Chapter 11
Monitoring Transactions and Activity

Contents of this Chapter

11.1. Introduction 146
11.2. Objectives 146
11.3. Obligations 147
11.4. PEP Relationships 147
11.5. High Risk Transactions or Activity 148
11.6. Real-Time and Post-Event Transaction Monitoring 148
11.7. Automated and Manual Monitoring 149
11.7.1. Automated Monitoring Methods 149
11.8. Examination 150
11.9. Ongoing Customer Due Diligence 151
11.10. Oversight of Monitoring Controls 152

11.1. Introduction

1. The regular monitoring of a *business relationship*, including any transactions and other activity carried out as part of that relationship, is one of the most important aspects of effective ongoing *CDD* measures.

2. It is vital that the firm understands a *customer's* background and is aware of changes in the circumstances of the *customer* and *beneficial owner* throughout the life-cycle of a *business relationship*. The firm can usually only determine when it might have reasonable grounds for knowing or suspecting that *ML* and/or *FT* is occurring if it has the means of assessing when a transaction or activity falls outside the normal expectations for a particular *business relationship*.

3. There are two strands to effective ongoing monitoring:

   (a) The first relates to the transactions and activity which occur on a day-to-day basis within a *business relationship* and which need to be monitored to ensure they remain consistent with the firm's understanding of the *customer* and the product or service it is providing to the *customer*.
   (b) The second relates to the *customer* themselves and the requirement for the firm to ensure that it continues to have a good understanding of its *customers* and their *beneficial owners*. This is achieved through maintaining relevant and appropriate *CDD* and applying appropriate ongoing screening.

4. This Chapter deals with the requirement for the firm to monitor *business relationships* on an ongoing basis, including the application of scrutiny to large and unusual or complex transactions or activity so that *ML* and *FT* may be identified and prevented.

11.2. Objectives

5. A key prerequisite to managing the *risk* of a *business relationship* is understanding the *customer*, and *beneficial owner*, and where changes to those parties occur. It is also important to maintain a thorough understanding of the *business relationship* and to appropriately monitor transactions in order to be in a position to detect, and subsequently report, suspicious activity.

6. The type of monitoring applied by the firm will depend on a number of factors and should be developed with reference to the firm's *business risk assessments* and *risk appetite*. The factors forming part of this consideration will include the size and nature of the firm's business, including the characteristics of its *customer*-base and the complexity and volume of expected transactions or activity.

7. The monitoring of *business relationships* should involve the application of scrutiny to large and unusual or complex transactions, as well as to patterns of transactions or activity, to ensure that such transactions and activity are consistent with the firm's knowledge of the *customer*, their business and *risk* profile, including where necessary, the source of *funds*. Particular attention should be paid to *high risk relationships* (for example, those involving *foreign PEPs*), high *risk* countries and territories and high *risk* transactions.

8. An unusual transaction or activity may be in a form that is inconsistent with the expected pattern of activity within a particular *business relationship*, or with the normal business activities for the type of product or service that is being delivered. For example, unusual patterns of transactions with no apparent or visible economic or lawful purpose.

9. The nature of the monitoring in any given case will depend on the business of the firm, the frequency of activity and the types of business. Monitoring may include reference to: specific

types of transactions; the relationship profile; a comparison of activities or profiles with that of a similar *customer* or peer group; or a combination of these approaches.

11.3. Obligations

10. In accordance with Paragraph 11(1) of *Schedule 3*, the firm shall perform ongoing and effective monitoring of any *business relationship*, which shall include –

(a) reviewing *identification data* and records to ensure they are kept up to date, accurate and relevant, and updating such data and records when they are not up to date, accurate or relevant;
(b) scrutinising any transactions or other activity to ensure that the transactions are consistent with the firm's knowledge of the *customer*, their business and *risk* profile (including, where necessary, the source of *funds*) and paying particular attention to all –

(i) complex transactions;
(ii) transactions which are both large and unusual; and
(iii) unusual patterns of activity or transactions,

which have no apparent economic purpose or no apparent lawful purpose; and
(c) ensuring that the way in which *identification data* is recorded and stored is such as to facilitate the ongoing monitoring of each *business relationship*.

11. In accordance with Paragraph 11(2) of *Schedule 3*, the extent of any monitoring carried out and the frequency at which it is carried out shall be determined on the basis of materiality and *risk* including, without limitation, whether or not the *business relationship* is a *high risk relationship*.

