Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector

This paper summarises the main findings and the proposed actions related to Credit Institutions (CI) and our point of view on the key considerations and practical steps firms should take to proactively address the findings in the joint opinion and pre-empt competent authority (CA) concerns.

Executive Summary

Article 6(5) of the EU's Fourth Money Laundering Directive (2015/849) (4MLD) requires the European Supervisory Authorities (ESAs) to issue their joint opinion on the risks of money laundering and terrorist financing (ML/TF) affecting the European Union's (EU's) financial sector every two years. On 3 March 2021, the European Banking Authority (EBA) issued the 3rd Joint Opinion. The EBA issued the joint opinion as part of its new mandate to lead, coordinate and monitor the fight against ML/TF in the financial system at the EU level. The European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA) were closely involved in the process.

The survey was informed by over 50 Competent Authorities (CAs) responsible for the AML/CFT supervision of credit and financial institutions. The joint opinion sets out proposed actions addressed to CA's, which are based on the detailed analysis and findings set out in the report. The key findings and proposed actions in relation to credit institutions include:

- **The majority of CA's considered CI's as presenting a significant or very significant level of ML/TF inherent risks.**
- Several CA's indicated they were **particularly concerned about the effectiveness of firms' transaction monitoring systems, deficiencies in the customer due diligence process, effectiveness of STR reporting and the quality of customer and business-wide risk assessments**.
- CA's identified a number of current risks in the sector, in particular: **the use of RegTech and concerns related to the quality of the outcomes of CDD processes, in particular in relation to the identification of beneficial owners and in some cases, inadequate processes and controls to identify PEPs; the increasing use of remote onboarding and IT related risks**.
- CA's also indicated they were concerned by a perceived greater risk appetite of some CI's for potentially riskier products and services. Some CA's referred to, for example, partnerships between CI's and FinTech companies offering digital payments through banking channels that could bear the risk, in their view, of operating as unregulated banks. **Risks associated with virtual currencies were also mentioned by many CA's as key for the sector. Concerns were mentioned in particular as regards CI's servicing VASPs as customers**.

- CA's further indicated in some instances that they were concerned that some **firms may not be sufficiently well equipped to maintain the quality of their CDD procedures and concerns in light of an increase in the use of remote onboarding**. CA's noted that this risk was exacerbated by the current COVID-19 pandemic.

To mitigate supervisory concerns and demonstrate robust systems and controls, Plenitude recommends the following actions be proactively undertaken by credit institutions/banks:

- Ensure that AML/CFT policies, procedures and internal controls fully reflect applicable laws, regulations and guidance.
- Conduct a formal review and gap analysis of the current ML/TF business-wide risk assessment and Customer Risk Rating Methodology to ensure they fully meet regulatory requirements.
- Ensure that Customer Due Diligence controls relating to the onboarding and ongoing due diligence of customers and beneficial owners is fully aligned to the expected outcomes of applicable laws, regulations and guidance and any deficiencies are articulated and subject to remediation with appropriate governance to be monitored and addressed.
- Conduct and evidence a review of the existing monitoring and controls testing plan to ensure testing is appropriate, meets regulatory expectations and provides appropriate coverage across AML/CFT controls including any outsourced activity.
- Ensure that the controls related to ongoing monitoring of transactions are effective and calibrate and test any transaction monitoring systems on an ongoing basis so that they remain aligned to ML/TF risk assessments and regulatory requirements.
- Ensure that the controls and process in relation to Suspicious Activity Reporting are effective and that current and emerging risks are fully considered in the implementation of these controls.
- Review the AML/CTF resources within the Credit Institution to ensure that there are sufficient staff with appropriate expertise to contribute to the effectiveness and maintenance of the implemented AML/CTF controls.
- Where new technologies are implemented (FinTech/RegTech) ensure that the ML/TF risks are understood, assessed and that AML/CTF controls are still effective.
- Link your financial crime risk appetite to your AML/CTF risk assessment.

1. Credit Institutions

The following text from the Joint Opinion identifies the key risks and proposals for the credit institution and banking sector:

- *"The majority of CA's considered the CI's sector as presenting a significant or very significant level of ML/TF inherent risks. This is an increase compared with the Joint Opinion 2019. CA's considered customers, products and services as the factors that present the highest level of inherent risk of ML/TF. Geographical risks have also been highlighted by those CA's supervising CI's that have a large proportion of non-resident customers, carry out large volumes of transactions with high-risk jurisdictions or have correspondent banking activities.*

In the light of those findings, the EBA suggested that the following steps should be taken by CA's with responsibility for supervising CI's/banks:

- *"The EBA proposes that CA's monitor closely the management of ML/TF risk by CI's and, if necessary, strengthen their supervisory efforts with more intrusive supervision in those firms that present the most significant ML/TF risks."*
- *"Where CA's identify widespread compliance failures or weaknesses in respect of a particular aspect of firms' ML/TF controls, they should consider setting clear regulatory expectations and, where necessary, consider whether additional guidance above and beyond that set out in the EBA's Risk Factors Guidelines would be appropriate."*
- *"The EBA moreover encourages CA's to monitor closely the evolution of key emerging risks identified in the sector, such as those identified with FinTech (including RegTech solutions) and those associated with the current pandemic."*

2. Quality of Controls

In total, 34 CA's covering all CA's responsible for the supervision of the banking sector at EU level responded to the EBA's questionnaire in respect of data for both 2018 and 2019. Those CA's are responsible for the AML/CFT supervision of 5,872 credit institutions (CI).

