Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Anti-Money Laundering Bulletin

Issue 6 / October 2020

Welcome to the latest edition of the Central Bank's Anti-Money Laundering Bulletin. This edition concerns the application of transaction monitoring. The bulletin sets out the Central Bank's findings following supervisory engagements across multiple credit and financial institutions, and also sets out the Central Bank's expectations with regard to the application of transaction monitoring controls.

Previous Central Bank bulletins and reports highlighted the importance of monitoring customer transactions to detect potentially suspicious activity. Effective transaction monitoring is not possible without an effective Customer Due Diligence ("CDD") process and, in turn, effective Suspicious Transaction Reporting ("STR") is not possible without effective Transaction Monitoring controls. This edition should be read in conjunction with previous bulletins, reports, and guidance issued by the Central Bank.

Transaction Monitoring

The importance of transaction monitoring has been highlighted in recent years following a number of high profile European cases whereby a failure to detect suspicious transactional activity enabled the international transfer of hundreds of billions of Euro which are now thought to have been suspicious in origin. The failure of a designated person to implement effective transaction monitoring controls that are commensurate to the risks inherent to that designated person's business activities and customer

Tommy Hannafin
Head of Anti-Money Laundering Division
Central Bank of Ireland

Links to useful sources of information available on the Central Bank website:

- Anti-Money Laundering and Countering the Finance of Terrorism Guidelines for the Financial Sector – September 2019
- Anti-Money Laundering Bulletin on Suspicious Transaction Reporting – November 2017
- Anti-Money Laundering and Countering the Finance of Terrorism – Correspondence with Industry
- COVID-19 – Regulated Firms FAQ

risk profile negatively impacts their ability to detect suspicious activity and to file STRs with the relevant authorities.

The requirement to monitor transactions is specified in the following provisions of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 ('The Act'):

- **Section 35 (3)** – states that a designated person "shall monitor any business relationship that it has with a customer to the extent reasonably warranted by the risk of money laundering or terrorist financing"
- **Section 36A (1) & (2)** – states that a designated person shall adopt policies and procedures to examine "the background and purpose of all complex or unusually large transactions, and all unusual patterns of transactions which have no apparent economic or lawful purpose", and that the degree and nature of the monitoring of a customer relationship shall be increased in order to determine whether such transactions are suspicious
- **Section 54 (1) & (3)** – states that a designated person will adopt internal policies, controls, and procedures to detect the commission of money laundering and terrorist financing and that they will include the monitoring of transactions and "the identification and scrutiny of complex or large transactions, unusual patterns of transactions that have no apparent economic or visible lawful purpose and any other activity that the designated person has reasonable grounds to regard as particularly likely, by its nature to be related to money laundering or terrorist financing"

The Act therefore specifies that a designated person must monitor customer transactions in order to identify transactions that may be suspicious in nature, and that the intensity of the monitoring should increase with the complexity and scale of those transactions so that the risk of ML/TF is also factored into the transaction monitoring process.

Central Bank Findings

From the inspections that were undertaken by the Anti-Money Laundering Division of the Central Bank, the following common themes were observed:

- Failure to use the business risk assessment and customer risk assessments to configure appropriate transaction monitoring controls
- Insufficient testing of transaction monitoring controls, and the configuration of automated transaction monitoring controls, by second or third lines of defence
- Failure by the Board and Senior Management to take appropriate measures to address weaknesses identified with the transaction monitoring process arising from assurance testing and reviews undertaken by Compliance and/or Internal Audit functions

Links to other sources:

- Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended
- Joint Opinion of the European Supervisory Authorities on the risks of Money Laundering and Terrorist Financing
- FATF: COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses

Joint Opinion of the European Supervisory Authorities on the risks of Money Laundering and Terrorist Financing

- *Published October 2019*

The ESAs acknowledge that the use of new technologies may offer opportunities to better fight financial crime, however, this Opinion also confirms that the increasing use of new technologies by credit and financial institutions may give rise to ML/TF risks if vulnerabilities are not understood and mitigated.

The key areas of concern relate to the quality of business-wide and individual risk assessments, transaction monitoring and the identification and reporting of suspicious transactions, as well as the adequacy of AML/CFT resources. These shortcomings are not mutually exclusive, as [a designated person's] failure to understand and assess ML/TF risks would have an impact on their ability to implement effective transaction monitoring controls and therefore would have an impact on their ability to identify and report suspicious transactions.

- Failure to document procedures for the monitoring and the investigation of potentially suspicious activity, including clear assignment of roles and responsibilities
- Inordinate time delays in reviewing and assessing unusual activity resulting in delays in reporting suspicious transactions to the relevant authorities
- No mechanism for prompt adjustment to transaction monitoring controls to reflect any new risks or potential new risks arising from the disruption caused to the financial system e.g. new threats that have become evident during the COVID-19 pandemic as detailed in FATF's "COVID-19-related Money Laundering and Terrorist Financing" paper in May
- The use of generic monitoring thresholds across varying product, service, or customer types which do not reflect the nuances of expected transaction patterns of those customer/product/service types
- The implementation of sample based approach to transaction monitoring which limits the ability to detect unusual patterns of transactions
- Placing reliance on an automated transaction monitoring solutions, that may be proprietary or provided by an affiliated or third party entity, where:
    - An assessment as to its adequacy in relation to the designated person's specific risks is not completed
    - The designated person has no input into the governance or management of the solution
    - Scenarios, rules, and thresholds not regularly reviewed and tested in light of changes to the designated person's business risk assessment
    - The designated person lacks autonomy and ability to request changes to the configurations of the transaction monitoring controls as necessary
- Failure to implement a robust AML/CFT control framework for the transaction monitoring process. Examples include:
    - Insufficient technological resources to ensure that all customers are in scope and accurate customer and transactional data is captured for the purpose of this process
    - Errors and control failures in the adjudication of alerts generated from the process
    - Generic and insufficient detail in the rationale used to disposition those alerts
    - Failure to maintain audit trails to fully reflect the review of those alerts