12. Examples of the additional monitoring arrangements for *high risk relationships* could include:

(a) undertaking more frequent reviews of *high risk relationships* and updating *CDD information* on a more regular basis;
(b) undertaking more regular reviews of transactions and activity against the profile and expected activity of the *business relationship*;
(c) applying lower monetary thresholds for the monitoring of transactions and activity;
(d) reviews being conducted by persons not directly involved in managing the relationship, for example, the *MLCO*;
(e) ensuring that the firm has adequate MI systems to provide the *board* and *MLCO* with the timely information needed to identify, analyse and effectively monitor *high risk relationships* and *accounts*;
(f) appropriate approval procedures for high value transactions in respect of *high risk relationships*; and/or
(g) a greater understanding of the personal circumstances of *high risk relationships*, including an awareness of sources of third party information.

13. The firm must consider the possibility for *legal persons* and *legal arrangements* to be used as vehicles for *ML* and *FT*.

11.4. PEP Relationships

14. The system of monitoring used by the firm must provide for the ability to identify where a *customer* or *beneficial owner* becomes a *PEP* during the course of the *business relationship* and whether that person is a *foreign PEP*, *domestic PEP* or *international organisation PEP*.

15. In accordance with Paragraph 5(3)(a)(ii) of *Schedule 3*, where a *customer* or *beneficial owner* becomes a *foreign PEP* during the course of an existing *business relationship*, as part of the *ECDD* measures subsequently applied the firm shall obtain senior management approval to continue that relationship.

16. Where the firm identifies during the course of a *business relationship* that the *customer* or *beneficial owner* is a *domestic PEP* or *international organisation PEP*, it should refer to the requirements of *Commission Rule* 8.45.

17. It is not expected that the firm will have a thorough knowledge of, or fully research, a family connection. The extent to which a connection is researched should be based upon the size, scale, complexity and involvement of the person in the context of the *business relationship* and the profile of the *business relationship*, including its asset value.

18. It is possible that family members and/or associates may not inform the firm, or even be aware, of their *PEP* status and therefore independent screening and monitoring should be conducted. It is also possible that an individual's *PEP* status may not be present at take-on, for example, where that person takes office during the life of a *business relationship*. It is therefore important that ongoing monitoring exists in order to identify changes of status and *risk* classification.

11.5. High Risk Transactions or Activity

19. When conducting ongoing monitoring, the following are examples of red flags which may indicate high *risk* transactions or activity within a *business relationship*:

(a) an unusual transaction in the context of the firm's understanding of the *business relationship* (for example, abnormal size or frequency for that *customer* or peer group, or a transaction or activity involving an unknown third party);
(b) funds originating from, or destined for, an unusual location, whether specific to an individual *business relationship*, or for a generic *customer* or product type;
(c) the unexpected dormancy of an *account*, or transactions or activity unexpectedly occurring after a period of dormancy;
(d) unusual patterns of transactions or activity which have no apparent economic or lawful purpose;
(e) an instruction to effect payments for advisory or consulting activities with no apparent connection to the known activities of the *customer* or their business;
(f) the involvement of charitable or political donations or sponsorship; or
(g) a *relevant connection* with a country or territory that has significant levels of corruption, or provides funding or support for terrorist activities.

20. Transactions or activity to or from jurisdictions specified in Appendix H to this *Handbook*, any *Commission* Notices, Instructions and Warnings and those covered by sanctions legislation applicable in the *Bailiwick* ~~the Business from Sensitive Sources Notices and Instructions issued by the *Commission*~~ must be subject to a greater level of caution and scrutiny.

https://www.gfsc.gg/commission/financial-crime/business-sensitive-sources-notices

11.6. Real-Time and Post-Event Transaction Monitoring

21. Monitoring procedures should involve a combination of real-time and post-event monitoring. Real-time monitoring focuses on transactions and activity where information or instructions are received before or as the instruction is processed. Post-event monitoring involves periodic, for example monthly, reviews of transactions and activity which have occurred over the preceding period.

22. Real-time monitoring of activity can be effective at reducing exposure to *ML*, *FT* and predicate offences such as bribery and corruption, whereas post-event monitoring may be more effective at identifying patterns of unusual transactions or activities.