- *"The majority of CA's assessed the quality and adequacy of controls put in place by firms in the sector overall as good or very good. This is an improvement compared to the Joint Opinion 2019. However, there is still a sizeable proportion of CA's that considered that the quality of some controls has remained poor. In particular, several CA's indicated they were particularly concerned about the effectiveness of firms' transaction monitoring systems, deficiencies in the customer due diligence process, effectiveness of STR reporting and the quality of the customers' and business-wide risk assessments. These concerns were also reflected in the CAs' identification of key current risks in the sector."*
- *"The main deficiencies identified in that regard are similar to those highlighted in the Joint Opinion 2019, suggesting that despite the supervision efforts provided by CA's and the improving trend in the adequacy and quality of overall controls, further improvement is still required. The EBA also notes that the sector's most well-rated controls are the adequacy of customer ID processes and policies and the awareness of ML/CFT risks."*

3. Breaches Identified

The most common breaches identified by CA's were related to customer due diligence; the effectiveness of transaction monitoring system and the subsequent filing of STRs and the management of ML/TF risks, including AML/CFT policies and procedures, internal controls and inadequate AML/CFT resources.

- *"The majority of breaches found in the sector were rated as moderate or minor in their seriousness by CA's. There was still a significant number of serious breaches that CA's found, likely to be concentrated in few banks. In comparison with the Joint Opinion 2019, there has been a considerable increase in the number of identified breaches overall, in line with increased levels of supervisory activity.*
- *"The most common follow-up by CA's consisted in orders to comply or implement measures in almost half of the cases, followed by fines and sanctions and the requests for the implementation of a remediation plan."*

4. Inherent Risk

- *"CA's identified a number of current risks in the sector, in particular: the use of RegTech and concerns related to the quality of the outcomes of CDD process, in particular in relation to the identification of beneficial owners and in some cases, inadequate processes and controls to identify PEPs; the increasing use of remote onboarding; IT risks. These concerns were reflected in the CAs' assessment of the quality of controls. Furthermore, several CA's indicated that they were concerned about the lack of understanding of TF risks in the sector; two CA's identified risks arising from tax-related crime and one CA identified risks associated with residency by investment schemes."*
- *"Risks associated with cross-border exposure also appeared to remain relevant for CA's from Member States that are known as international financial centres. Moreover, the possibility of regulatory arbitrage between Member States, due to the uneven application of EU regulation and the different approaches to AML/CFT supervision by national authorities, is of concern to several CA's."*

5. Overall Risk Profile and Emerging Risks

Half of all CA's assessed the sector as presenting a significant residual risk. This shows some improvement in comparison to the CAs' assessment of the inherent risk, especially because more firms in the sector are now rated as presenting a less significant risk profile. This suggests that CA's consider that controls in place, in some firms, were effective in mitigating inherent risks.

- *"The number of CA's that assessed the sector as presenting significant and very significant risk profiles remains significant and can be attributed to the concerns outlined above in key controls for the sector, but also to the fact that CA's may take into consideration the importance of the sector in the prevention of ML/TF."*
- *"As in the Joint Opinion 2019, risks associated with FinTech were mentioned by many CA's as key risks, both current and emerging. CA's also indicated they were concerned by a perceived greater risk appetite of some CI's for potentially riskier products and services. Some CA's referred to, for example, partnerships between CI's and FinTech companies offering digital payments through banking channels that could bear the risk, in their view, of operating as unregulated banks. Risks associated with virtual currencies were also mentioned by many CA's as key for the sector. Concerns were mentioned in particular as regards CI's servicing VASPs as customers."*

- *"CA's further indicated in some instances that they were concerned that some firms may not be sufficiently well equipped to maintain the quality of their CDD procedures and concerns in light of an increase in the use of remote onboarding. CA's noted that this risk was exacerbated by the current COVID-19 pandemic."*

6. Key Considerations for Credit Institutions/Banks

Our view is that the joint opinion clearly signals that CA's should apply a greater focus on the quality of controls in Credit Institutions as part of their supervisory approach, including the review of AML/CFT returns and inspections. Separately the breach findings provide thematic considerations with respect to internal controls, AML/CFT policies and procedures, customer and business-wide risk assessments.

