Unsigned copy of a Dear CEO letter sent to Retail Banks (only) on 22 May 2021.

FINANCIAL CONDUCT AUTHORITY

12 Endeavour Square
London
E20 1JN

Tel: +44 (0)20 7066 1000
Fax: +44 (0)20 7066 1099
www.fca.org.uk

Email:RetailBankingPortfolioCommunications@fca.org.uk

21 May 2021

May 2025 update:
This letter is historical. See our supervisory correspondence page for more information and current views.

Dear Chief Executive

Action needed in response to common control failings identified in anti-money laundering frameworks

I write to share with you the common themes coming out of our recent assessments of retail banks' financial crime systems and controls.

Although we have observed examples of effective control frameworks and good practice, we are disappointed to continue to identify, across some firms, several common weaknesses in key areas of firms' financial crime systems and control frameworks. These areas include:

- Governance and Oversight
- Risk Assessments
- Due Diligence
- Transaction Monitoring
- Suspicious Activity Reporting

In several cases these are persistent failings that have resulted in regulatory intervention such as:

- requiring firms to appoint a skilled person to carry out a detailed review
- business restrictions
- enforcement action

The issues summarised in this letter reflect the key areas where some firms have fallen short of the requirements set out in **SYSC 6.3**, the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 (the MLRs) **as amended** by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019, and the provisions of the **Joint guidance on money laundering and terrorist financing**. We have detailed the specific issues in an Annex below.

The consequences of poor financial crime controls in a high-risk sector such as retail banking[1] are significant. It can lead to criminals abusing the financial system to launder the proceeds of crime, supporting further criminal activity and damaging the integrity of the UK financial market.

The Senior Managers and Certification Regime (SMCR) places a responsibility on **all** senior management to counter the risk that their firm might be used to further financial crime. Particular responsibility lies with those SMCR roles holding responsibility for financial crime, including Senior Manager Function (SMF) 17 (Money Laundering Reporting Officer) and Prescribed Responsibility D (Financial Crime). **In the supervisory work we conduct, we will continue to consider carefully whether the relevant SMF holders have carried out their responsibilities appropriately.**

Action you need to take

You do not need to contact us to respond to this letter. However, you and your senior management should carefully consider its contents and take the necessary steps to gain assurance that your firm's financial crime systems and controls are commensurate with the risk profile of your firm and meet the requirements of the MLRs.

We expect you to complete a gap analysis against each of the common weaknesses we have outlined **by 17th September 2021**. You should take prompt and reasonable steps to close any gaps identified.

We expect the senior manager holding the financial crime function to have sufficient seniority to be able to carry it out effectively and to ensure that the gap analysis is promptly completed and its findings shared internally and acted upon as appropriate.

In future engagement with your firm we are likely to ask you to demonstrate the steps you have taken.

Where we assess firms' actions in response to this letter to be inadequate, we will consider appropriate regulatory intervention to manage the financial crime risk posed.

If you have any questions please contact the FCA Supervision Hub on 0300 500 0597, or your normal supervisory contact where applicable.

Yours faithfully

David Geale
Director
Retail Banking and Payments Supervision

[1] The **National Risk Assessment for 2020** published by HMT assessed that retail banking services continue to be at high risk of being abused for money laundering.

ANNEX – COMMON CONTROL FAILINGS

Assessments conducted in recent years have comprised onsite firm visits, desk-based assessments and other targeted supervisory interventions. We set out below some weaknesses commonly identified during our firm-specific assessments. This follows feedback from the sector that we should share our findings more widely.

These weaknesses are not exhaustive, but they should provide a basis for firms to review key controls and assess whether they meet our expectations, alongside other relevant guidance such as the **Joint guidance** and the FCA's **Financial Crime Guide** which contains further examples of good and poor practice. (See also pp8-9 of our **retail banking portfolio strategy letter**.)

