AFB COMPLIANCE PLATFORM

FINANCIAL CRIME EXPERT PANEL 30 NOVEMBER 2020

NOTE OF QUESTIONS & ANSWERS

UK'S MONEY LAUNDERING AND TERRORIST FINANCING (AMENDMENT) REGULATIONS 2019

The views provided in this paper are the authors' own on behalf of Promontory and do not constitute legal opinion.

1. **What should transaction monitoring look like in a small, wholesale foreign banking branch operation? Is an automated system required? Do individual transactions need to be monitored, and what would this involve?**

There is currently no regulatory requirement for a firm to have an automated system in place for monitoring transactions. In the FCA's 2007 thematic review on Automated Anti-Money Laundering (AML) Transaction Monitoring Systems[1], the Financial Conduct Authority (FCA) notes that there may be smaller firms that are able to "monitor credibly and effectively using manual procedures". However, as a statement of good practice, the FCA also notes that depending on the nature and size of the business, automated controls may be an "important component"[2] to an effective monitoring framework. Firms can look to this report for further examples of good practice.

As with any transaction monitoring control framework, manual or automated, firms should conduct an assessment of the transactional risks posed by its customer base and product offering and build out a risk-based approach with a selection of thresholds and rules to manage these risks. Firms should ensure they have adequate resource to assess transactions effectively, and within SLA's, and should consider each transactional alert against customer profile and expected activity, with a holistic view of the customer.

2. **Is it acceptable for low-risk clients to be subject to customer due diligence (CDD) review on the occurrence of a "trigger event" - meaning no hard-wired periodic review?**

The regulations require firms to conduct ongoing monitoring of business relationships[3], which includes scrutiny of transactions to ensure they are in line with what the firm knows about the customer. Under

[1] FCA Handbook, FCTR 4.1.2 [G]. https://www.handbook.fca.org.uk/handbook/FCTR/4/1.html
[2] FCA Handbook, FCTR 4.3.2 [G].
[3] The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (MLR 2019), Regulation 28 (11) (a). https://www.legislation.gov.uk/uksi/2019/1511/contents/made

these requirements, CDD documents (including information around the purpose and intended nature of the relationship) must be kept up to date[4][5].

However, the guidance does not explicitly define how this should be executed, and therefore some firms choose to take a risk-based approach to periodic reviews by not including a review cycle for their lowest risk customers. With this, there is a significant increase in the reliance on ongoing monitoring controls such as transaction monitoring and trigger event reviews, and therefore where firms do choose this approach, they must ensure that these alternative controls provide comprehensive coverage and adequately manage the risks.

Where periodic reviews are not performed there is a risk that some customers may not be reviewed for a significant period of time. Trigger event controls may need to be enhanced to ensure that customers exempt from the review cycle are still being flagged for any changes or unusual behaviours. Firms may choose to include an automated trigger when a customer has not been reviewed for a set period, for example 5 years, as an alternative to ensure they are still being looked at during the course of the relationship. This may also be used as an opportunity to consider whether existing trigger controls can be enhanced, or rules implemented where changes or risk may not have been flagged previously.

Firms should consider how they can still meet CDD requirements and assess transactions where data is historic. There may be additional controls that help keep customer data current, for example:

- using external verification sources that use public data to verify customer information;
- enhancing controls in the first line of defence through RM engagement with clients to regularly obtain updated CDD;
- working with other areas of the bank to collect, and cleanse, customer data.

Assurance checks through internal audit reviews or regular compliance monitoring may be used for sampling of low-risk customer files to determine whether CDD information is up to date and assess whether trigger event controls are appropriately flagging customers that require attention. Firms should also consider whether this approach will result in lookback or remediation exercises, as these customers may not be updated where standards and policies change, for example changes made to the customer risk assessment model.

There is a significant risk that some customers are not reviewed for an extended period of time, which may lead to deficiencies in due diligence standards and challenges in fully understanding the risk profile of those customers, requiring costly systems and control enhancements. As any decisions are being made, firms should balance the cost savings of reducing the periodic review burden against the cost of system upgrades and enhancements and potential control failures resulting in the facilitation of financial crime.

3. Would you say that the only instance where firms are not required to obtain beneficial ownership details is when the company is listed on what is considered to be an equivalent exchange?

There may be instances where beneficial ownership information is not accessible, or low risk situations where simplified due diligence (SDD) can be applied[6] and therefore it is not required. For example, where the customer is a public administration or a publicly owned enterprise[7]; certain funds or pooled accounts[8]; or where the beneficial owner is a minor with a trust or ISA account[9].

---

[4] MLR 2019, Regulation 28 (11) (c)

[5] MLR 2019, Regulation 28 (13)

[6] Regulation 37, MLR 2017.

[7] Joint Money Laundering Steering Group Guidance (JMLSG) Part 1, 5.3.192, July 2020. https://secureservercdn.net/160.153.138.163/a3a.8f7.myftpupload.com/wp-content/uploads/2020/07/JMLSG-Guidance_Part-I_-July-2020.pdf

[8] JMLSG Guidance Part 1, 5.3.142, July 2020.

[9] JMLSG Guidance Part 1, 5.4.5-5.4.7, July 2020.

The requirement for when firms must identify beneficial ownership has not changed under MLR 2019; it has however been extended with additional reporting and record keeping requirements where discrepancies and challenges are encountered.

There may be instances where ownership structures are very complex, and it may be challenging to obtain beneficial ownership and control information. Firms should consider all challenges encountered in obtaining this due diligence and assess whether these difficulties may be an indicator of suspicion for financial crime when looking to maintain or open a customer account and raise a suspicious activity report (SAR) as appropriate.

