5.7 Monitoring customer activity

The requirement to monitor customers' activities

Regulation 28(11)

5.7.1 Firms must conduct ongoing monitoring of the business relationship with their customers. Its monitoring arrangements should be risk based, driven by the nature, size and complexity of the firm's business and form part of its financial crime control framework. Ongoing monitoring of a business relationship includes:

- Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, its business and risk profile;
- Ensuring that the documents or information obtained for the purposes of applying customer due diligence are kept up to date.

5.7.2 Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps firms know their customers, assist them to assess risk and provides greater assurance that the firm is not being used for the purposes of financial crime

What is monitoring?

5.7.3 The essentials of any system of monitoring are that:

- it flags up transactions and/or activities for further examination;
- these reports are reviewed promptly by the right person(s); and
- appropriate action is taken on the findings of any further examination.

5.7.4 Monitoring can be either:

- in real time, in that transactions and/or activities can be reviewed as they take place or are about to take place, or
- after the event, through some independent review of the transactions and/or activities that a customer has undertaken. This may be conducted over a reasonable time period to identify patterns/trends

and in either case, the objective is to identify or flag unusual transactions or activities for further examination.

5.7.5 Monitoring may be by reference to specific types of transactions, to the profile of the customer, to networks of connected persons, or by

comparing their activity or profile with that of a similar, peer group of customers, or through a combination of these approaches.

5.7.6 Firms should also have systems and procedures to deal with customers who have not had contact with the firm for some time, in circumstances where regular contact might be expected, and with dormant accounts or relationships, to be able to identify future reactivation and unauthorised use.

5.7.7 In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer and product risk.

5.7.8 Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. The scope and complexity of the process will be influenced by the firm's business activities, and whether the firm is large or small. The key elements of any system are having up-to-date customer information and being aware of evolving financial crime risks and typologies that are relevant to the firm, on the basis of which it will be possible to spot the unusual, and asking pertinent questions to elicit the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious.

5.7.8A Transaction monitoring is a dynamic process, and therefore monitoring arrangements, including automated monitoring system rules and thresholds should be reviewed regularly to ensure that they remain effective. This may include reallocating resources from less productive or less efficient monitoring arrangements (i.e. activity that never or seldom contributes to the management of financial crime risk) to higher priority risks to ensure that monitoring provides more effective outcomes.

These arrangements and any changes to them should be documented appropriately and be subject to regular review.

Nature of monitoring

5.7.9 Some financial services business typically involves transactions with customers about whom the firm has a good deal of information, acquired for both business and regulatory reasons. Other types of financial services business involve transactions with customers about whom the firm may need to have only limited information. The nature of the monitoring in any given case will therefore depend on the business of the firm, the frequency of customer activity, and the types of customers that are involved.

5.7.10 Effective monitoring is likely to be based on a considered identification of transaction characteristics, such as:

- the unusual nature of a transaction: e.g., abnormal size or frequency for that customer or peer group; the early surrender of an insurance policy;

- the nature of a series of transactions: for example, a number of cash credits;
- the geographic destination or origin of a payment: for example, to or from a high-risk country; the parties concerned: for example, a request to make a payment to or from a person on a sanctions list;
- known threats or typologies (in the public domain); and
- depending on and in keeping with a firm's nature, size and complexity - networks of connected accounts / counterparties / customers / beneficial owners.

5.7.11 The arrangements should include the training of staff on procedures to spot and deal specially (e.g., by referral to management) with situations that arise that suggest a heightened money laundering risk; or they could involve arrangements for exception reporting by reference to objective triggers (e.g., transaction amount). Staff training is not, however, a substitute for having in place some form of regular monitoring activity.

Regulation 33(1), 33(5)(d)

5.7.12 Higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring on a risk-based approach.

Manual or automated?

5.7.13 A monitoring system may be manual, or may be automated to the extent that a standard suite of exception reports are produced, or it may be a combination of the two. One or other of these approaches may suit most firms. In firms where there are major issues of volume, or where there are other factors that make a basic exception report regime inappropriate, a more sophisticated automated system may be necessary. Where manual monitoring is in place, firms should have procedures to manage the risk of manual error.