Revenue

Since 7 September 2020, STRs must be submitted to Revenue using Revenue's Online Service (ROS) only. To submit an STR online, the designated person must firstly be registered for ROS and have a digital certificate. You can then register for STR Reporting and request a sub user certificate for all MLROs. For further guidance on submitting STRs online, please see the Revenue Website.

Section 54 of the CJA 2010 requires a designated person to adopt policies and procedures to prevent and detect the commission of ML/TF. The Central Bank expects that all designated persons are registered with ROS.

Central Bank Expectations

In addition to the guidance set out in Section 5.8 of the Guidelines and the Joint Opinion of the European Supervisory Authorities on the risks of Money Laundering and Terrorist Financing, included in this document, designated persons should note the following:

In order for Transaction Monitoring controls to be effective, they must detect what suspicious activity looks like in the context of the designated person's business activities and also in the context of the designated person's specific customer profile(s). As such, the controls should be tailored to the designated person's business risk assessment[1], and the customer risk assessment[2].

By using the business wide risk assessment, a designated person can determine the appropriate transaction monitoring solution for that designated person's specific business activities. The Central Bank recognises that an automated transaction monitoring system will not always be possible or appropriate based on the nature, scale and complexity of the designated person's business. However, in many cases an automated transaction monitoring solution will be necessary and if a designated person determines that a manual process is adequate, the Central Bank expects that the decision is based upon a full assessment of the manual controls ability to detect suspicious transactions, including unusual patterns of transactions. The decisions should be documented and approved by senior management within the firm. In addition, the controls should be fully documented in the policies and procedures, and included in the risk assessment.

While the use of an automated transaction monitoring solution is desirable, a designated person should not place absolute reliance on any such system and employees should still be aware of the need to manually identify any transactional activity which may be suspicious.

The Central Bank expects to see connectivity between a designated person's CDD, transaction monitoring, and STR processes. A designated person should have sufficient and up to date information on file and obtained during the CDD process to determine whether transactional activity is suspicious.

The adequacy of a designated person's controls should be subject to continued and regular review. If an automated system is employed, the rules, scenarios, and thresholds must be regularly reviewed to ensure that they continue to detect identified risks and emerging risks.

There should be a mechanism for making changes to the controls to take into account altering risks and new risk indicators, for example the COVID-19 FAQs for regulated businesses published by the Central Bank noted that transaction monitoring levels may need to be recalibrated to reflect the stalled nature of the economy and changes to patterns of customer behaviour brought about by the pandemic.

Transaction Monitoring Guidance

Anti-Money Laundering and Countering the Finance of Terrorism Guidelines for the Financial Sector ("the Guidelines") *- published by the Central Bank September 2019*

Section 5.8

Firms should put in place adequate policies and procedures to identify unusual transactions or patterns of transactions. Examples may include transactions or patterns of transactions that are:

- Larger than the Firm would normally expect based on its knowledge of the customer, the business relationship or the category to which the customer belongs;
- Of an unusual or unexpected pattern compared with the customer's normal activity or the pattern of transactions associated with similar customers, products or services; or
- Very complex compared with other similar transactions associated with similar customer types, products, or services; and the Firm is not aware of an economic rationale or lawful purpose or doubts the veracity of the information it has been given.

Where Firms detect unusual transactions or patterns of transactions, they should apply EDD measures sufficient to help the Firm determine whether these transactions give rise to suspicion. Such EDD measures should at least include:

- Taking reasonable and adequate measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or

[1] Section 30A Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

[2] Section 30B Criminal Justice (Money Laundering and Terrorist Financing) Act 2010

When using an automated solution, that may be proprietary or provided by an affiliated or third party entity, a full assessment as to its suitability for the risks inherent to the designated person's specific business, including jurisdictional considerations, must be completed. The designated person should be able to effect changes to the configuration of the transaction monitoring controls as necessary, and the controls should be fully reflective of the risks identified in the designated person's business and customer risk assessments.

Conclusion

As part of the Central Bank's continued supervision in the area of AML/CFT, focus will remain on the compliance of a designated person with the sections of the Act pertaining to transaction monitoring. It should be evidenced that the expectations outlined in this bulletin, in addition to the guidance set forth in the Guidelines, are fully considered and implemented where appropriate.

finding out more about the customer's business to ascertain the likelihood of the customer making such transactions; and

- Monitoring the business relationship and subsequent transactions more frequently and with greater attention to detail. A Firm may decide to monitor individual transactions where this is commensurate to the risk it has identified.