4. If you identify suspicious activity by a client in a high-risk sector, file a SAR, but do not exit the business relationship, what additional type of enhanced due diligence would the regulator expect you to perform?

Firms may take a holistic look at existing controls for higher risk customers when considering options for enhanced monitoring. The JMLSG refers to enhanced monitoring of a business relationship as "increasing the number and timing of controls applied and selecting patterns of transactions that need further examination"[10]. In practice, this may involve:

- placing the customer on a 6-monthly review cycle;
- increasing transaction monitoring by reducing thresholds, or putting a flag on the account so all transactions alert for review;
- conducting enhanced due diligence, where this has not already been obtained;
- conducting more detailed EDD by taking more intrusive measures to corroborate information from independent third parties; and
- increasing sign-off requirements to include more than one senior manager or committee approval.

In addition to enhanced monitoring, some firms choose to apply a control where, for example, if 3 suspicious activity reports (SARs) are raised on the same customer, this customer will automatically be considered for exit through relevant governance channels.

As part of the FSA's 2011 thematic review of Bank's Management of High Money Laundering Risk Situations[11], the FSA published examples of good and bad practice. Good practice includes transaction monitoring against expected account activity; lower alert thresholds; regular reviews of relationships with proactive follow up for gaps in CDD; knowledge amongst staff of the highest risk customers; and increased senior involvement for resolving alerts, among other examples.

It is ultimately a business decision for a firm to continue an existing customer relationship where there are live concerns of suspicious activity. All decisions to retain or exit customers should be recorded on file so that the rationale is clear, and firms should ensure this is considered as part of regular reviews. Firms should also consider whether they need to make any Defence Against Money Laundering (DAML) SARs to the National Crime Agency to obtain consent to release client funds when exiting a relationship, in order to avoid committing a money laundering offence under the Proceeds of Crime Act (2002).

5. Are there any concerns with Compliance staff multitasking and therefore only spending a fraction of time on financial crime matters?

In our experience, regulators expect firms to dedicate sufficient resources to the management of financial crime risks across all lines of defence, and that those resources are skilled and capable to execute required activities. The FCA has Threshold Conditions in place that require firms to meet minimum standards, one of which requires firms to have adequate resources in place proportionate to the firms'

[10] JMLSG Guidance, Part 1, 4.62 (b), July 2020.

[11] FCA Handbook, FCTR 12.3.5

size and business model[12], which includes the framework for financial crime. The threshold conditions are enforceable and may result in the loss of permissions where breaches are identified.

Where resource constraints are identified, these should be raised with senior management for discussion at Board and Ex-Co levels, and all decisions recorded through committee minutes. Firms should carefully consider the cost and reputational implications for non-compliance with their regulatory obligations, and the possible impact of enforcement, against any cost savings made from inadequate resourcing.

6. Where can I find more information about EID&V?

Sources for further information and guidance on Electronic identification and Verification include:

- Financial Action Task Force (FATF) Guidance on Digital Identity[13];
- JMLSG, Part 1, Section 5.3.33 and 5.3.45[14]; and
- FCA Financial Crime Guide for Firms, Section 3.2.4[15].

Third-party vendors and system providers should provide detail around the specific technologies being utilised, for example accuracy rates and potential system deficiencies that may exist e.g. challenges with the verification of certain ethnicities. Firms should have a thorough understanding of any EID&V system they may use or accept and conduct a financial crime risk assessment to get a view of risk exposures, for example fraud. Firms should also put in place adequate assurance controls to comply with the regulatory requirement that the systems are secure from fraud, and to obtain an appropriate level of assurance that customers are verified accurately[16].

7. Should a firm submit a SAR if the firm has issues in identifying the beneficial owners? Should this be considered suspicious?

There is no defined rule around whether difficulties in obtaining beneficial ownership and control information should be considered suspicious however the JMLSG provides guidance around when issues arising out of the customer identification process may be cause for concern[17], which includes customer reluctance to provide information, or challenges with identifying and understanding the legal structure. The JMLSG also states that it is the obligation of firms to take reasonable measures to be satisfied they know the beneficial ownership structure of customers[18]. Firms should take a view of the customer and make a judgement based on all information available, raising a SAR where suspicion exists. All decisions should be recorded on file and considered as part of any future ongoing monitoring activities e.g. transaction monitoring, periodic reviews, SAR assessments.

QUERIES AND FOLLOW-UP

If you would like any further information about any of these matters, please feel free to contact the following individuals from the team at Promontory below:

Priya Giuliani, Managing Director

pgiuliani@promontory.com

+44 (0)7384 832770

[12] FCA Handbook, COND 2.4.1 (A) Paragraph 2D of Schedule 6 to the Act. https://www.handbook.fca.org.uk/handbook/COND/2/4.html
[13] "Digital Identity", FATF Guidance, March 2020. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf
[14] JMLSG Guidance: Part 1, Section 5.3.33 and 5.3.45, July 2020. https://secureservercdn.net/160.153.138.163/a3a.8f7.myftpupload.com/wp-content/uploads/2020/07/JMLSG-Guidance_Part-I_-July-2020.pdf
[15] FCA Financial Crime Guide for Firms, Section 3.2.4, October 2020. https://www.handbook.fca.org.uk/handbook/FCG.pdf
[16] Regulation 5(2) MLR 2019, amending Regulation 28 MLR 2017. https://www.legislation.gov.uk/uksi/2019/1511/regulation/5/made
[17] JMLSG Guidance Part 1, 7.34, July 2020.
[18] JMLSG Guidance Part 1, 5.3.14, July 2020.

Leeanne Grassnick, Senior Principal

lgrassnick@promontory.com

+44 (0)7850761121

Hollie Rowe-Roberts, Associate

hrowe-roberts@promontory.com

+44 (0)7467 330329