1. Governance and Oversight

Three lines of defence (3LOD)
Firms often blur responsibilities between the first line business roles and second line compliance roles. We have identified circumstances where compliance departments undertake first line activities, for example completing all due diligence checks or all aspects of customer risk assessment. The implications of this are that first line employees often do not own or fully understand the financial crime risk faced by the firm, impacting their ability to identify and tackle potentially suspicious activity. It also restricts the ability of compliance personnel to independently monitor and test the control framework, which can lead to gaps in the understanding of risk exposure.

In our experience, firms where those in business roles fully understand the relevant risks and know that part of their role and responsibilities is to help mitigate those risks, are significantly better at mitigating risks than their peers.

Ownership of key controls
The key controls of UK regulated branches or subsidiaries of overseas firms are often determined and run by the Head Office/Group functions. Whilst this is an acceptable practice when done well, we have found that firms are often reliant on ready-made controls, frameworks, and products. For example, using centralised sanctions screening or transaction monitoring capabilities and alert handling.

In these circumstances, senior management of the UK branch or subsidiary are often unable to demonstrate the assurance work undertaken regarding the effectiveness of those processes, or to evidence an adequate assessment of whether they fit with the UK entity's business model and risk exposure or UK laws and regulatory requirements. For example, in one firm we were informed that the UK branch had no oversight of the transactional data feed into its transaction monitoring system and lacked management information to verify that the transaction data input at Group level was complete, accurate or segmented appropriately.

Similar issues arise where firms outsource their controls to third parties (**SYSC 13.9 (Outsourcing)**).

We have seen good practice in firms which appreciate that 'one size' does not 'fit all' and ensure any systems or controls which are not bespoke are reviewed and tailored to the financial crime risks within their firm, branch or subsidiary.

Senior Management sign-off
Sign-off by senior management in certain high-risk scenarios is mandated in the MLRs. However, firms did not always evidence this level of governance. Where higher risk factors are identified,

or where approval of senior management is mandated, good practice involves firms having a governance committee responsible for key decision making on matters such as material financial crime related escalations and customer sign-off at onboarding and at periodic review. Where lower risk is determined and senior management sign-off is not mandated, we would expect to see evidence of the first line of defence's assessment and rationale for acceptance at on-boarding and at periodic review.

We have previously taken enforcement action where firms' governance arrangements were not adequately designed or effective. For example, our action has highlighted the importance of branches of overseas banks and their senior management having sufficient understanding of their UK regulatory responsibilities. We also highlighted that these firms should ensure that their UK obligations are met with appropriate resources and an effective 3LOD model; thereby enabling sufficient oversight and ownership of financial crime risk.

2. Business-wide risk assessment (BWRA)

Generally, the quality of the BWRAs we have reviewed is poor. In some instances, there is insufficient detail on the financial crime risks to which the business is exposed. In other instances, firms have considered and documented the inherent risks but have not adequately evidenced their assessment of the strength of the mitigating controls or recorded their rationale to support conclusions drawn on the level of residual risk to which the firm is exposed.

For UK branches and/or subsidiaries of overseas firms, we have seen BWRAs completed at the Group entity level which do not cover specific risks present in the UK, and which require a separate risk assessment.

Where used correctly, the BWRA is a powerful tool to help firms understand their risk exposure, set risk appetite, and inform their mitigating controls including the customer risk assessment and levels and types of customer due diligence. Additional information on completing an effective BWRA is available from a number of sources.

3. Customer risk assessment (CRA)

A common issue identified through our supervisory work is that CRAs are often too generic to cover different types of risk exposure which are relevant to different types of relationships. For example, we don't always see firms differentiate between money laundering and terrorist financing risks, or the differing risks presented by a correspondent banking relationship as compared to a customer undertaking trade finance activity.

We also see instances where there are significant discrepancies in how the rationale for specific risk ratings are arrived at and recorded by firms. There is often a lack of documentation recording the key risks and the methodology in place to assess the aggregate inherent risk profile of individual customers.

