Revised Implementing Procedures Part I
Section 4.5 – Ongoing Monitoring

FIAU Training Event
18/19 December 2018

Clara Borg Bonaci
Requirement under PMLFTR

Regulation 7(1)(d) sets the requirement to conduct ongoing monitoring.

Regulation 7(2) breaks down ongoing monitoring:

(a) the **scrutiny of transactions** undertaken throughout the course of the relationship to ensure that the transactions being undertaken are **consistent** with the subject person’s knowledge of the customer and of his business and risk profile, including, where necessary, the source of funds; and

(b) ensuring that the documents, data or information held by the subject person are **kept up-to-date**.
Scrutiny of transactions

Using your knowledge of the customer

- Information on the **purpose and intended nature** of the business relationship
- Customer’s business and risk profile

To **identify** unusual transactions/patterns

- Unusual by nature: suspicious, illogical, unnecessarily complex, unreasonable
- Inconsistent with customer’s profile
- Significantly different to customer’s usual transactions or requests

Examine purpose and background of all **complex and unusually large transactions** and **unusual patterns of transactions** with no apparent economic or lawful purpose

(Reg 11(9))
Purpose of ongoing monitoring

*Possible outcomes*

Ongoing monitoring + assessing transaction, pattern, or behaviour

- Identify suspicious activity
  - File a STR
- Consider updating CRA
  - Still within risk appetite?
  - Adjust CDD
- No action to be taken
Identifying unusual transactions

- Significant change in the **value** of individual transactions
- Significant change in the **overall volume or frequency** of transactions (*pattern*)
- A number of transactions in **rapid succession**
  - Purchase and immediate resale of securities
  - Deposit and immediate withdrawal of funds
- A change in the geographical destination or origin
- A change in the source of funds of the customer

Remember: Reg 11(9): examine purpose and background of complex and unusually large transactions, and unusual patterns of transactions, which do not have any apparent or economic lawful purpose
Assessing unusual transactions

Determining legitimacy

Determining whether there is a legitimate reason for a transaction or for the divergence from known patterns of activity:
Obtain information or documents on:

- Source of funds of that transaction
- Any new operational activities
- Significant relevant changes on the customer
  - e.g.: change in occupation
- Any other information you may consider necessary to be satisfied of the legitimacy of the source of funds

Level of data:
- Enough to come to a reasonable conclusion on the legitimacy of the transaction
- Should not be excessive, disproportionate or irrelevant
- Requests should make sense in the context of the transaction and the customer
Assessing unusual transactions

Doubts or reluctance – next steps?

• If you are not satisfied with the information/documents
• If you have doubts on the veracity of the information or the authenticity of the documents
• If the customer is being unreasonably uncooperative

CONSIDER FILING A STR
How to conduct transaction monitoring

Real time (pre-transaction)
- Face-to-face scenarios
- Non-face-to-face where transactions are not executed immediately
- More control and reassurance
- Requires awareness of relevant trigger events and red flags
- Requires understanding of the expected behaviour/use of the relationship
- EDD measure for high-risk customers and transactions
- Best combined with post-transaction monitoring to detect patterns

After the event (post-transaction)
- Not all relationships/services permit real-time monitoring and flagging of transactions
- Must still file STR, even after the event
- Permits detection of patterns
Transaction monitoring methods

• On the basis of a customer’s specific profile
  • A set of parameters within which transactions are considered normal
  • Question behaviour outside the parameters

• By comparing against peer group information
  • Group customers with similar characteristics and risk ratings
  • Extract information and create an average profile
  • Compare customers against that profile, question diverging behaviour
  • Requires sufficient statistics from a wide customer-base
  • May use official economic indicators such as average national income, from reputable sources
  • Not targeted – not ideal in high-risk situations
Transaction monitoring methods

• **On the basis of detection rules**
  • Analysis of transactions (individual and series) against set of thresholds, scenarios and parameters
  • Alert is triggered when a pre-defined detection rule is met
  • Detection rules must be relevant to be effective
  • Must be periodically tested and fine-tuned
  • Must strike balance between effective detection and not too many false positives
  • Updated to reflect trends and typologies

Relevant factors to be taken into account:

• Specific product or service
• Customer risk rating
• Anticipated level and value of transactions as determined through profile
• Anticipated value of transactions when taking into account the customer’s background, occupation and claimed source of wealth
• Anticipated jurisdictional connections
• Distribution channels
• New activity in formerly dormant account
Transaction monitoring methods

Manual vs automated monitoring systems

- Depends on size of subject person, number of clients and transactions, level of risk
- System must yield the desired results, including relevant alerts within adequate timeframes
- Large transactions are better monitored through automated systems

Automated system

- Does system generate a report showing reasons, rules and parameters?
- Can system be easily adapted to cater for changes?
- Can the system learn from previous false positive? (fine-tuning)

Assess effectiveness of alerts
Demonstrate good understanding of how the system operates
Ongoing monitoring of high-risk scenarios

Stricter ongoing monitoring to mitigate the higher ML/FT risk

Increasing the frequency and nature of the transaction monitoring
- Regular reviews of transactions to detect warning signs
- Stricter or more stringent detection rules
- Lower transaction value thresholds
- More weighting to factors such as high value transactions/other jurisdictions
- Adjusted thresholds for different products and services in same relationship

Consider applying pre-transaction monitoring where possible
Ensuring that documents, data and information are up-to-date

Information obtained in fulfilment of CDD obligations

• CRA, CDD measures, mitigating measures all based on information obtained at onboarding
• Relationships are not static, circumstances surrounding customer change
• Information must remain relevant, accurate, sufficient

• To retain clear understanding of ML/FT risks at all times
• To ensure that mitigating measures remain effective at all times
Remaining up-to-date:
*Information monitoring methods*

**Trigger events:**
*Events indicating a change in circumstances – update the information held on the customer*

- e.g.: Student with fixed income has graduated and set up a small consultancy firm.
  - Change in transaction patterns and values triggers a review
  - Information on the customer’s profile is updated to reflect the new occupation, anticipated source of funds, anticipated value of transactions

- e.g.: New product request: customer with savings account requests a bank loan
  - Consider whether information held is enough
  - Obtain more information on anticipated source of funds

- e.g.: Request for information about customer received from FIAU/Police
  - May be a trigger to take a closer look at the relationship
Remaining up-to-date:

Information monitoring methods

Periodic reviews:
Reviewing information at regular intervals

• Useful tool to update expired verification documents where necessary
• Risk-based reviewing
  Vary frequency depending on:
  • Customer’s risk rating
  • The kind of information to be updated
  • What risks are being mitigated through updating

Vary extent depending on:
• Above factors
• Relevance of the information in terms of CDD and AML
• The necessity of the information to be updated

Consider whether the information is necessary, proportionate and adds value