6 ON-GOING MONITORING: SCRUTINY OF TRANSACTIONS & ACTIVITY

Please Note:

- Regulatory requirements are set within this section as *AML/CFT Codes of Practice*.
- This section contains references to Jersey legislation which may be accessed through the JFSC website.
- Where terms appear in the Glossary this is highlighted through the use of italic text. The Glossary is available from the JFSC website.

6.1 Overview of Section

1. This section outlines the statutory provisions concerning on-going monitoring. On-going monitoring consists of:
   - Scrutinising transactions undertaken throughout the course of a business relationship; and
   - Keeping documents, data or information up to date and relevant.
2. The obligation to monitor a business relationship (a business relationship, as explained in Section 1, is also sometimes referred to in the legal profession as a "matter") finishes at the time that it is terminated. In a case where a relationship has been terminated but where payment for a service remains outstanding, a firm will still need to consider reporting provisions summarised in Section 8, e.g. where there is suspicion that payment for the service is made out of the proceeds of criminal conduct.
3. This section explains the measures required to demonstrate compliance with the requirement to scrutinise transactions and also sets a requirement to scrutinise client activity.
4. The requirement to keep documents, data and information up to date and relevant is discussed at Section 3.4 of this Handbook.

6.2 Obligation to Perform On-Going Monitoring

Statutory Requirements

5. *Article 3(3) of the Money Laundering Order sets out what on-going monitoring is to involve:*
   - *Scrutinising transactions undertaken throughout the course of a business relationship to ensure that the transactions being conducted are consistent with the relevant person's knowledge of the customer, including the customer's business and risk profile. See Article 3(3)(a) of the Money Laundering Order.*
   - *Keeping documents, data or information up to date and relevant by undertaking reviews of existing records, particularly in relation to higher risk categories of clients. See Article 3(3)(b) of the Money Laundering Order.*
6. *Article 13 of the Money Laundering Order requires a relevant person to apply on-going monitoring throughout the course of a business relationship.*
7. *Article 11(1) of the Money Laundering Order requires a relevant person to establish and maintain appropriate and consistent policies and procedures for the application of CDD measures, having regard to the degree of risk of money laundering and the financing of terrorism. The policies and procedures referred to include those:*

- *which provide for the identification and scrutiny of:*
  - *complex of unusually large transactions;*
  - *unusual patterns of transactions, which have no apparent economic or lawful purpose; or*
  - *any other activity, the nature of which causes the relevant person to regard it as particularly likely to be related to money laundering or the financing of terrorism.*
- *which determine whether:*
  - *business relationships or transactions are with a person connected with a country or territory in relation to which the FATF has called for the application of enhanced CDD measures; or*
  - *business relationships or transactions are with a person:*
    - subject to measures under law applicable in Jersey for the prevention and detection of money laundering,
    - connected with an organization that is subject to such measures, or
    - connected with a country or territory that is subject to such measures.

8. *Article 11(3A) of the Money Laundering Order explains that, for the purposes of Article 11(1), "scrutiny" includes scrutinising the background and purpose of transactions and activities.*

6.2.1 Scrutiny of Transactions and Activity

Overview

9. **Scrutiny** may be considered as two separate, but complimentary processes:

10. Firstly, a firm **monitors** all client transactions and activity in order to **recognise notable transactions or activity,** i.e. those that:
    - are inconsistent with the firm's knowledge of the client;
    - are complex or unusually large;
    - form part of an unusual pattern; or
    - present a higher risk of *money laundering* or *the financing of terrorism*.

11. Secondly, such notable transactions and activity are then **examined** by an appropriate person, including the background and purpose of such transactions and activity.

12. In addition to the scrutiny of transactions, as required by the *Money Laundering Order*, *AML/CFT Codes of Practice* set in this section requires a firm to also scrutinise client activity (though this will already be the effect of *policies and procedures* required by Article 11(3)(a)(iii) of the *Money Laundering Order*).

13. A firm must therefore, as a part of its **scrutiny** of transactions and activity, establish appropriate procedures to **monitor** all of its clients' transactions and activity and to **recognise** and **examine** notable transactions or activity.

14. Sections 3 and 4 of this Handbook address the capturing of sufficient information about a client that will allow a firm to prepare and record a client business and risk profile which will provide a basis for recognising notable transactions or activity.

15. **Unusual transactions or activity, unusually large transactions or activity, and unusual patterns of transactions or activity** may be recognised where transactions or activity are

inconsistent with the expected pattern of transactions or expected activity for a particular client, or with the normal business activities for the type of service that is being delivered.

