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

5 March 2024

Email: firmqueries@fca.org.uk

Dear Chief Executive Officer,

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

The fight against financial crime is a significant focus for both the Financial Conduct Authority (FCA) and the UK. It is important that firms have appropriate policies, controls and procedures in place to reduce and prevent money laundering, terrorist financing and proliferation financing (hereafter for the purpose of this letter referred to as "Financial Crime"). The FCA supervises firms to help ensure they comply with the relevant legal and regulatory requirements, which includes testing of their policies, controls and procedures.

The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 (the MLRs) define financial institutions with a variety of different business models that provide services in the UK as Annex 1 financial institutions (Annex 1 firms). A list of these services can be found here. For the avoidance of doubt, Annex 1 firms are not authorised persons pursuant to the Financial Services and Markets Act 2000, nor are they money service businesses. Your firm is a registered Annex 1 firm as it provides one or more of these services and is supervised by us for compliance with the MLRs.

As part of our supervision work, we undertake assessments of Annex 1 firms' Financial Crime policies, controls and procedures. We use a data-led approach to identify the firms that are selected for review. The firms we assess are informed of our findings and supervisory action is taken with those firms based on those findings. We have enhanced the monitoring of Annex 1 firms, and we are increasing our proactive work in this area.

To help support improvements across Annex 1 firms' Financial Crime controls, I write to share with you the common themes coming out of recent assessments and to set out our expectations.

From the firms selected for review, we observed common weaknesses in the following critical areas:

- Business Model – discrepancies between firms' registered and actual activities, and lack of Financial Crime controls to keep pace with business growth

- Risk Assessment – weaknesses in Business Wide Risk Assessments and Customer Risk Assessments

- Due Diligence, Ongoing Monitoring and Policies and Procedures – lack of detail in policies creating ambiguity around actions staff should take to comply with their obligations under the MLRs

- Governance, Management Information and Training – lack of resources for Financial Crime, inadequate Financial Crime training and absence of a clear audit trail for Financial Crime related decision-making

The issues summarised in this letter reflect the key areas where firms assessed have fallen short of the requirements set out in the MLRs. We have detailed the specific issues in Appendix A below.

The impact of poor Financial Crime controls can be 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. We have a range of tools which we may use when we identify poor Financial Crime policies, controls and procedures leading to the risk of material harm. These range from requiring third-party reviews to enforcement action that can result in outcomes such as fines and removal of Annex 1 firm registration.

Actions 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 policies, controls and procedures are commensurate with the risk profile of your firm and meet the requirement of the MLRs.

We expect you to complete a gap analysis against each of the common weaknesses we have outlined within six months of receipt of this letter. You should take prompt and reasonable steps to close any gaps identified. We expect the senior manager responsible for the gap analysis to have sufficient seniority to be able to carry it out effectively. We also expect them to make sure that the gap analysis is completed promptly, and its findings shared internally and acted upon.

In future engagements with your firm we are likely to ask you to provide us with the findings from the gap analysis, evidence of the actions you have taken to address the gaps identified, and the progress of any remedial work and testing to show that the policies, controls and procedures are effective and working as intended.

Where we assess a firm's 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 visit the Contact Us page of the FCA Supervision Hub for ways to get in touch.

Yours faithfully,

APPENDIX A - COMMON CONTROL FAILINGS

Recent assessments have included onsite firm visits and desk-based assessments. We set out below some weaknesses commonly identified during our assessments of Annex 1 firms.

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 Money Laundering Steering Group (JMLSG) guidance and the FCA's Financial Crime Guide which contains examples of good and poor practice.

1. Business Model

Discrepancies between firms' registered and actual activities

There have been discrepancies between the activities that firms have told us they would undertake when they registered with the FCA, and the activities firms have told us they undertake when asked during the assessment.

When you make an application to register as an Annex 1 firm with the FCA, we ask for the specific activities undertaken by a firm to meet the classification of an Annex 1 firm. It is your responsibility to make sure the details provided on the application are correct.