23. In this respect, regardless of the split of real-time and post-event monitoring, the over-arching purpose of the monitoring process employed should be to ensure that unusual transactions and activity are identified and flagged for further examination.

11.7. Automated and Manual Monitoring

24. The firm's monitoring processes should be appropriate having regard to its size, activities and complexity, together with the *risks* identified by the firm within its *business risk assessments*. While bigger firms with large volumes of transactions will likely favour an automated system, the firm may conclude that a manual real-time and/or post-event monitoring process is sufficient given the size and scale of its business.

25. Notwithstanding the method of monitoring used, in accordance with the requirements of Paragraph 11(2) of *Schedule 3*, the firm should adapt the parameters of its processes, in particular the extent and frequency of monitoring, on the basis of materiality and *risk*, including, without limitation, whether or not a *business relationship* is a *high risk relationship*.

26. In establishing the expected norms of a *business relationship* and in turn the appropriate parameters for its monitoring processes to be effective, the firm should consider, as a minimum, the nature and level of expected transactions and activity and the assessed *risk* of the *business relationships* that are being monitored.

27. The rationale for deciding upon either a manual or automated method of monitoring, together with the criteria in defining the parameters of that monitoring, should be based on the conclusions of the firm's *business risk assessments* and *risk appetite*. The decision made by the firm should be documented as part of this process, together with an explanation demonstrating why the *board* consider the chosen method to be appropriate and effective.

11.7.1. Automated Monitoring Methods

28. Where the firm has a large number of *business relationships* or a high level of activity, effective monitoring is likely to necessitate the automation of the monitoring process. Such automated systems may be used to facilitate the monitoring of significant volumes of transactions or *business relationships*, and associated *customers* and *beneficial owners*. Automated systems may also be utilised where the firm operates in an environment where the opportunity for human scrutiny of individual transactions and activity is limited, for example, in e-commerce.

29. The use of automated monitoring methods can be effective in both strands of ongoing monitoring:

    (a) identifying a transaction and/or activity which warrant further scrutiny; and
    (b) screening *customers* and *beneficial owners* to *business relationships*, as well as the *payers* and *payees* to individual transactions, for connections to persons subject to UN or EU sanction or posing an increased *risk*. For example, *PEPs*, those convicted of criminal acts, or those persons in respect of whom adverse media exists.

30. With regard to the monitoring of transactions and activity, exception procedures and reports can provide a simple but effective means of monitoring all incoming and outgoing transactions and activity to identify those involving, amongst other things:

    (a) particular countries, territories or geographical locations;

(b) particular products, services and/or *accounts*; or
(c) transactions or activity falling outside of predetermined parameters within a given time frame.

31. Where an automated monitoring method is used, whether specific to the firm or a group-wide system, the firm must:

(a) understand how the system works and how to use the system (for example, making full use of guidance);
(b) understand when changes are to be made to the system (including the nature and extent of any changes);
(c) understand the system's coverage (including the extent of the transactions, activity and/or parties monitored);
(d) understand the sources of data used (including both the source(s) of internal data fed into the system and the source(s) of external data to which it is compared);
(e) understand the nature of the system's output (exceptions, alerts etc.);
(f) set clear procedures for dealing with potential matches, driven on the basis of *risk* rather than resources; and
(g) record the basis for discounting alerts (for example, false positives) to ensure there is an appropriate audit trail.

32. Subject to *Commission Rule* 11.33. below, the firm must ensure that the parameters of any automated system allow for the generation of alerts for large and unusual, complex, or higher *risk* transactions or activity which must be subject to further investigation.

33. Where the firm is a branch office or subsidiary of an international group and uses group-wide systems for transaction and activity monitoring, the ability for the firm to dictate the particular characteristics of the monitoring conducted by the system may be limited. Where this is the case, notwithstanding the group-wide nature of the system, the firm must be *satisfied* that it provides adequate mitigation of the *risks* applicable to the business of the firm.

34. The firm should be aware that the use of computerised monitoring systems does not remove the requirement for *relevant employees* to remain vigilant. It is essential that the firm continues to attach importance to human alertness. Factors such as a person's intuition; direct contact with a *customer* either face-to-face or on the telephone; and the ability, through practical experience, to recognise transactions and activities which do not seem to have a lawful or economic purpose, or make sense for a particular *customer*, cannot be automated.

