BSG 2021 026

12 April 2021

BANKING STAKEHOLDER GROUP

# BSG own-initiative advice[1]: AML strategy

In 2020, the EBA's enhanced mandate for AML across the financial services sector took effect[2] and the European Commission also published its Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing.[3]

The Banking Stakeholder Group (BSG) welcomes these developments and has developed this Own-Initiative Advice on AML Strategy to support the EBA's work and reflection on the future evolution of AML in the Union. The Advice provides a framework within which we will respond to the EBA's forthcoming consultations on specific aspects of the new regime. We have also reflected on how the risk environment is impacted by the COVID-19 pandemic as this will be an important consideration in the years ahead.

## General considerations

Global integration of the financial system, together with the rise of new technologies, contribute to further sophistication and development of financial crime.

The recent scandals implicating institutions across the EU financial sector have affected the reputation of the EU's financial system and have seen the EU increasingly under pressure to address shortcomings - in particular those resulting from a lack of cooperation between local authorities at EU level, as well as a lack of harmonisation across the EU's legal system.

A considerable amount of resources is invested by both the public and private sectors to fight against money laundering. Financial institutions notably invest huge amounts in compliance systems, while also filing millions of suspicious transactions reports with the authorities. As such, banks are currently by far the largest contributors of suspicious activity/transaction reports (SARs/STRs) to public authorities. Although some European banks may recently have not been fully successful in complying with their AML obligations, and it is important that such failings are addressed, the more fundamental question of the effectiveness of the overall AML system arises.

[1] In accordance with Article 37 of Regulation (EU) No 1093/2010 the BSG may submit advice to the Authority on any issue related to the tasks of the Authority with particular focus on the tasks set out in Articles 10 to 16, 29, 30 and 32. These represent the independent views of the BSG.

[2] Regulation (EU) No 1093/2010, in particular Articles 9a and 9b.

[3] https://ec.europa.eu/finance/docs/law/200507-anti-money-laundering-terrorism-financing-action-plan_en.pdf

While financial institutions play a key role in tackling money laundering and prevention of terrorism, the regulated sector for AML is much wider and rightly includes lawyers, accountants and others with the potential to facilitate - or prevent – the laundering of funds. It is important to ensure that these sectors are also subject to high quality, co-ordinated supervision in order to prevent weak links in the AML regime and to ensure that there is appropriate interaction between these supervisors and financial sector AML supervisors. As typologies evolve, and particularly given the use of social media and other technology platforms to attract consumers to fraudulent offers, consideration may also need to be given to further widening the regulated sector. Where the perimeter is broadened, as with the recently-implemented inclusion of virtual asset services providers under the 5AMLD, it is important not only that the European Commission continues to ensure effective transposition, but that the EBA leads and co-ordinates supervisors' oversight of the new regime to ensure that it is properly embedded and provide effective, common solutions to supervisory challenges that arise.

Given the global interconnection of the financial system noted above, and the potential for criminals to operate cross-border, it is also important that as well as fostering enhanced co-ordination and co-operation within the EU, AML standards are aligned as far as possible to those in place internationally and they are implemented in a way that promotes international consistency and collaboration. This will enhance both the effectiveness and efficiency of AML.

New technologies and analytical techniques provide opportunities to enhance and streamline the identification of potentially suspicious activity and the quality of information which can be provided to law enforcement. However, fully capitalising on these possibilities means enhanced collaboration between authorities, between the public and private sectors, and the pooling and analysis of data across financial institutions.

This in turn needs to be done in a way that is not unduly cumbersome for consumers wishing to access and use financial services and does not disadvantage consumers who have a legitimate need to access financial services but may, for example, have non-standard identification. It will therefore be important for EBA to continue to monitor de-risking and to ensure that new AML initiatives do not have unintended consequences.

We welcome the EBA's efforts to integrate more systematically the consideration of AML in core supervisory areas so that risks are taken into account in prudential supervision and given appropriate weight by firms' management bodies and supervisory boards.

This is particularly important given the renewed challenges that financial institutions and consumers face from fraud and money laundering during the pandemic. It will be crucial that supervisory and management attention remains focused on managing AML risks.

However, as discussed further below, we consider that legislative changes are likely to be needed to ensure that AML rules are consistent across the Union and with other EU legislation, and to facilitate the necessary information sharing at different levels.