It is also your responsibility to notify us of a relevant change to your business details, or a correction of an inaccuracy, within 30 days beginning with the date of the change, or the discovery of the inaccuracy. For example, if firms no longer carry out any of the activities they previously informed the FCA they were conducting, if your core details - such as business address - change, or if you begin to offer another service(s) that falls within the list of Annex 1 activities. You must inform the FCA by submitting the notification to amend firms details for an Annex 1 financial institution form. In addition, you must inform us of any MLR Individual changes by submitting this form.

Lack of Financial Crime controls to keep pace with business growth

Most firms have an ambition to grow, but this should not come at the cost of Financial Crime controls. In our review we have seen instances where firms have grown significantly in a relatively short period, however their Financial Crime policies, controls and procedures have not kept pace with the size and complexity of the business, resulting in an inadequate Financial Crime framework.

Some firms we assessed also failed to adequately resource their Financial Crime teams as their business grew. We observed a lack of Financial Crime training for employees, and a lack of engagement at senior management level in this area. In one example, the officer responsible for the firm's compliance with the MLRs was not involved in any operational activities to oversee compliance, including reviews of high-risk accounts and sign-off.

Senior managers must consider the size and nature of firms' businesses when assessing and implementing policies, controls and procedures, and a firm should ensure their Financial Crime policies, controls and procedures remain appropriate for the size of their business.

2. Risk Assessment

Business Wide Risk Assessments (BWRA)

In some instances, we found that the BWRA was completely absent despite the requirement under the MLRs to identify and assess the money laundering (ML), terrorist financing (TF) and proliferation financing (PF) risks to which the business is subject. In other instances, we found firms had failed to document in writing all the steps they had undertaken to identify and assess these risks. The lack of a BWRA prevents firms from having a clear view of the ML, TF and PF risks they are exposed to and being able to design and implement appropriate controls to mitigate those risks.

In other instances, where a BWRA was present, we found the quality to be poor. The BWRA often lacked sufficient detail, and the methodology used by the firms was often unclear. In one example, a firm was able to identify the high-level risks that it was exposed to, such as fraud risk. However, the BWRA failed to clearly articulate the relevant mitigation measures in place to counteract this risk. These instances of insufficiently detailed BWRAs resulted in a failure to identify the inherent ML, TF and PF risks faced by a firm, determine the effectiveness of the controls in place to mitigate these risks, or to establish the residual risks a firm remained exposed to.

Firms should review and update their BWRAs to ensure compliance with the MLRs and to reduce the risk that the firm is used to facilitate Financial Crime. We expect firms' BWRAs to identify and assess the ML, TF and PF risks to which it is exposed to as a result of, for example, its customers, the countries or geographic areas in which it operates, its products or services, transactions, and its delivery channels. Firms can then design appropriate mitigating policies, controls and procedures to target their Financial Crime resources on the areas with the greatest risk.

Customer Risk Assessments (CRA)

CRAs allow firms to assess individual customer risk. By using tailored CRAs, firms can then categorise their customers based on the identified risk level and apply the appropriate customer due diligence (CDD) measures.

However, some firms assigned a level of risk to a group of customers and failed to tailor their CRAs towards individual customer characteristics. These firms therefore failed to assess the potential Financial Crime risk each customer posed to the firm and did not effectively assess the subsequent level of customer due diligence required to mitigate that risk. In one example, the CRA did not take into consideration the nature of the business relationship, or the jurisdiction the customer operates in.

Firms should review their CRAs to ensure compliance with the MLRs. We expect CRAs to reflect the risks identified in firms' BWRAs. CRAs should enable firms to take a holistic view of the risk associated with the relationship, considering all relevant risk factors, and enable firms to apply the appropriate level of due diligence to manage the risks identified.

3. Due Diligence, Ongoing Monitoring, and Policies and Procedures

The CDD policies and procedures of the firms we have assessed generally lacked sufficient detail. We found some instances where policies were vague on the actions staff should take to comply with the firms' ML, TF and PF obligations. In other instances, policies were not kept up to date, putting the firm at risk of non-compliance with the current required legal and regulatory standards. We found that inadequate CDD policies and procedures resulted in ambiguity over the level of CDD measures that should be applied to different risk ratings. This issue was particularly evident at the onboarding stage.

