EBF Response to Public Consultation on Guidance on the Rules Applicable to the Use of Public-Private Partnerships in The Framework of Preventing and Fighting Money Laundering and Terrorist Financing

General comments

Information sharing in the context of fighting financial crime is critical in ensuring the effectiveness of the AML/CFT rules. FATF, in its Guidance on Private Sector Information Sharing[1], has recognised that effective information sharing is one of the cornerstones of a well-functioning AML/CFT framework. Weaknesses in information sharing between obliged entities, financial intelligence units and law enforcement authorities may inadvertently facilitate the activities of criminals who operate nationally or across borders.

At present, obliged entities send large numbers of SARs to FIUs with no or insufficient quantitative feedback. This situation does not allow obliged entities to focus on the most relevant predicate offenses and leads to an increased number of false positives. Often finding the relevant information for law enforcement authorities may feel like finding a needle in a haystack. Allowing for a two-way information stream would hence lead to an improvement in the overall quality of SARs and reduce the number of false positives, which would allow focusing on actionable data. Therefore, if an intelligence-led approach were applied in the AML/CFT framework, obliged entities could receive information on current trends and typologies, as well as operational data which would allow them to focus their efforts on priorities as defined by law enforcement authorities. As a result, obliged entities would be able to send back more actionable data and do it in a smarter and aligned with data minimisation requirements way, reporting information when truly necessary.

Furthermore, while the intention of the AML/CFT regime may be for obliged entities to identify suspicions of crime within their business, at present there are practical challenges in doing so on an individual basis. The complex nature of money laundering and terrorism financing, often involving cross-border flows of funds and the involvement of many layers of entities, makes it challenging to detect such crimes when the data available to do so is mainly limited to a regulated entity's own customer base and available open-source intelligence. Being able to enrich this view with information from other private sector entities and competent authorities enhances the likelihood of effective detection for all parties involved in a public-private partnership (PPP). It also allows both obliged entities and public authorities to form a holistic overall view of the current trends.

[1] FATF (2017), Guidance on Private Sector Information Sharing, FATF, Paris www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-information-sharing.html.

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

In practical terms, there are already numerous examples of PPPs in the AML/CFT domain across Europe. Those initiatives vary in terms of maturity. Some have already proven their value, while others are still in more nascent stages of development. The following examples could illustrate the PPP landscape across Europe:

- The UK Joint Money Laundering Intelligence Taskforce (JMLIT) was launched as a pilot in 2015 and has become permanent since April 2016. Between its inception in 2015 and September 2021, JMLIT resulted in partnership impacts including: £59m in suspect criminal assets restrained; over 265 arrests; 4,200 accounts identified that were not previously known to law enforcement; and 41 alerts (typology knowledge products) produced[2].
- The Netherlands Terrorist Financing Taskforce (TF Taskforce) was formally created in 2017. In 12 months, the partnership presented 15 cases, prompting the investigation and reporting of more than 300 reports from regulated entities. Of these reports, 64% were declared 'suspicious' by the FIU and disclosed to law enforcement agencies, compared to a national average of 10% of all the reported transactions being declared suspicious in the Netherlands[3].
- Latvia's Cooperation Coordination Group (CCG) was launched in May 2018. In 2019, FIU Latvia organised 107 CCG meetings, 58 of which focused on operational cases, 17 CCG on feedback, and 32 on other issues. There have been several cases solved at operational level as a result of the functioning of the CCG.
- SAMLIT, the Swedish Anti-Money Laundering Intelligence Taskforce, is an initiative that was launched in 2020 in which the Swedish Police Authority and the five largest banks in Sweden cooperate to further strengthen efforts to combat ML/TF. At the end of 2020, a decision was made to turn the project into a permanent, formalised cooperation. The object of SAMLIT is to enable improved effectiveness in the sharing of intelligence between the participating banks and the Swedish Police Authority to support the detection, investigation and prevention of ML/TF.
- In Luxembourg, an Expert Working Group in Private Banking has been established which encompasses representatives of the private banking sectors, the financial supervisor and the financial intelligence unit. Typologies and best practices are shared within this group, sometimes with the issuance of risk analysis stemming from the financial supervisor (the CSSF).
- In Denmark, there is an ongoing analytical work on an AML/Transaction Monitoring initiative which has been initiated by the Danish Central Bank, the Ministry of Industry, Business and Financial Affairs, and the financial sector.
- The Europol Financial Intelligence Public Private Partnership (EFIPPP), created in December 2017, is an example for a PPP of a cross-border nature. Participants and observers are large financial institutions, FIUs and law enforcement agencies from an increasing number of jurisdictions, mainly European countries. As of February 2021, EFIPPP has contributed to the development of 22 typologies covering, e.g. investment fraud, correspondent nesting structures, trade-based money laundering, human trafficking, terrorist financing, virtual currencies, and narcotics, among others. Those numbers have increased throughout the rest of 2021[4].

