficult to communicate information to public authorities located outside the home jurisdiction. Lack of adequate information and intelligence sharing with all relevant bodies impedes the speed with which organised crime should be addressed. Enabling banks to share information with other authorities could radically enhance the response to cross-border organised crime.

The EBF believes that public-private partnerships (PPP), where law enforcement information can be shared with obliged entities, should be strongly encouraged and embraced first and foremost by public authorities. Sharing of aggregated data, with the objective of fighting against criminals should already be possible under the existing legal framework, including GDPR. Exchange of operational data, however, is, at this stage only possible in counter-terrorism financing or where national PPPs have supplemented the EU regime with local legal gateways. The EBF

would welcome an EU AML/CFT framework that broadens the conditions under which operational data could be shared, including on a cross-border basis. Examples of national PPPs in jurisdictions inside and outside the EU could be used as best practices to develop a European model. This would imply the necessary removal of legal obstacles that may impede data sharing. A solid legal framework endorsed by, among others, data protection authorities, authorising under specific conditions such data sharing (including personal data) should be put in place.

Although challenging, it is also crucial that PPPs are supported at EU level to tackle cross-border threats. Given the limited competence the EU has in the area of law enforcement, the EBF would suggest that the mandate of Europol should be reviewed in such way that Europol would be entrusted with the competent EU law enforcement agency.

17/ Support at EU level the Europol Financial Intelligence Public Private Partnership (EFIPPP)

In this context, the existing Europol Financial Intelligence Public Private Partnership (EFIPPP) should be supported by authorities and reinforced in its role as the first EU-wide PPP.

Existing national Public-Private Partnerships (PPPs)

In Europe:

- **Austrian:** Public-Private-Partnership (PPP) Initiative
- **Germany:** Anti Financial Crime Alliance (AFCA)
- **Ireland:** Joint Intelligence Group (JIG)
- **Latvia:** Cooperation Coordination Group (CCG)
- **The Netherlands:** Terrorist Financing Taskforce
- **The Netherlands:** Serious Financial Crime Task Force (currently in pilot stage)
- **The UK:** Joint Money Laundering Intelligence Taskforce (JMLIT)

Outside Europe:

- **The Australian** Fintel Alliance
- **The Singapore** Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership (ACIP)
- **Hong Kong** Fraud and Money Laundering Intelligence Taskforce (FMLIT)
- **The US** FinCEN Exchange
- **US** 314(b) Financial Information Sharing Partnership

18/ Improve cooperation between public authorities

Several reports (e.g. consolidated FATF standards on information sharing, European Parliament Resolution for the state of play of the implementation of AML/CFT legislation, EBA Opinion on the communication of

money laundering/terrorist financing risks to supervised entities) have concluded that there is a need for closer coordination and information exchange among the main actors in the financial ecosystem and the wider regulated economy, both domestically and cross-border. Effectively, tackling financial crime requires a change of mindset from regulators and supervisors. Working in silos can no longer be the practice and all players should adapt and establish frequent communication channels between themselves based on trust and effective intelligence sharing legal gateways and procedures. In line with the RBA, this should include regulators responsible for non-financial regulated bodies, including money service businesses, law firms, estate agents, accountants, as well as trust and company service providers.

Similar issues also arise beyond the regulated sectors, with AML/CFT risks exacerbated by vulnerabilities and abuse of other sectors such as telecommunications and social media. While not all sectors pose sufficient AML/CTF risk to be regulated for customer due diligence and other AML/CFT requirements, all sector regulators should require companies to protect their customers from financial crime, such as by cooperating to close system vulnerabilities and by sharing financial crime intelligence.

Better cooperation and information sharing between prudential and AML/CFT competent authorities

- AMLD5 establishes an obligation for competent authorities to cooperate and exchange information, but it does not set out in detail how this should be achieved.
- The ESAs proposed Guidelines for AML/CFT colleges which aim to improve such cooperation and to clarify the practical modalities.
- These draft Guidelines propose the creation of AML/CFT colleges of supervisors and set out the rules governing their establishment and operation.
- AML/CFT colleges should be set up whenever three or more competent authorities from different Member States are responsible for the AML/CFT supervision of the same credit/ financial institution and its establishment. Since a firm with branches/establishments in three member states will be covered by the regime, a mapping exercise of firms is required prior to the establishment of colleges.
- Where the conditions for setting up an AML/CFT college are not met, supervisors will continue their cooperation and information exchange on a bilateral basis.
- Since information available to AML/CFT supervisors may also be relevant for prudential supervisors and vice versa, the Guidelines propose gateways to ensure that:
  - prudential supervisors can participate as observers in AML/CFT colleges; and
  - information from AML/CFT college meetings is available to colleges of prudential supervisors.

