

Our position

AmCham EU's position on anti-money laundering



AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2018, directly supports more than 4.8 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

Introduction

The American Chamber of Commerce to the EU (AmCham EU) has been a longstanding supporter of a robust anti-money laundering (AML) framework within the European Union. Recent cases of significant AML scandals in Europe have highlighted the need for further policy reforms to address weaknesses in regulatory requirements and policy harmonisation. According to the 2019 'True Cost of Financial Crime' report¹, 47% of firms have been victims of financial crime in the last 12 months and estimated \$1.5 trillion lost revenue in the private sector. We should also consider that less than 1% of criminal proceeds in the EU are confiscated by authorities, according to Europol.² Simply, there is more for us to do collectively to enhance the effectiveness of the current AML regime.

The true cost of financial crime extends far beyond statistics. Critical social consequences include proceeds of financial crime being used to fund terrorism; environmental crime; and human rights abuses such as slavery and child labour. With an estimated 40 million people living in modern day slavery, the human and economic costs are enormous. A 2014 report by the International Labour Organisations puts the cost at \$150 billion. In the EU, a survey into the total cost of organised crime put the cost of slavery/human trafficking at €30 billion. In concrete terms, \$1 billion in lost revenue can pay for vital services in the vital area of education in different countries across the globe.

Policy recommendations

AmCham EU would like to put forward the following recommendation to build a robust anti-money laundering (AML) framework within the European Union:

1. Develop a better understanding of the threat posed by financial crime and our performance in combatting it. EU authorities should collaborate on a joint strategic threat assessment on financial crime and focus on specific threat areas where collaborative public-private work is seen to be particularly beneficial, including:
 - a. Develop performance indicators to measure what works. Measuring the impact of efforts to reduce financial crime has proved difficult as there is insufficient data collected that both the public and private sectors can take to disrupt financial crime. This could involve mapping what information is already collected and held by the public and private sectors and leverage pre-existing work to collect performance metric from agencies.
 - b. Such a threat assessment should be at the EU level to help move focus away from national level impacts and on the threat to the collective EU financial services system. For example, mirror trading would not impact an individual country in the EU in terms of its population so may not be considered a threat domestically but it does impact the soundness and credibility of EU banking system if used as a vehicle.

¹ <https://www.refinitiv.com/en/resources/special-report/innovation-and-the-fight-against-financial-crime>

² 'Does crime still pay? Criminal Asset Recovery in the EU, Survey of statistical information 2010-24', Europol

2. Establish a European-wide public-private information-sharing working group. The TAX3 Committee of the European Parliament recently published a report on financial crime and called for the importance of developing enhanced channels for the exchange of information between the public and private sectors.³ This builds on the work of the Future of Financial Intelligence Sharing research programme which has conducted comparative research into the role of public-private financial information sharing partnerships to detect, prevent and disrupt crime. Europol's Financial Intelligence Public-Private Partnership, which promotes strategic information-sharing between banks, Financial Intelligence Units, law enforcement agencies and national regulators highlights the positive results of these arrangements. The EU should establish a working group to include a cross-sectoral private sector representatives with the aim of furthering work on the future collective ambition to improve information-sharing and use, including:
 - a. Identify where barriers to information-sharing lie across legislative, regulatory, financial and cultural inhibitors, and suggest proposals to address these barriers. Per guidance issued by the Financial Action Task Force, this group could consider the following types of information-sharing:
 - i. Information-sharing between the public and private sectors, including both regulated and un-regulated sectors;
 - ii. Information-sharing within corporate groups;
 - iii. Cross-border information-sharing
 - b. The working group should also focus on what types of information-sharing should be promoted (e.g. intelligence, typologies, best practice). It could assess whether gateways are sufficient to enable the private sector to fulfil their regulatory obligations (e.g. in fulfilling customer due diligence obligations under the Money Laundering Regulations). It could also consider potential 'de-risking' obligations that could arise from greater information-sharing.
 - c. Finally, the new working group should work in partnership with Europol to avoid any risk of competing working groups seeking the same or similar objectives.
3. Further the harmonisation of AML rules: We see variations between due diligence requirements within the EU, including a lack of harmonised guidance on the implementation of Know Your Customer (KYC) requirements under the Fourth AML Directive. There is also significant divergence between the extent and detail of guidance provided in individual EU Member States. Consistent requirements would better serve protection of the sector and a more efficient European sector would assist in more effective use of resources to align with law enforcement priorities. As proposed by the European Commission, turning the AML Directive into a Regulation could be helpful in order to go towards a harmonisation of rules, but a convergence of national level guidance is likely to have a more important impact. Examples of other potential areas for enhanced harmonisation include; definition of suspicion, predicate crimes to money laundering and law enforcement responses between EU Member States, as well as information sharing with Europol. Another priority for harmonised rules could be requirements around Suspicious Activity Reports (SARs) where a pan-European approach could reduce friction.
4. Give the private sector greater access to relevant government information where there is a legitimate interest in the organisation accessing the information in order for them to fulfil their regulatory obligations.
5. We would also support greater supervisory cooperation at the EU level, which we think may result in more consistent application of rules, reducing risk of national interest impacting supervision effectiveness and increasing efficiency of regulatory interaction and enforcement. Moves towards an AML authority could help, if their role goes beyond only the coordination of national authorities and are able to promote more uniform national-level guidance.