To be effective, the fight against AML/CFT should be based on true and in-depth cooperation between public and private entities with an emphasis on effective risk mitigation rather than tick-box compliance.

It is opportune and timely to address current shortcomings of the AML/CFT framework and its implementation. It is therefore welcome that the EU is currently working - after a critical review - on the improvement of its AML/CFT regime.

## Further harmonisation

Legal requirements for AML/CFT currently vary across the EU. 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.

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.

The objective of turning AML directives into directly applicable EU regulation is therefore to be supported. Such harmonisation would enable European banks that operate cross-border, and 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. This should also be followed by a simplification and standardisation of the rulebook on how cross-EU banking groups manage risk but also minimising options and discretions to Member States, coupled with sufficient minimum powers for competent authorities to supervise and, where necessary, enforce the rules.

Finally, the review of the current regulatory framework also offers the opportunity of a better alignment between AML/CFT requirements and other sometimes conflicting requirements in the practical implementation by financial institutions, e.g.

- **PAD (Payment Account Directive 2014/92/EU).** The conflict between the right for all EEA citizens to have access to a payment account while at the same time preventing financial crime is a delicate balance for financial institutions and it is important to ensure that AML risks can be appropriately managed without putting unreasonable obstacles in the path of individuals trying to obtain basic banking services. The EBA should clarify the interplay between the AML/CFT provisions and the EU Directive on payment accounts which grants the right to a basic bank account to all citizens. The EBA should also convene discussions on practical solutions which have been identified in Member States to provide appropriate access to basic banking alongside appropriate, risk-based AML measures and how this has been achieved.

- **Competition law.** Competition authorities have in some cases disallowed exiting of customers, also where there is an elevated risk for financial crime including ML/TF. Competition authorities should work closely with the financial supervisors in cases where there are considerations of compliance with financial crime regulations and coordinate such decisions so that the financial institutions do not come into conflict with the Money Laundering Acts as a result of compliance with a decision from the competition authorities.

- **GDPR.** There are several situations where GDPR conflicts with effective prevention of financial crime. For example authorities have asked financial institutions for records of historical AML cases for an ongoing investigation and these have not existed because the bank was obliged to delete them. This is further enhanced by the fact that obliged entities often face different local supervisory authorities (such as local financial services regulators and data protection authorities (DPAs), the local guidance and interpretation of the legislation tends to get one sided and obliged entities are left balancing conflicting areas.

- **GDPR.** Screening for adverse media is another challenge. If an entity is a customer of a bank in more than one country, the bank/branch of country X would not be permitted to disclose adverse media screening information to the bank/branch of country Y, as part of the customer specific risk assessment conducted in bank/branch of country Y. Also, adverse media screening is not allowed in all jurisdictions. Further, screening for additional sanction lists other than the EU and UN lists is another challenge: e.g. the US obliges banks to screen certain OFAC lists but there is little guidance as to what extent such screening would be permitted and relevant. In fact, in some jurisdictions the local DPA does not allow screening against all relevant lists. Our recommendation is to add sanction lists screening beyond EU/UN lists. This issue is further complicated by the UK leaving the EU, which will necessitate the inclusion also of the UK relevant lists in the screening process by the DPA.

- **GDPR.** Recognition of foreign jurisdictions and foreign supervisory mandates for cross border institutions. International institutions face issues when it comes to data retention and data submissions, e.g. in connection with supervisory requests if they have a presence which spans outside of the EEA. As an example, a supervisory request for information by a US regulator is not fully recognised as a lawful purpose to retain data for an EU institution which creates unnecessary unclarity for any institution that operates in the US market.

- **PSD II.** PSD II requires banks to provide payment account services for PSPs (Payment Service Providers). However, there is unclarity regarding how AML concerns (e.g. regarding identification of beneficial owners(s)) should be used in connection to declining an account for a PSP. This is further emphasised by the fact that local competition authorities are usually unaware of AML issues connected to this segment of market participants. While PSD II provides a right for PSPs to obtain 'payment account services', there are different interpretations when it comes, for instance, to the type of account that is to be provided, the responsibility for credit institutions to conduct transaction monitoring on such accounts and any requirements to identify and verify the PSPs' customers (i.e. the persons/entities whose funds are transferred through such accounts) and ultimately the right to reject PSPs' payment account services on ML/TF grounds. We recommend that further clarification be provided regarding account holding banks' obligations, also regarding their responsibilities in terms of transaction monitoring.