[2] Source: UK Finance.

[3] Nick J Maxwell – 'Expanding the Capability of Financial Information-Sharing Partnerships', Royal United Services Institute for Defence and Security Studies Occasional Paper (March 2019).

[4] Source: Europol.

Taking into account their potential and the positive results achieved already, the EBF welcomes the European Commission's efforts with regards to strengthening the role of PPPs as a crucial step in the right direction on the path to tackling financial crime. It is important to note, however, that enhanced information sharing between banks and FIUs, as well as between banks, will also require legislative actions. This particularly concerns operational data sharing on specific transactions and individuals/corporates. A sound legal basis for such information exchange would ensure legal certainty and striking the balance between fighting organised financial crime, on the one hand, and personal data protection consideration, on the other hand.

Role of PPPs in the exchange of strategic information

The exchange of strategic information within PPPs in the AML/CFT domain contributes to overcoming many of the challenges that both obliged entities and public authorities are facing in their efforts to enhance the effectiveness of the fight against money laundering and financing of terrorism. The biggest advantage of this type of cooperation is the possibility to establish a two-way communication channel between obliged entities, on the one side, and FIUs and law enforcement authorities, on the other.

Information from FIUs enables banks to perform deeper and broader analyses, which in turn contributes to improving the effectiveness of their AML/CFT programmes. It allows banks to search for similar patterns, connected individuals and transactions, thus improving their transaction monitoring. Likewise, sharing strategic risk information allows FIUs and banks to develop more detailed risk typologies that can be used to improve awareness of new criminal techniques and emerging threats.

It is important to recognise that strategic information sharing can improve the targeting of AML/CFT procedures and the proportionality of data processing. For example, by developing and communicating detailed risk typologies, PPPs can seek to reduce the number of scenarios where a whole industry is identified as high risk, and instead improve understanding of the specific indicators of risk, or the specific activities that may be undertaken within an industry that are higher risk and require enhanced due diligence. In this way, strategic information sharing can help reduce the risk of wholesale de-risking or elevated risk ratings being applied too broadly to customers and clients.

EU-level guidance could support wider and deeper public-private sharing of aggregated data and trend analysis. To be able to improve risk assessments, KYC-processes, transaction monitoring and reporting, obliged entities need to receive information on an ongoing basis. Criminals are constantly adapting their activities and modus operandi in order to exploit identified weaknesses in, e.g., legislation, products and services. Therefore, feedback from FIUs and law enforcement authorities needs to be regular and up to date. Given the difficulties faced by FIUs to provide feedback to obliged entities on an individual basis, PPPs provide an opportunity to exchange information on current trends and typologies.

Furthermore, it is common observation that national risk-assessments are not updated frequently. Therefore, the sharing of information between obliged entities and relevant authorities is of great importance for keeping up with criminals' activities. This in turn leads to obliged entities detecting more criminal networks and to improving the quality of investigations through focusing resources where the real threats actually lie.

In concrete terms, feedback on at least the following points would contribute to improving the quality of SARs and hence to reducing false positives:

- general feedback on the outcome of reporting, i.e. how many of the bank's reports have resulted in further investigations and, subsequently, in convictions;
- on the quality of SARs, i.e. whether the reported information is complete and of good technical quality;
- whether the obliged entity has missed certain red flags and/or certain ML/FT-risks associated with its products and services;
- whether there are known modus operandi and typologies the obliged entity has seemingly missed.

Role of PPPs in the exchange of operational information

The EBF believes that PPPs, where law enforcement information can be shared with obliged entities, should be strongly encouraged and embraced first and foremost by public authorities.