16. For many clients of law firms, a complete profile and appropriate risk assessment may only become evident whilst acting for the client, making the updating of documents, data or information and monitoring of client activity and transactions key to obtaining a complete understanding of client relationships. The more a firm knows about its clients and develops an understanding of the instructions, the better placed it will be to assess risks.

17. **Higher risk transactions or activity** may be recognised by developing a set of "red flags" or indicators which may indicate *money laundering* or *the financing of terrorism*, based on a firm's understanding of its business, its products and its clients (i.e. the outcome of its business risk assessment – Section 2.3.1).

18. **Complex transactions or activity** may be recognised by developing a set of indicators, based on a firm's understanding of its business, its products and its customers (i.e. the outcome of its business risk assessment – Section 2.3.1).

19. External data sources and media reports will also assist with the identification of notable transactions and activity.

20. Where notable transactions or activity are **recognised**, such transactions or activity will need to be **examined**. The purpose of this examination is to determine whether there is an **apparent** economic or **visible** lawful purpose for the transactions or activity recognised. It is not necessary (nor will it be possible) to conclude with certainty that a transaction or activity has an economic or lawful purpose. Sometimes, it may be possible to make such a determination on the basis of an existing client business and risk profile, but on occasions this examination will involve requesting additional information from a client.

21. Notable transactions or activity may indicate *money laundering* or *the financing of terrorism* where there is no apparent economic or visible lawful purpose for the transaction or activity, i.e. they are no longer just unusual but may also be suspicious. Reporting of knowledge, suspicion, or reasonable grounds for knowledge or suspicion of *money laundering* or *the financing of terrorism* is addressed in Section 8 of this Handbook.

22. Scrutiny may involve both **real time** and **post event** monitoring and may involve manual or automated procedures. However, for most law firms, it is unlikely that automated transaction or activity monitoring procedures will be relevant. Monitoring is likely to be most effective when undertaken on a case-by-case basis by fee earners, administration and accounts staff which may be expected to highlight notable transactions or activity.

23. The examination of notable transactions or activity may be conducted either by fee earners or some other independent reviewer. In any case, the examiner must have access to all client records.

24. The results of an examination should be recorded and action taken as appropriate. Refer to Section 10 of this Handbook for record-keeping requirements in relation to the examination of some notable transactions and activity.

25. In order to recognise *money laundering* and *the financing of terrorism*, employees will need to have a good level of awareness of both and to have received training. Awareness raising and training are covered in Section 9 of this Handbook.

26. Where on-going monitoring indicates possible *money laundering* or financing terrorism activity an internal *SAR* must be made to the *MLRO*. Reporting of knowledge, suspicion, or reasonable grounds for knowledge or suspicion of *money laundering* and *the financing of terrorism* is addressed in Section 8 of this Handbook.

AML/CFT Codes of Practice

27. In addition to the scrutiny of transactions, on-going monitoring must also involve scrutinising activity in respect of a business relationship to ensure that the activity is consistent with the firm's knowledge of the client, including the client's business and risk profile.

28. A firm must establish and maintain appropriate and consistent *policies and procedures* which provide for the identification and scrutiny of:

    › complex or unusually large activity;

    › unusual patterns of activity, which have no apparent economic or visible lawful purpose; and

    › any other activity the nature of which causes the firm to regard it as particularly likely to be related to *money laundering* or the *financing of terrorism*.

29. As part of its examination of the above transactions, a firm must examine, as far as possible, their background and purpose and set forth its findings in writing.

Guidance Notes

30. A firm may demonstrate that *CDD policies and procedures* are appropriate where **scrutiny** of transactions and activity has regard to the following factors:

    › its business risk assessment (including the size and complexity of its business);

    › the nature of its legal business and services;

    › whether it is possible to establish appropriate standardised parameters for automated monitoring; and

    › the monitoring procedures that already exist to satisfy other business needs.

31. A firm may demonstrate that *CDD policies and procedures* are appropriate where the following are used to **recognise** notable transactions or activity:

    › **client business and risk profile** – see Section 3.3.5 of this Handbook;

    › **"Red flags" or indicators of higher risk –** that reflect the risk that is present in the firm's client base – based on its business risk assessment (refer to Section 2.3.1 of this Handbook), information published from time to time by the *Commission* of *JFCU*, e.g. findings of supervisory and themed examinations and typologies, and information published by reliable and independent third parties; and

    › **"Red flags" or indicators of complex transactions or activity** – based on business risk assessment (refer to Section 2.3.1 of this Handbook), information published from time to time by the *Commission* or the *JFCU*, e.g. findings of supervisory and themed examinations and typologies, and information published by reliable and independent third parties.