- **EU Wire transfer regulation (2015/847).** The operational set-up of some PSPs through bundled payments, for instance, makes it impossible for the account-holding banks on the recipient and sending side to identify the payer and the ultimate beneficiary. Further, there are examples of bundled payments going through a chain of PSPs where each individual PSP in the chain does not necessarily know the ultimate beneficiary or even how many underlying transactions there are. In cases where these chains involve multiple PSPs in multiple jurisdictions, there is an increased risk that each PSP is following local legislation with the information available to them. However, they do not have access to the full payment information, which could entail restricted persons or

corporates. Compared to interbank transactions where the SWIFT communication system is used, each bank has full details of the remitter and beneficiary and will also take full responsibility for screening the transaction.

- **AML in relation to securities.** Less attention has been paid to supervisory expectations in relation to AML monitoring in securities markets and this is an area where further guidance would be useful. In addition, it would be helpful to reflect on whether all securities firms and infrastructure providers are subject to the appropriate AML obligations to ensure there are no 'weak links' in the holding chain.

## Empowering EU authorities

Legal requirements for AML/CFT currently vary across the EU. 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. Current institutional and functional fragmentation renders the fight against financial crime more difficult, as financial activities, as well as criminal activities, are cross-border.

Coordination and cooperation at European level is essential, in particular, where the risks are more significant. Such co-ordination is needed internally within the EU, and will also support appropriate coordination and cooperation with international standard setters and supervisory authorities.

It is a positive step that EBA is now benefitting 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. The enhanced role of the EBA as a rule setter, which is its DNA, is to be supported.

The role of supervisors in AML/CFT should also be reinforced, with the aim to enhance supervisory convergence focusing on risks and ensure efficient EU/EEA and cross-border coordination of AML/CFT supervisors. The objective should be to ensure high quality and consistent risk-based AML/CFT supervision, seamless information exchange and optimal cooperation between all financial supervisory authorities.

Furthermore, 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.

If a better coordination between supervisors is materialised through a centralisation of supervisory powers in one European body (as suggested by the European Commission), then the mandate should be clarified 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 financial institutions, duplicate supervision must be avoided and a broad scope including all Member States and all obliged entities (beyond the financial sector) must be considered while ensuring that sufficient resource and geographical coverage is maintained to support effective supervision, including where on-site assessment is needed.

The assessment as to the respective institution's risk profile should take into account a number of measures such as the risk profile of the business undertaken, the possible impact of these activities and, importantly, the risk mitigation techniques and past supervisory track record of the respective institution, including any action the institution has taken to address past deficiencies. Any transfer of supervisory responsibility or decision on a possible joint EU and Member State supervision should follow a rigorous review and should not be taken based on automatic thresholds or by designating particular sectors.

In addition to the regulatory and supervisory authorities, the EU should also improve cooperation and strengthen the Financial Intelligence Unit (FIU) functions across the EU/EEA. The FIUs should be interconnected to avoid duplication and enhance the efficiency of the investigation, in particular at cross-border level. Some sort of central coordination should be organised, possibly with the support of Europol, notwithstanding the recent European Data Protection Supervisor decision that prohibited Europol from processing personal data. In line with the reasoning on regulation and supervision, a more European approach would reduce the risk of criminals exploiting weaknesses across jurisdictions, while it would also mirror the cross-border nature of financial crime.

## Enhancing cooperation and consistency

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.

Cooperation remains unfortunately subdued and often quite ineffective. It can be caused by legal restrictions or uncertainties on what is possible in terms of information sharing. Impediments to information sharing impact the ability of both the private and the public sector to share essential information to detect malicious activity effectively, creating potential systemic risks and eventually threatening financial stability.

Adopting a coherent approach for information sharing, balancing data protection and financial crime prevention is essential. Consistency between the AML and the GDPR frameworks is very important to ensure an effective approach in AML/CFT. A preferred approach could be to adopt an EU/EEA-wide GDPR AML/CFT Guidance. 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.

Information sharing capabilities and cooperation need to be improved on three levels.

- Firstly, **between authorities**, both between different authorities within countries as well as cross-border.