5.7.14 It is essential to recognise the importance of staff alertness. Such factors as staff intuition, direct exposure to a customer face-to-face or on the telephone, and the ability, through practical experience, to recognise transactions that do not seem to make sense for that customer, cannot be automated (see Chapter 8: Staff awareness, training and alertness).

5.7.15 In relation to a firm's monitoring needs, an automated system may add value to manual systems and controls, provided that the parameters determining the outputs of the system are appropriate. Firms should understand the workings and rationale of an automated system, and should understand the reasons for its output of alerts, as it may be asked to explain this to its regulator.

5.7.16 The greater the volume of transactions, the less easy it will be for a firm to monitor them without the aid of some automation. Systems available include those that many firms, particularly those that offer credit, use to monitor fraud. Although not specifically designed to identify money laundering or terrorist financing, the output from these anti-fraud monitoring systems can often indicate possible money laundering or terrorist financing.

5.7.17 There are many automated transaction monitoring systems available on the market; they use a variety of techniques to detect and report unusual/uncharacteristic activity. These techniques can range from artificial intelligence to simple rules. The systems available are not designed to detect money laundering or terrorist financing, but are able to detect and report unusual/uncharacteristic behaviour by customers, and patterns of behaviour that are characteristic of money laundering or terrorist financing, which after analysis may lead to suspicion of money laundering or terrorist financing. The implementation of transaction monitoring systems is difficult due to the complexity of the underlying analytics used and their heavy reliance on customer reference data and transaction data.

The ongoing effectiveness of these systems also depends on the system parameters that are used (e.g. rules/thresholds). Firms should ensure that the thresholds used are relevant and applicable to their business and customer activities.

5.7.18 Monitoring systems, manual or automated, can vary considerably in their approach to detecting and reporting unusual or uncharacteristic behaviour. It is important for firms to ask questions of the supplier of an automated system, and internally within the business, whether in support of a manual or an automated system, to aid them in selecting a solution that meets their particular business needs best. Questions that should be addressed include:

- How does the solution enable the firm to implement a risk-based approach to customers, third parties and transactions?
- How do system parameters aid the risk-based approach and consequently affect the quality of transactions alerted?
- What are the money laundering/terrorist financing typologies that the system addresses, and which component of the system addresses each typology? Are the typologies that are included with the system complete? Are they relevant to the firm's particular line of business? How often are they updated?
- What functionality does the system provide to implement new typologies, how quickly can relevant new typologies be commissioned in the system and how can their validity be tested prior to activation in the live system?
- What functionality exists to provide the user with the reason that a transaction is alerted and is there full evidential process behind the reason given?
- Does the system have robust mechanisms to learn from previous experience and how are unproductive alerts/ 'false positives' continually monitored and reduced?

Although monitoring processes may be outsourced, firms remain responsible for their regulatory obligations.

5.7.19 What constitutes unusual or uncharacteristic behaviour by a customer, is often defined by the system. It will be important that the system selected has an appropriate definition of 'unusual or uncharacteristic' and one that is in line with the nature of business conducted by the firm.

5.7.20 The effectiveness of a monitoring system, automated or manual, in identifying unusual activity will depend on the quality of the parameters which determine what alerts it makes, and the ability of staff to assess and act as appropriate on these outputs. The needs of each firm will therefore be different, and each system will vary in its capabilities according to the scale, nature and complexity of the business. It is important that the balance is right in setting the level at which an alert is generated; it is not enough to fix it so that the system generates just enough output for the existing staff complement to deal with – but equally, the system should not generate large numbers of unproductive alerts/'false positives', which require excessive resources to investigate.

Firms should establish an appropriate governance mechanism for the oversight, review and approval of monitoring processes and parameters, which will include documenting its monitoring arrangements and rationale. This may include consideration of the following, for example:

- Defining responsibilities for the governance mechanism
- Measuring the effectiveness and relevance of monitoring arrangements
- Supporting changes to systems to address evolving ML/TF risks
- Approach and governance for reallocation of resource (e.g. turning off/dialling down less efficient monitoring parameters or introducing different parameters)

5.7.21 Monitoring also involves keeping information held about customers up to date, as far as reasonably possible. Guidance on this is given at paragraphs 5.3.27 - 5.3.28.