6. Implement an Asset Recovery Action Plan to ensure that we are making the best use of the legal powers at the EU's disposal to increase the volume of assets that are taken out of criminal hands.
7. Improve our collective capabilities by mapping the capabilities of law enforcement and major financial institutions to combat financial crime. This mapping exercise will inform future work on taking an EU-wide action to be taken against major financial crime threats. This work could establish how various capabilities inter-relate to each other including the Suspicious Activity Reporting (SAR) regime, as well as the non-financial sectors (such as legal, accountancy, property and gaming) to identify how best their skills, experience and capability can be harnessed to combat financial crime.
8. The EU might review barriers in regulation in adopting new technologies by the private sector. For instance, there are opportunities for Europe to be a leader in adopting Digital Identity. Managing the authentication of user's identity is critical when adopting biometrics and behavioural analytics. The EU could facilitate a collaborative approach across a consortium of banks, payment providers, innovation hubs, governments and regulators to create a world-leading digital identity framework. However, regulatory oversight might also be expanded to non-bank firms (e.g. fintech firms) who may then be subject to the same compliance requirements and standards as financial institutions.
9. Similarly, the arrangement of third-party firms auditing on behalf of local regulators could also be examined, as such firms may have limited incentive to apply a risk-based interpretation of the rules. Rather, such firms may instead create "quasi-rules" based on their own interpretations and not those of the regulators.
10. A stronger AML framework will come from consistency across different firms and from consistency within firms, where the firms are large. This involves creating central utilities that large firms can rely upon (e.g. client on-boarding, AML investigations, SAR filing). However, barriers to "outsourcing" to other affiliates are often created by national regulators, raising the cost and difficulty of doing so. Common approaches and guidelines for national regulators should be created so as to promote consistency and trust between regulators.
11. Over the past number of years, citizens have rightly demanded both strong data privacy rules and high levels of security following the terrorist attacks across Europe. However, greater guidance should be considered between the General Data Protection Regulation (GDPR) provisions as it relates to AML regulatory obligations which necessitate the processing of personal information. For instance, key aspects of GDPR include the requirement to obtain 'consent' (Art 7) to process data in the absence of certain exceptions and a data subject's 'right to be forgotten' (Art 17), whereby citizens have the right to request that data controllers to delete their information. While AMLD does provide for the processing of information in the 'public interest', further clarity on how this applies to the private sector and how it interacts with GDPR would be welcome. This would also help to provide legal certainty to market operators who otherwise are left with the option of potentially either breaching GDPR or breaching the AMLD - which may stop them from operating in the EU for fear of sanctions and litigation.