- Secondly, there is a need to strengthen the capabilities of financial institutions and authorities to combat financial crime through increased possibilities to share and analyse information e.g. in the form of **designated PPPs**. This would enable the analysis of financial crime activities across several financial institutions.

- Thirdly, enhanced possibilities to **share information between financial institutions** would strengthen capabilities to identify individuals and corporates that engage in financial crime. This is

challenging to achieve within the current legal framework without breaching customer confidentiality.

Improved cooperation between public authorities - both domestically and cross-border - is key. This was highlighted by several reports from EU authorities in the post-mortem scandals' assessment. Cross-border co-operation is also essential from a reputational point of view. There are also examples of where data sharing between the different departments of, for instance, a tax authority has prevented the effective prevention of tax fraud. Working in silos can no longer be the practice and all players should adapt and establish frequent communication channels between them based on trust and effective intelligence sharing, legal gateways and procedures. This should include banks' supervisors, AML authorities, FIUs, police and other law enforcement agencies.

Facilitating information sharing between financial institutions, notably by removing legal obstacles to the use of shared utilities, would greatly help banks and enhance the effectiveness of the AML/CFT framework. It would not only create synergies but also help to combine efforts and alerts from different institutions, as well as develop further intelligence with the ability to better detect crimes. However, the current EU data protection limits mechanisms for sharing AML/CFT information outside the organisation (bank-to-bank). Public/private partnerships (PPPs) can be much more effective where data-sharing of individual cases is allowed as well as 'trend spotting/modus operandi' information.

Third party information sharing, e.g. via a shared utility, is generally limited. Some jurisdictions are exploring this idea within the legal boundaries and may have to modify their existing laws. The new AML/CFT rules should allow a centralisation of the KYC and transaction data collected by banks with the necessary security and data protection safeguards. Consideration would need to be given to appropriate mechanisms to ensure that users or consumers were not inappropriately excluded from access on the basis of such a mechanism, and also to enabling appropriate participation in the mechanism by non-bank financial institutions.

Alongside the potential benefits of PPPs (which can give participants additional insight into sources of risk) and KYC utilities (which likewise give participants additional access to risk information from third parties), consideration needs to be given to how respond to the potential transfer of additional risk (such as higher risk clients, or less information on which to base effective risk management) to non-participants who may not have access to these insights, particularly where participation in the PPP or KYC utility is restricted.

Public-private information sharing in the broader sense should also be supported. When filing an SAR/STR with their national FIUs, it is vital for financial institutions to receive feedback on their reporting. Such two-fold information streams would facilitate the efforts of banks to more clearly identify, 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.

Having harmonised templates to file an SAR/STR, appropriately tailored to the needs of different reporting sectors, would make the system more efficient and this would facilitate cooperation. Currently, it is at the member countries' discretion whether non-domestic institutions (which operate in a country though a passported license) are subject to local AML rules and reporting requirements, or not. This should, in our view, be taken care of through a reporting infrastructure between EU FIUs, rather than though each individual obliged entity, which should be able to file through its 'home' FIU.

More generally, public-private partnerships (PPPs), where law enforcement information can be shared with obliged entities, should be strongly encouraged and embraced first and foremost by public authorities. Exchange of operational data, under strict conditions, would dramatically help banks and other obliged entities to identify criminal activities. Furthermore, it would enhance the capabilities of institutions and potentially the authorities including FIUs, to identify patterns of criminal activity across different financial institutions and thus identify weakness in AML systems and controls and individuals and corporates that are involved in financial crime activities e.g. by using advanced analytics/new technology such as network analysis. The adoption of an EU AML/CFT framework that broadens the conditions under which operational data could be shared, including on a cross-border basis, would therefore be rather decisive. Such a solid legal framework would need to be endorsed by the data protection authorities.

Finally, sharing information between financial institutions would enhance capabilities to detect financial crime, e.g. in situations where one financial institution has ended a customer relationship based on suspicions of financial crime. The financial institution to which the customer turns has no information of the (potentially criminal) activities at the previous bank as bank-to-bank information sharing is difficult. Amending AML/CFT legislation to include possibilities of sharing information based on the same transaction criteria alone would provide better opportunities to share information and identify financial crime. Moreover, it is likely that financial institutions would be more positive about onboarding customers also when there is a higher risk because they would be better able to assess the risk. Information sharing between financial institutions regarding this type of information could also be organised by utilising the PPP and the central registry of bank accounts in each country.