32. A firm may demonstrate that *CDD policies and procedures* are appropriate if **examination** of notable transactions or activity includes:

    › reference to the client's business and risk profile;

    › as far as possible, a review of the background and purpose of a transaction or activity (set in the context of the business and risk profile); and

    › where necessary, the collection of further information needed to determine whether a transaction or activity has an apparent economic or visible lawful purpose.

33. For example, a firm may have acted for a client in preparing a will and purchasing a modest family home. The client may then instruct the firm in the purchase of a holiday home, the

value of which appears to be outside the means of the client's financial situation as the firm had previously been advised in earlier matters. While the firm may be satisfied that it still knows the identity of the client, as part of on-going monitoring obligations it would be appropriate in such a case to ask about the *source of funds* for this purchase. Depending on the client's willingness to provide such information, and the answer that is provided, the firm should consider whether it is satisfied with that response, wants further proof of the *source of funds*, or needs to discuss with the *MLRO* whether a SAR should be made.

34. A firm may demonstrate that *CDD* and reporting *policies and procedures* are effective if **post-examination** of notable transactions or activity it:

- revises, as necessary, its client's business and risk profile;
- adjusts, as necessary, its monitoring system e.g. refines monitoring parameters, enhances controls for more vulnerable services; and
- considers whether it knows, suspects or has reasonable grounds for suspecting that another person is engaged in *money laundering* or *the financing of terrorism*, or that any property constitutes or represents the proceeds of criminal conduct.

6.2.2 Monitoring and Recognition of Business Relationships – Person Connected with an Enhanced Risk State or Sanctioned Country or Organization

Overview

35. The risk that a business relationship is tainted by funds that are the proceeds of criminal conduct or are used to finance terrorism is increased where the business relationship is with a person connected with a country or territory:

- in relation to which the *FATF* has called for the application of enhanced *CDD* measures – **an enhanced risk state**; or
- that is subject to measures for purposes connected with the prevention and detection of *money laundering* or *the financing of terrorism*, such measures being imposed by one or more countries or sanctioned by the *EU* or the *UN* – a **sanctioned country or territory**.

36. Similarly, the risk that a business relationship is tainted by funds that are the proceeds of criminal conduct or are used to finance terrorism is increased where the business relationship or transaction is with a person connected with an organization subject to such measures or who is themselves subject to such measures - a **sanctioned country or territory**.

37. As part of its on-going monitoring procedures, a firm will establish appropriate procedures to **monitor** all client transactions and activity in order to **recognise** whether any business relationships are with such a person.

38. There is not a separate requirement to **examine**, or have *policies and procedures* in place to examine, business relationships with an **enhanced risk state** once they are recognised. This is because enhanced *CDD* measures must be applied in line with Article 15(1)(c) of the *Money Laundering Order*. See Section 7.5 of this Handbook.

39. There is not a Statutory Requirement to **examine**, or have *policies and procedures* in place to examine, business relationships with a **sanctioned person, organization, country or territory** once they are recognised. This is because provisions in financial sanctions legislation must be followed. Inter alia, such provisions may prohibit certain activities or require the property of listed persons to be frozen. Further guidance[1] is published on the *Commission*'s website.

[1] https://www.jerseyfsc.org/industry/international-co-operation/sanctions/

AML/CFT Codes of Practice

40. On-going monitoring must involve **examining** transactions and activity recognised as being with a person connected with an enhanced risk state.

41. A firm person must establish and maintain appropriate and consistent *policies and procedures* which provide for the **examination** of transactions and activity recognised as being with a person connected with an enhanced risk state.

42. As part of its examination of the above transactions, a firm must examine, as far as possible, their background and purpose and set forth its findings in writing.

Guidance Notes

43. A firm may demonstrate that *CDD policies and procedures* are appropriate where **scrutiny** of transactions and activity has regard to the following factors:

    › its business risk assessment (including the size and complexity of its business);

    › whether it is practicable to monitor transactions or activity in real time (i.e. before client instructions are put into effect); and

    › whether it is possible to establish appropriate standardised parameters for automated monitoring.

44. A firm may demonstrate that *CDD policies and procedures* are appropriate where the following are used to **recognise** connections with persons connected to enhanced risk states and sanctioned countries:

    › **All -** Client business and risk profile in line with Section 3.3.5 of this Handbook.