Based on Plenitude's extensive work across the Credit Institution sector and interaction with regulators, the following actions should be proactively undertaken by Credit Institutions to mitigate supervisory concerns and demonstrate robust systems and controls:

- **Ensure and evidence that AML/CFT policies and procedures fully reflect applicable laws, regulations and guidance** by conducting a formal gap analysis against a comprehensive Obligations Register, such as Plenitude RegSight;

- **Conduct and evidence a formal annual review and gap analysis of the current AML/CFT risk assessment**, in particular ensure that the methodology meets regulatory requirements with respect to risk factors (Customer, Products and Services, Jurisdiction, Transactions, and Delivery channels); and consider control effectiveness and quality. As required, the approach and methodology should be enhanced and executed across all AML/CFT controls for relevant supervised entities;

- **Conduct and evidence a formal review and gap analysis of the Customer Risk Rating methodology** to ensure it meets regulatory requirements, in particular ensure the methodology reflects all risk factors i.e. Customer Characteristics, Countries/Locations, Products, Distribution Channels and Transactions/Operations; and has an appropriate weightings applied to determine the overall risk score. Supporting risk lists should also be reviewed on a regular basis to ensure they meet regulatory requirements and evolving risk indicators;

- To mitigate the risk associated with perceived vulnerabilities in relation to Customer Due Diligence (including ongoing monitoring)**, conduct and evidence a review of the existing monitoring and controls testing plan to ensure that it provides appropriate coverage across all Customers, Beneficial Owners and related AML/CFT controls**, and determine whether current testing is appropriate and meets regulatory expectations;

- For ongoing monitoring of transactions, **ensure that the controls related to ongoing monitoring of transactions are effective by amongst other things: including mechanisms to identify and implement relevant risk typologies into the ongoing monitoring of transaction, using sources such as the latest EBA Guidelines on ML and TF risk factors** and calibrate and test any transaction monitoring systems on an ongoing basis so that they remains aligned to AML/CFT risk assessments and regulatory requirements;

- To mitigate the risk of the increased use of FinTech and RegTech solutions, Credit Institution**s must seamlessly align and integrate all associated business processes, data systems, and technical architectures. There should be a documented methodology (where appropriate) to ensure Credit Institutions can evidence they understand the configuration and operation of the solution,** with regular reviews to ensure alignment with evolving regulatory requirements;

- For STR reporting, consider the requirement to file a report with the domestic FIU in relation to funds that are related to the proceeds from criminal activity or terrorism. **Putting in place a STR training regime helps to raise awareness for staff reporting suspicion and ensures Credit Institutions have the ability, competence and resources to identify and report suspicious activity promptly;**

- **Review the current Management Information reporting suite in terms of existing Key Performance Indicators (KPI's) and Key Risk Indicators (KRIs).** Candidate metrics relating to quality of controls include: QC pass rates for CDD and EDD, Transaction Monitoring (TM) alert volumes and ageing, QC pass rates for TM, STR filings, including 1st Line of defence escalations to AML/CTF teams responsible for STR filing. These should also

be considered for Risk Appetite metrics and be presented on a regular basis to appropriate governance forums and senior management, and;

- **Consider broader training and awareness activity with 1st and 2nd Line staff across all financial crime controls to raise awareness of ML/TF risks** using specific examples, being aware of current trends and typologies, reinforce roles and responsibilities across the Three Lines of Defence to drive the required 'culture of compliance' and more effective risk management.

AUTHORS

Daniel Keay
Senior Manager
E-mail: daniel.keay@plenitudeconsulting.com
Tel: +44 (0)203 102 9525

Joby Carpenter
Senior Manager
E-mail: joby.carpenter@plenitudeconsulting.com
Tel: +44 (0)203 102 9525
Mobile: +44 (0)7813 603 555

ABOUT PLENITUDE

Plenitude are Financial Crime, Risk and Compliance specialists, offering advisory, transformation services and innovative cloud-based RegTech subscription products. We help our clients meet their regulatory obligations and reduce their financial crime risk exposure by providing deep subject matter expertise, advisory and transformation services. Our RegTech subscription products which are used by leading financial institutions, offer clients enhanced insight into the vast array of FCC laws, regulations, guidance and risk indicators globally.

Plenitude has extensive experience of assisting banks and other financial institutions with assessing and improving their financial crime controls and have a proven suite of assets and deliverables developed specifically for the banking industry that can be rapidly deployed and customised for client's needs. This includes a multi jurisdiction FCC Obligations Register (RegSight), benchmark Policies and Procedures, Customer Risk Rating methodologies, Financial Crime Risk Assessments and Monitoring and Controls Testing Plans covering all AML/C controls, which fully reflect the requirements of the 4th/5th Money Laundering Directives and ESA Risk Factor Guidelines.
Our consultants come from a variety of backgrounds and disciplines across consulting, in-house financial crime compliance, regulators, government and law enforcement. As experts in financial crime compliance, we fully understand the financial crime compliance challenge, and have the expertise and skills to design and implement effective programmes or initiatives.

To find out more go to: www.plenitudeconsulting.com