Priority 4
BE SMARTER

A major part of the financial crime challenge is to make sure that reporting entities are using the appropriate tools to fight money laundering and the financing of terrorism. However, banks create their investment priorities in line with supervisory expectations, which on their side are too often narrowly focused on meeting compliance requirements. With the annual cost of compliance for European banks reaching €100billion, funding from the development of new AML/CTF capabilities in the areas of artificial intelligence, machine learning and automation is often left aside for the biggest obliged entities. Nevertheless, efforts should not necessarily focus on using the most sophisticated or complicated tools, but on developing effective ones, which at the same time are in line with statutory and supervisory expectations.

Regulators should help demystify new technologies, as tools having the potential to increase the probability of banks' identifying and mitigating money laundering risk, by allowing for their wider application, following a RBA and within the boundaries of the GDPR. This would mean that the use of an Artificial Intelligence tool would in practice assist experts' judgment and make it more productive. Also, the use of Robotics Process Automation (RPA) (e.g. in the handling of transaction alerts) as well as advanced analytics increase the effectiveness and efficiency of AML/CFT processes. The Commission and EBA should closely monitor these initiatives in order to identify best practices, potential regulatory roadblocks and explore how they can be promoted at EU level. The use of shared utilities also requires the legal obstacles related to privacy and data protection to be mitigated or removed.

Shared KYC check capabilities ("KYC utility")

The EU framework should explicitly allow obliged entities to create joint KYC capacities under certain conditions, provided data protection and privacy rules are respected.

These KYC utilities should be:

- based on clients' consent;
- in line with competition law rules (notably, the utility should not exclude new members from joining on a reasonable basis).

KYC utilities are not only useful tools for banks, but they also have the potential to bring about significant efficiency gains for customers, as they would spend less time responding to KYC requests. In turn, this would allow banks to re-orientate staff to areas where they can contribute more significantly to the fight against financial crime.

A good example for such an initiative is the new KYC shared utility within the beneficial owner register of Austria, which provides legal entities the capability to upload the documents for the identification and verification of the beneficial owners via qualified parties (e.g. lawyers or tax advisers) ("Compliance Package"). Banks are then able, generally, to rely on these documents, which need to be updated or confirmed by the qualified party on an annual basis.

19/ Ensure beneficial ownership transparency based on better designed UBO registers that are checked by public authorities and are useable for obliged entities

One of the most striking examples of how technology can facilitate banks' compliance work is the ultimate beneficial owners' (UBO) registers developed under AMLD4 and AMLD5. Beneficial ownership transparency is a key step towards enhancing the efficiency and effectiveness of the AML/CFT framework. At the same time, transparency of legal entities in the respective registers is a crucial contribution to the system against financial crime and the disruption of society as a whole.
However, these registers have not been adequately designed to help reporting entities perform due diligence more consistently, or to allow for global beneficial ownership transparency.

From the European banking sector perspective, what is important is the quality (completeness, accuracy and timeliness) and accessibility of beneficial ownership information, which is required for customer due diligence purposes. Publicity does not necessarily guarantee quality, however, so it is important that national authorities establish their own checks to ensure accurate and up-to-date information.
It is important that inconsistencies between the national implementation of these new reporting requirements are identified and addressed through legislative harmonisation, to improve overall efficiency and effectiveness.
The EBF also supports the interconnection of national UBO registers, as required by the AMLD5, which would provide competent authorities with a holistic oversight of the relevant information and also provide for the uploading of documents for the verification of the beneficial owners. In this regard, transnational cooperation between authorities is crucial for finding the necessary common ground in order to alleviate legal (incl. data protection) barriers. Specific attention should be paid to ensure a full access to data by obliged entities throughout the EU.
In addition, banks should be allowed to rely on publicly verified UBO registers' data for KYC purposes.

Prerequisites for efficient UBO registers

- The quality (completeness, accuracy and timeliness) and accessibility of beneficial ownership information, which is required for CDD purposes, is key in the creation of effective tools.
- AMLD4 and AMLD5 impose on banks mandatory reporting of discrepancies identified between beneficial ownership information held on public registers and the banks' own UBO information. This is not an efficient use of resources and it would be more effective if

national authorities would verify beneficial ownership information to ensure accurate and up-to-date information.