Some firms' CDD policies and procedures also lacked detail about when and how simplified CDD and enhanced due diligence (EDD) measures should be applied. For example, policies and procedures did not clearly document what should be done for customers established in or transacting with a party established in a high risk third country as defined by Regulation 33(3)(a) of the MLRs. In this situation, firms should ensure EDD and enhanced ongoing monitoring measures are applied and that this is clearly documented within their policies and procedures.

Similar issues were present in firms' ongoing monitoring policies and procedures, where a lack of clarity created ambiguity about whether ongoing monitoring was taking place, and how this was being achieved. We also observed a lack of appropriately documented policies and

procedures for investigating and recording Suspicious Activity Reports (SARs).

CDD and ongoing monitoring processes are crucial in preventing firms from being used as conduits to launder the proceeds of crime. By applying effective CDD and ongoing monitoring controls, firms mitigate the risk of financial loss and contribute towards maintaining the integrity of the UK financial markets.

Firms should review their policies and procedures to ensure clear guidance is provided to staff to ensure compliance with the MLRs. CDD and ongoing monitoring policies should be appropriately applied to individual customers depending on the level and nature of risk they pose. Firms should clarify when simplified CDD or EDD measures should be applied, and outline when and how a customer's source of funds and source of wealth will be effectively captured. It is also important for firms to ensure CDD and ongoing monitoring documents are kept up to date.

4. Governance, Management Information and Training

Lack of resources for Financial Crime

We found that some firms' Financial Crime teams were not adequately resourced to carry out their functions effectively, and there was a lack of appropriate oversight from senior management.

We expect senior management to take clear responsibility for managing Financial Crime risks, which should be treated in the same manner as other risks faced by the business.

Inadequate training

During our firm assessments we identified that some firms' Financial Crime training has not been given the importance that it demands. We observed instances where employees were not provided with role-specific training, and some of the training failed to cover crucial topics, such as SAR reporting guidance. The lack of effectiveness of the training provided to staff has also been evident during interviews with employees, who, in some instances, have demonstrated low levels of Financial Crime awareness.

Firms must take appropriate measures to ensure that its employees are made aware of the law relating to ML, TF and PF. Employees must be given regular training in how to recognise and deal with transactions and other situations which may be related to money laundering or terrorist financing. Firms must maintain a record in writing of the measures taken and the training given to its employees.

Absence of a clear audit trail for Financial Crime related decision-making

We identified weaknesses in firms' governance and management information in relation to record keeping for Financial Crime decisions, including a failure by some firms to document how they have responded to risks, or the rationale for the decisions taken by firms.

A common issue is that firms do not have Financial Crime as a standing agenda item at senior management meetings, and it is instead considered on an exception basis. This results in the absence of a clear audit trail to support firms in their decision-making process where Financial Crime concerns are discussed.

We expect senior management to be actively engaged in firms' approaches to addressing their Financial Crime risks. Where appropriate, with regard to the size and nature of its business, firms must appoint one individual who is a member of the board of directors (or if there is no board, of its equivalent management body) or of its senior management as the person responsible for firms' compliance with the MLRs.

Firms' efforts to combat Financial Crime should also be subject to challenge. Where appropriate in regard to the size and nature of its business, firms must also establish an independent audit function with the responsibility to examine and evaluate the adequacy and effectiveness of the policies, controls and procedures adopted by firms.

The independent audit function is expected to make sure firms' adopted policies, controls and procedures comply with the requirements of the MLRs; to make recommendations in relation to those policies, controls and procedures; and to monitor firms' compliance with those recommendations.

Where firms' size and nature of their business means they are not required to do the above, firms should adopt other appropriate measures that monitor the effectiveness of firms' policies, controls and procedures and compliance with the MLRs. Without clear governance and management information in place, firms may not have sufficient information to oversee and comply with their money laundering requirements.