THE TA FORUM
AML Working Group

Definition of trigger events and expected actions

Introduction

Firms must ensure they have measures in place to identify financial crime risks to their business and customers. These measures must also be proportionate to the business and implemented based on an assessment of risk.

This risk assessment should include the identification of trigger events that may pose an increased risk to Money Laundering or financial crime. Policies and procedures should include the trigger events assessed by a firm that may require a re-verification of anti-money laundering documentation (or electronic verification) or enhanced due diligence based on the event identified.

Regulations

The Money Laundering, Terrorist financing and Transfer of Funds (Information on the Payer) Regulations 2017 came into force on 26th June 2017, replacing the Money Laundering Regulations 2007 and implementing the EU 4th Money Laundering Directive.

The government consulted on the new regulations and as part of this consultation ongoing monitoring obligations were considered. The published consultation outcome included the following:

A risk-based approach and ongoing monitoring obligations (3.1)

The government requested views on what changes in circumstances should warrant obliged entities applying CDD measures to their existing customers. Stakeholders specifically mentioned the following which can be applied to the Transfer Agency industry:

- the majority thought that a change of name would require new CDD checks to avoid confusion over identity. This would become apparent at the point of a new transaction, but also if a customer informed the business, or for example if mail was returned to sender
- a change in marital status was thought to be relevant if the customer married a PEP. If it led to a name change there would be associated re-verification, but this would not necessarily link to increased risk of money laundering
- a change of address could affect risk if it involved moving to a higher risk jurisdiction. for companies, a change in the corporate structure, or significant change in beneficial ownership
- a change in vocation or promotion at work for a customer could affect their money laundering risk, for example if the customer became a PEP. However, some respondents also highlighted that information on vocation was more burdensome to request than information verifying identity and address. It may be more relevant for Source of Wealth or Source of Fund checks or, for example, for private banking
- a combination of two or more changes at the same time were more likely to trigger CDD or EDD

THE TA FORUM
AML Working Group

Potential Trigger Events (the list is not exhaustive)

- JISA trigger event - Client becoming 18
- Client taking out a new product or service
- When a certain transaction threshold is reached
- Change of Address
- Change of telephone number (especially if overseas / different country to address on file)
- Change of Name
- Adding a Power Of Attorney
- Increase in savings amount
- Top up to investment
- Redemption
- Sale followed by a quick redemption
- Death Claim
- Stock Transfer
- Returned Mail
- Change of bank details
- Change of Agent (especially if overseas)
- Change of beneficial owners
- Change of corporate structure

These events can be used to assess the documentation held. Upon identification of a trigger event the following should be considered:

An assessment of risk
Does the due diligence already performed still meet requirements?
Does it need to be refreshed?
Is enhanced due diligence required?
Has the event led to a suspicion?

Assessment of Risk

A low risk scenario may be as follows: A UK client who has previously been verified increases their savings amount by £50.00 per month. Re-verification is unlikely to be necessary.

A higher risk situation may be as follows: A UK client substantially increases their savings amount per month. This may require further due diligence to be performed, which may include a new Source of Funds and Source of Wealth declaration from the client with evidence to support the information provided in some cases. Some of our members have enhanced due diligence process in place, requiring senior leadership approval, for a request to change bank accounts to a bank located in a country different to the investor's residency i.e. third country bank account. Level of due diligence will differ, depending on the firm's determination of the country risk of new bank's location.

Ongoing monitoring

The transaction monitoring completed within a firm will most likely include reviewing transaction monitoring reports but this should also include real time monitoring by staff. A trigger event may result in a referral to compliance, a request to the client for additional information (for 3rd party providers) or a suspicious activity report. In addition to considering one-off events, monitoring should also consider the cumulative effect of multiple events occurring over a specific time period that may give rise to concern when considered collectively, but not individually.

Procedures

A firm's procedures need to include its definition of a trigger event and the action that will be taken when a trigger event occurs. This could be achieved by using checklists for staff to follow or flow diagrams. For example a client who is currently a UK resident who moves to another address in the UK with no other trigger events, would not be deemed suspicious or higher risk. Standard procedures would apply with regards to verification of the new address. Procedures will already be in place for the identification of Fraud such as verifying the new address and mailing the old and new address with confirmation of the change.

However, should a UK client move to a country deemed by the firm to be high risk, or a change of name occurs at the same time as a substantial investment, enhanced due diligence measures should be applied.

Suspicious Activity Reporting

A trigger event may identify a suspicious activity. In the event that this occurs the member of staff who has identified the suspicious trigger event must raise an internal report as per the firm's internal procedures. This report should include full details of the customer under suspicion and full details of the reason for the suspicion.

The relevant team along with the MLRO will determine whether there is knowledge, suspicion, or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering, or that terrorist property exists. If this is determined to be the case the MLRO or deputy must make a report to the National Crime Agency (NCA) as soon as is practicable. Consent must be sought from the NCA before proceeding with a suspicious transaction or entering into arrangements.

All decisions and communications regarding suspicious activity reports must be clearly documented and maintained on file. Policies and procedures should be in place to guard against the risk of 'tipping off' the customer whilst these activities take place.

Training

SYSC 6.3.7G states that a firm should ensure that the systems and controls include:

(1) appropriate training for its employees in relation to money laundering.

Training can take the form of computer based training with a test at the end to demonstrate understanding; however it is also important to provide interactive, face to face training with members of staff whose role involves the administration of customer accounts and finance functions. This should include examples of trigger events and why and how they could be an indication of a suspicious event.

Training records must be maintained and escalations made to the board if training remains outstanding for members of staff.

Summary

- **Firms must have systems and controls and policies and procedures in place to enable it to identify, assess, monitor and manage the risks that defined trigger events may identify or present.**
- **Each trigger event may have a different level of risk associated to it.**
- **Firms must train their staff to ensure they understand how to identify trigger events along with when a trigger event will result in either a refresh of due diligence information, enhanced due diligence requirements or a suspicious activity report, and the steps required to prevent 'tipping off' the customer if suspicions exist.**
- **Records regarding the decisions and approach taken must be maintained.**
- **Where there is knowledge of suspicion or reasonable grounds for knowledge or suspicion a report must be made by the MLRO or a deputy to the NCA**
- **All decisions and communications regarding suspicious activity reports must be clearly documented and maintained on file.**