11.8. Examination

35. In accordance with Paragraph 11(3) of *Schedule 3*, where within an existing *business relationship* there are complex, or large and unusual, transactions, or unusual patterns of transactions, which have no apparent economic or lawful purpose, the firm shall:

(a) examine the background and purpose of those transactions, and
(b) increase the degree and nature of monitoring of the *business relationship*.

36. As part of its examination, the firm should give consideration to the following:

(a) reviewing the identified transaction or activity in conjunction with the *relationship risk assessment* and the *CDD information* held;
(b) understanding the background of the activity and making further enquiries to obtain any additional information required to enable a determination to be made by the firm as to whether the transaction or activity has a rational explanation and economic purpose;

(c) reviewing the appropriateness of the *relationship risk assessment* in light of the unusual *transaction* or activity, together with any supplemental *CDD information* obtained; and
(d) considering the transaction or activity in the context of any other connected *business relationships* and the cumulative effect this may have on the *risk* attributed to those relationships.

37. For the purposes of Paragraph 11(3) of *Schedule 3*, what constitutes a large and unusual or complex transaction will be based on the particular circumstances of a *business relationship* and will therefore vary from *customer* to *customer*.

38. The firm must ensure that the examination of any large and unusual, complex, or otherwise higher *risk* transaction or pattern of transactions or other activity is sufficiently documented and that such *documentation* is retained in a readily accessible manner in order to assist *the Commission*, the *FIS*, other domestic competent authorities and auditors.

39. The firm must ensure that procedures are *maintained* which require that an internal disclosure is filed with the *MLRO* in accordance with the requirements of Chapter 13 of this *Handbook* where the circumstances of the transaction or activity raise a suspicion of *ML* and/or *FT*.

40. Following the conclusion of its examination, the firm should give consideration to whether follow-up action is necessary in light of the identified transaction or activity. This could include, but is not limited to:

(a) applying *ECDD* measures where this is considered necessary or where the firm has re-assessed the *business relationship* as being high *risk* as a consequence of the transaction or activity;
(b) considering whether further *employee* training in the identification of large and unusual, complex, or higher risk transactions and activity is needed;
(c) subject to *Commission Rule* 11.33. above, considering whether there is a need to adjust the monitoring system (for example, refining monitoring parameters or enhancing controls for more vulnerable products, services and/or business units); and/or
(d) applying increased levels of on-going monitoring for particular relationships.

11.9. Ongoing Customer Due Diligence

41. The requirement to conduct ongoing *CDD* will ensure that the firm is aware of any changes in the development of a *business relationship*. The extent of the firm's ongoing *CDD* measures must be determined on a *risk*-sensitive basis. However, the firm must be aware that as a *business relationship* develops, the risks of *ML* and *FT* may change.

42. *The Commission* would expect ongoing *CDD* to be conducted on a periodic basis in line with the requirement to review *relationship risk assessments* in accordance with Paragraph 3(4)(b) of *Schedule 3*, or where a trigger event occurs in the intervening period.

43. It should be noted that it is not necessary to re-verify or obtain current *identification data* unless an assessment has been made that the *identification data* held is not adequate for the assessed *risk* of the *business relationship* or there are doubts about the veracity of the information already held. Examples of such could include a material change in the way that the business of the *customer* is conducted which is inconsistent with its existing business profile, or where the firm becomes aware of changes to a *customer's* or *beneficial owner's* circumstances, such as a change of address.

44. In order to reduce the burden on *customers* and other *key principals* in *low risk relationships*, trigger events (for example, the opening of a new *account* or the purchase of a further product) may present a convenient opportunity to review the *CDD information* held.

11.10. Oversight of Monitoring Controls

45. The *MLCO* should have access to, and familiarise his or her self with, the results and output from the firm's monitoring processes. Such output should be reviewed by the *MLCO* who in turn should report regularly to the *board*, providing relevant MI such as statistics and key performance indicators, together with details of any trends and actions taken where concerns or discrepancies have been identified.

46. The *board* should consider the appropriateness and effectiveness of the firm's monitoring processes as part of its annual review of the firm's *business risk assessments* and associated policies, procedures and controls. This should include consideration of the extent and frequency of such monitoring, based on materiality and *risk* as set out in the *business risk assessments*.

47. Where the firm identifies weaknesses within its monitoring arrangements, it should ensure that these are rectified in a timely manner and consideration should be given to *notifying the Commission* in accordance with the requirements of Section 2.7. of this *Handbook.*