At present, due to the widespread lack of feedback, obliged parties usually have only abstract typology papers on modus operandi of money laundering and terrorist financing. Similarly, the specifications in the cascading risk analyses are too often overly general and not very flexible. A regular and/or occasional and flexible exchange of more detailed risk analyses and operational information between law enforcement authorities and obliged parties under money laundering legislation offers the opportunity for more up-to-date and focused investigations with better results. Examples in various EU Member States and other leading financial centres have already proven this as mentioned above. These improved results are not limited to more efficient analysis and investigations by obliged entities, or even to an increase in the number of reports, but include a significant increase in high-value intelligence provided to the national FIU as well as the actionable intelligence provided by the national FIU to law enforcement.

Consensus on more detailed and actionable typologies and on the information to be shared between the private and public sectors for the purposes of identifying unusual/suspicious activities would improve the quality of the reporting and contribute to the efficiency of the process. FIUs, law enforcement authorities and obliged entities have unique roles and perspectives on combating financial crime and enabling effective communication between them would in turn render better results. In this context, better cooperation between FIUs and financial institutions is an absolute priority.

Sharing of aggregated data, with the objective of fighting against criminals should be possible under the existing legal framework, including GDPR. Sharing of public sector analyses and trends with obliged entities is already taking place, although we believe EU-level guidance could support wider and deeper public-private sharing of aggregated data and trend analysis. Sharing operational data, however, seems to only be possible, at this stage, in the context of counter-terrorism financing (within the limits established by the local laws implementing EU AML/CFT legislation), in line with fraud prevention, or where the EU regime has been supplemented with local legal gateways.

By receiving operational data, obliged entities who are members of such PPPs are made aware of priority threats from the perspective of law enforcement or other public agencies and can use this information to search their systems in response to that identified suspicion or indicator. Consequently, they would be able to more effectively identify suspect

accounts linked to money laundering activity and report them, which can contribute to the data minimisation principle as enshrined in the GDPR. 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, like the ones mentioned above, 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. The EBF maintains that the proposed AML package should provide for such legal basis.

Data security arrangements need to be proportionate to the information being shared, and PPP arrangements for operational information sharing include a range of safeguards including vetting of participants, clear guidance and undertakings on use of data, secure channels for sharing and formal governance structures including procedures for dealing with breaches of the guidelines. Banks are familiar with these types of safeguards due to their obligations to report suspicious activity and avoid tipping off, and manage the sharing of information required for AML/CFT within international banking groups. PPP arrangements can therefore build on established banking systems to ensure confidentiality of information and to ensure that relevant information is only used for ML/TF risk management.

Transnational public-private partnerships

It is crucial to recognise the international dimension of cross-border financial crime schemes. In almost every case there is an international footprint, but laws and regulations can prevent or prohibit the effective sharing of information across the borders. Where cross-border sharing is possible, it is often restricted to a one-way disclosure with little or no feedback. Further work on this issue is required to ensure that PPPs can make a full contribution to the international fight against financial crime.

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 more rapidly share and receive information with other authorities could radically enhance the response to cross-border organised crime, including existing campaigns to map and disrupt international networks of human trafficking, money mules and card fraud.

We believe the potential of PPPs needs to be further explored, especially in the cross-border context. The work of the Europol Financial Intelligence Public Private Partnership (EFIPPP) and its growing network allows for the dissemination of strategic information, such as up-to-date threats and typologies, to a broad array of actors at the forefront of fighting financial crime, adding to the effectiveness and efficiency of ongoing investigations. The potential of EFIPPP could be further exploited through expanding its role so that it acts as a coordination mechanism for existing national AML/CFT public-private initiatives. As part of this coordination role, EFIPPP could assist in identifying priorities and in the exchange of actionable data. We would also support the exchange of operational data in the context of EFIPPP, which would be limited to full members of the initiative only and under conditions that allow being respectful of the privacy rights of

individuals, whereas the identification of priorities may be linked to the European Commission's Supranational Risk Assessment.

Concluding remarks

PPPs are a valuable tool for improving the efficiency and effectiveness of the EU AML/CFT framework. Some very positive examples have already made a substantial contribution to improving outcomes by fostering productive information exchange. To reap the full potential of PPPs and information sharing, however, the existing legal limitations need to be addressed. Money laundering/terrorist financing cannot be fought in isolation. Information sharing should be supported between public authorities and the private sector, both across the single market and internationally. Focus needs to be put on personal data protection rules and ensuring legal certainty in their application while respecting requirements related to personal data protection principles such as data minimisation, proportionality and transparency.