- It is important that inconsistencies in national transposition laws are addressed through maximum harmonisation of EU law. For instance, currently, some national reporting requirements apply to all discrepancies, including spelling and formatting, while others are more narrowly focused on material anomalies and contradictions, indicating that the beneficial owner is not as described as in the public register.
- It is also important that any new obligations do not undermine the efficient functioning of the market.

20/ Encourage the use of enhanced analytics and machine learning tools for KYC purposes which are respectful of privacy rights

Rapidly evolving business and technology make conventional methods for AML/CFT inefficient and call for a more innovative approach towards the fight against crime. Both banks and competent authorities should encourage the use of new technologies for building tools that leverage on advanced analytics and machine learning, making sure that there is room to explore these possibilities taking into account the privacy principles of the GDPR.
The EBF welcomes the recent EBA guidelines on regulatory sandboxes and innovation hubs, with national initiatives demonstrating the potential for supervisors to use these approaches to support financial crime-focused innovation. It would be helpful if EU authorities support the industry in understanding emerging best practice in the use of new technologies/analytics and provide a regulatory "safe space" to test these, e.g. as seen in the UK at the FCA TechSprint.

In particular, data science could be exploited to put in place common digital platforms to assist reporting entities in collecting, processing, updating and sharing KYC information, while centralising these operations in a synergy with all participating banks. Properly designed machine learning algorithms and AI can help reporting entities monitor transactions by sorting through the enormous amount of "alerts" and selecting only the critical ones. Machine learning will allow algorithms to identify patterns in criminal activity and update accordingly the screening filters of the tools in an agile manner.
Smart technologies are even more pertinent in a world where both legislation and consumers mandate quick transactions, both the wholesale markets and consumers. The emergence of instant payments, where the time to spot suspicious activity is clearly reduced significantly, is a prime example of this challenge.

Table of abbreviations

AFCA	Anti Financial Crime Alliance (Germany)
AI	Artificial Intelligence
AML/CFT	Anti-money laundering and counter-terrorist financing
AMLD	Anti-money laundering Directive
AMLR	Anti-money laundering Regulation
CCG	Cooperation Coordination Group (Latvia)
CDD	Customer due diligence
CRD	Capital Requirements Directive
CRS	Common Reporting Standard
DAC	Directive on Administrative Cooperation
EBA	European Banking Authority
EBF	European Banking Federation
EC	European Commission
ECB	European Central Bank
EDD	Enhanced due diligence
EDPB	European Data Protection Board
EFIPPP	Europol Financial Intelligence Public Private Partnership
EPPO	European Public Prosecutor's Office
ESAs	European Supervisory Authorities
FIU	Financial Intelligence Unit
GDPR	General Data Protection Regulation
FATF	Financial Action Task Force
JIG	Joint Intelligence Group (Ireland))
JIMLIT	Joint Money Laundering Taskforce (UK)
KYC	Know Your Customer
MER	Mutual Evaluation Report
OECD	Organisation for Economic Co-operation and Development
PPP	Public-private partnership
PSD	Payment Services Directive
RBA	Risk-based approach
SAR	Suspicious Activities Report
SNRA	Supranational Risk Assessment
SREP	Supervisory Review and Evaluation Process
SSM	Single Supervisory Mechanism
STR	Suspicious Transactions Report
TM	Transactions Monitoring
UBO	Ultimate Beneficial Owner
VAT	Value Added Tax

About European Banking Federation

The European Banking Federation is the voice of the European banking sector, bringing together national banking associations from across Europe.

The EBF is committed to a thriving European economy that is underpinned by a stable, secure and inclusive financial ecosystem, and to a flourishing society where financing is available to fund the dreams of citizens, businesses and innovators everywhere.

For more info on the report please contact

Roger Kaiser
Senior Policy Adviser - Fiscal & Anti-Money Laundering
r.kaiser@ebf.eu

Iliana Koutoulakou
Policy Adviser - Compliance, Tax & Security
i.koutoulakou@ebf.eu

Photo credits: Adobe Stock
Design: alchemiser.com


#AMLactions
www.ebf.eu

Brussels I 56 Avenue des Arts, B-1000, Brussels
Frankfurt I Weissfrauenstrasse 12-16, D-60311, Frankfurt am Main

+ 32 3 508 37 11 I **www.ebf.eu** I **info@ebf.eu** I **#EBF**

twitter.com/EBFeu
linkedin.com/company/europeanbankingfederation