Finally, while firms tend to focus on the AML and sanctions risks posed by their customers, the assessment of other risks, for example tax evasion or bribery and corruption, is often overlooked.

4. Customer due diligence (CDD) and Enhanced due diligence (EDD)

We often identify instances where CDD measures are not adequately performed or recorded. This includes seeking information on the purpose and intended nature of a customer relationship (where appropriate) and assessments of that information. Where expected activity has been recorded, firms do not always demonstrate that they have assessed whether actual account

activity is in line with expectations or that they have undertaken appropriate investigations with the customer when it is not in line with expectations.

Some firms' approach to EDD is weak and does not always mitigate the risks posed by the customer. In some instances, we found that firms have identified a Politically Exposed Person (PEP) relationship but do not evidence an adequate assessment of source of wealth (SOW) and source of funds (SOF). In addition, firms do not always assess the level of risks posed by a PEP and tailor the extent of their due diligence, in line with Regulation 35(3) of the MLRs. We have produced **guidance (FG17/6)** to help you establish such a risk-based approach.

We also found that firms confuse the purpose of obtaining SOW and SOF information, often requesting, obtaining and verifying the same documents to satisfy these two distinct requirements. This can lead to circumstances where the origin and legitimacy of a customer's wealth is not clearly understood or verified and/or the origin of funds accepted into an account at onboarding or throughout the relationship is unknown.

In other high-risk scenarios (where SOW and SOF is not mandated by legislation but the origins of a customer's monies are a key risk to the firm) we often find little evidence of risk-based measures taken to establish the customer's SOW and SOF.

For example, we identified a case of crystallised money laundering risk where failure to conduct adequate EDD led to the firm being used as a conduit to launder the proceeds of an overseas fraud. This places the firm at risk of substantial financial loss and creates potential harm to UK market integrity, particularly where firms act as a gateway to the UK financial system.

Firms must ensure that they apply EDD measures in all high-risk situations and can clearly evidence what work has been undertaken.

5. Transaction monitoring

For branches and subsidiaries of overseas firms, we often see group-led transaction monitoring solutions which have not been calibrated appropriately for the business activities and underlying customer base of the UK regulated entity. In these circumstances firms must test whether the system is fit for purpose for the UK entity and where it is not, either tailor the system appropriately, or implement additional risk-based transaction monitoring measures.

More broadly, we also find some firms' transaction monitoring systems are based on arbitrary thresholds, often using 'off-the-shelf' calibration provided by the vendor without due consideration of its applicability to the business activities, products or customers of the firm. We often find that firms have difficulty in demonstrating how the thresholds would relate to the levels of expected activity of specific customers or customer cohorts.

We also find a lack of understanding of the technical set up of the transaction monitoring systems from those individuals that have responsibility for its operation and effectiveness. Some firms fail to undertake regular appropriate assessments of the data feeds and data integrity of the systems. In some circumstances, this can lead to transactional activity from whole business lines, products or customers being excluded from the monitoring systems, in error.

Finally, we frequently find that the rationales supporting the discounting of transaction monitoring alerts require strengthening. Discounting rationales often fail to demonstrate the level of investigation undertaken or record a sufficient explanation as to why activity is no longer considered unusual when scrutinised against the customer's expected activity.

We identified instances where firms failed to assess alerted transactional activity against the established customer profile to validate the source of funds for high-value transactions. In one example we saw, a firm failed to do this despite adverse media allegations that funds had been obtained through illicit means, and that failure placed the firm at significant risk of facilitating money laundering.

6. Suspicious Activity Reports (SARS)

We often find instances where the process by which firms' employees can raise internal SARs to the nominated officer is either unclear, not well documented or not fully understood by staff. In one example, a customer may have been alerted to money laundering concerns due to investigators not being appropriately trained in how to investigate potential suspicious activity.

An additional concern is that often firms are unable to adequately demonstrate to us their investigation, decision-making processes and rationale for either reporting or not reporting SARs to the National Crime Agency.