    › **Enhanced risk states** - Appendix D1 of the *AML/CFT Handbook*.

    › **Sanctioned countries** - Appendix D2 of the *AML/CFT Handbook* (Source 6 only).

45. A firm may demonstrate that *CDD policies and procedures* are appropriate if **examination** of transactions or activity recognised as being with a person connected with an enhanced risk state includes:

    › reference to the client's business and risk profile;

    › as far as possible, a review of the background and purpose of a transaction or activity (set in the context of the business and risk profile); and

    › where necessary, the collection of further information needed to determine whether a transaction or activity has an apparent economic or visible lawful purpose.

46. A firm may demonstrate that *CDD* and reporting *policies and procedures* are appropriate if **post-examination** of transactions or activity recognised as being with a person connected with an enhanced risk state it:

    › revises, as necessary, its client's business and risk profile;

    › adjusts, as necessary, its monitoring system e.g. refines monitoring parameters, enhances controls for more vulnerable services; and

    › considers whether it knows, suspects or has reasonable grounds for suspecting that another person is engaged in *money laundering* or *the financing of terrorism*, or that any property constitutes or represents the proceeds of criminal conduct.

6.3 Automated Monitoring Methods

Overview

47. Automated monitoring methods may be effective in recognising notable transactions and activity, and business relationships and transactions with persons connected to enhanced risk states and sanctioned countries and territories.

48. **Exception reports** can provide a simple but effective means of monitoring all transactions to or from particular geographical locations or accounts and any activity that falls outside of pre-determined parameters - based on thresholds that reflect a client's business and risk profile.

49. Large or more complex firms may also use automated monitoring methods to facilitate the monitoring of significant volumes of transactions, or - in an e-commerce environment - where the opportunity for human scrutiny of individual transactions is limited.

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

51. Where an automated monitoring method (group or otherwise) is used, a firm will need to understand:

- How the system works and when it is changed;
- Its coverage (who or what is monitored and what external data sources are used);
- How to use the system, e.g. making full use of guidance; and
- The nature of its output (exceptions, alerts etc).

52. Use of automated monitoring methods does not remove the need for a firm to otherwise remain vigilant. Factors such as staff intuition, direct contact with a client, and the ability, through experience, to recognise transactions and activity that do not seem to make sense, cannot be automated.

53. In the case of **screening** of a business relationship (before establishing that relationship and subsequently) and transactions, the use of electronic external data sources to screen clients may be particularly effective. However, where a firm uses group screening arrangements, it will need to be satisfied that it provides adequate mitigation of risks applicable to the Jersey business. In all cases, it is important that a firm:

- Understands which business relationships and transaction types are screened.
- Understands the system's capacity for "fuzzy matching" (technique used to recognise names that do not precisely match a target name but which are still potentially relevant).
- Sets clear procedures for dealing with potential matches, driven by risk considerations rather than resources.
- Records the basis for "discounting" alerts (e.g. false positives) to provide an audit trail.

54. By way of example, fuzzy matching arrangements can be used to identify the following variations:

Variation	Example
Different spelling of names	"Jon" instead of "John" "Abdul" instead of "Abdel"
Name reversal	"Adam, John Smith" instead of "Smith, John Adam"
Shortened names	"Bill" instead of "William
Insertion/removal of punctuation and spaces	"Global Industries Inc" instead of "Global-Industries, Inc."
Name variations	"Chang" instead of "Jang"

55. Further information on screening practices may be found in a report published by the *Commission* in August 2014[2].

6.4 Warning Signs for the Legal Sector

Guidance Notes

56. Article 13 of the *Money Laundering Order* requires firms to apply on-going monitoring throughout the course of a business relationship and take steps to be aware of transactions with heightened *money laundering* and *the financing of terrorism* risks. The *Proceeds of Crime Law* requires firms to report suspicious transactions and activity (see Section 8 of this Handbook).

57. Firms should be alert in particular to alterations in instructions or who is instructing them where either instructions change or the client changes. The obligation to re-conduct *CDD* may well arise.

58. In relation to on-going monitoring, law firms should have regards to the warning signs contained in Sections 2.3.1.1 and 3.3.4 of this Handbook, where law firms may become vulnerable to *money laundering* or the *financing of terrorism*. These warning signs apply just as much to on-going relationships as to circumstances that may arise at the start of a business relationship.

[2] https://www.jerseyfsc.org/media/1721/banking-aml-sanctions-summary-findings-2014.pdf