## Supporting the use of appropriate tools

A major part of the financial crime challenge is to make sure that reporting entities are using/have access to the appropriate tools to fight money laundering and the financing of terrorism.

Regulators and supervisors could help demystify new technologies, as tools with the potential to increase the probability of banks' identifying and mitigating money laundering risk, by allowing for their wider application.

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. 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. 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. The interconnection of national UBO registers is also essential within the single market as companies are crossing the borders to do business. In time, further harmonisation of the method of determining beneficial ownership may need to be considered.

## Avoiding unintended consequences

It is important to ensure that regulated firms do not respond to the AML challenge with blanket 'de-risking' of types of consumer or other customer. In particular, it must remain possible for consumers with non-standard identification to access payment services, and important for fully realising internal market benefits that ID requirements are not unduly onerous for EU consumers opening accounts in other Member States.

In this respect it is important to ensure that AML/CFT rules do not exacerbate financial exclusion by including continuing provisions for the opening of a limited payment account (maximum withdrawal and transfers, maximum deposit) supported by adapted requirements on proof of identity and customer due diligence. Consideration therefore needs to be given to how to support not only millions of EU citizens who are financially excluded, including those who may, for example, not have a fixed address, but also incoming asylum seekers who risk being further marginalised if they cannot access mainstream financial services.

It is also important to enable effective competition as well as risk mitigation by ensuring that a consistent approach is taken to supervision of the same risk whichever type of institution it arises in (e.g. supervisors need to consider the payments business in a consistent way whether in a bank, PSP or e-money provider). Where supervisory authorities combine prudential and AML responsibilities they may need to ensure that sufficient supervisory focus and resources are dedicated to institutions carrying out higher-risk business from an AML perspective even where they might not otherwise be prudentially significant. It is also important that the ability of all financial institutions to effectively manage AML risk is assessed, proportionately to the risk, when they initially seek authorisation.

It will also be important to ensure that the AML/CFT 'perimeter' is kept under review as business models and technologies evolve.

## Ensuring a continued firm and supervisory focus during the pandemic

A final consideration concerns exposure to AML risk in times of crisis, such as the emergency we are experiencing, in which companies and the most fragile people are exposed to greater risk. Several institutions[4] in charge of fighting crime have already pointed out how, taking advantage of the economic-health crisis and the increased liquidity needs of companies and families, organised crime has intensified crimes related to *usury*, *extortion* and *fraud*, by introducing large amounts of money of illicit origin into the legal circuit. In other words, in times of crisis like the present, the risk of altering the free market and compromising the socio-economic system is enormously increased. No European country is immune to this risk given that criminal associations and crimes relating to AML/FT affect all territories and are often also related to the use of virtual currency. Particular attention should therefore be paid to the interrelationships, already verified by Criminalpol in Italy and also observed elsewhere, between the NPL market (whose management has enormous impacts on the real

[4] REFERENCES:

*Money laundering and terrorism financing trends*, in MONEYVAL jurisdiction during the COVID-19 crisis;

*How COVID-19 related crime infected Europe during 2020*, in EUROPOL report of 12/Nov/2020;

*Interpol warns of organized crime threat in COVID-19 vaccines* in EUROPOL report of 2/Dec/2020;

*Prevenzione e repressione delle attività predatorie della criminalità organizzata durante l'emergenza*

*Sanitaria,* Hearing of the UIF Italian Chief Claudio Clemente at the Parliamentary Commission of Inquiry on the phenomenon of mafia and other criminal associations – Senato della Repubblica Italiana, Roma 28/Jan/2021.

economy) and criminal appetites. For this type of operation, organised crime uses ‘dummies/front names’ and ‘front companies’, taking advantage of some ‘openings’ offered by the market and by the law. Consequently, the companies that deal with payment systems, management and credit recovery should also be addressed and subjected to banking regulations in general and AML/FT in particular, given the infiltrations already verified.

Given this challenging context, it is particularly important that firms continue to ensure appropriate focus on AML, with strong governance oversight and appropriate resources, and that supervisors use the many existing tools available to address any shortcomings pending further enhancement of the Level 1 regime. In this regard, the EBA also needs to ensure that it retains focus on fully implementing its enhanced AML powers despite the additional challenges posed by the pandemic.