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 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 *relevant person* 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 customer activity.
4. The requirement to keep documents, data or information up to date and relevant is discussed at Section 3.4 of the *AML/CFT 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 customers. 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:*

Deleted: 12 June 2019

a. *Complex or unusually large transactions;*

b. *Unusual patterns of transactions, which have no apparent economic or lawful purpose; or*

c. *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:*

a. *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*

b. *Business relationships or transactions are with a person:*

i. subject to measures under law applicable in Jersey for the prevention and detection of money laundering,

ii. connected with an organization that is subject to such measures, or

iii. 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 *relevant person* **monitors** all customer transactions and activity in order to **recognise notable transactions or activity,** i.e. those that:

› Are inconsistent with the *relevant person's* knowledge of the customer (unusual transactions or activity);

› Are complex or unusually large;

› Form part of an unusual pattern; or

› Present a higher risk of *money laundering* or *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 *relevant person* to also scrutinise customer activity (though this will already be the effect of *policies and procedures* required by Article 11(3)(a)(iii) of the *Money Laundering Order*). This is particularly relevant where a business relationship does not involve transactions, e.g. where a *relevant person* gives investment advice or acts as a director to a company, but will be relevant also in a transaction-based business relationship.

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

14. Sections 3 and 4 of the *AML/CFT Handbook* address the capturing of sufficient information about a customer that will allow a *relevant person* to prepare and record a customer business and risk profile which will provide a basis for recognising notable transactions or activity.

Deleted: 12 June 2019

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 customer, or with the normal business activities for the type of product or service that is being delivered.

16. Where a *relevant person's* customer base is homogeneous, and where the products and services provided to customers result in uniform patterns of transactions or activity, e.g. deposit-taking activity, it will be more straightforward to establish parameters to identify usual transactions and unusual activity. However, where each customer is unique, and where the product or service provided is bespoke, e.g. acting as trustee of an express trust, a *relevant person* will need to tailor monitoring systems to the nature of its business and facilitate the application of additional judgement and experience to the recognition of unusual transactions and activity. For such businesses, appropriate staff training in the recognition of unusual transactions and activity is vital, and will often already be necessary in order to satisfy fiduciary responsibilities placed on the *relevant person* under other legislation. For example, the approval of a transaction for a discretionary trust will involve two or three senior people in a person carrying on trust company business.

17. **Higher risk transactions or activity** may be recognised by developing a set of "red flags" or indicators which may indicate *money laundering* or *financing of terrorism*, based on a *relevant person's* understanding of its business, its products and its customers (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 *relevant person'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 customer business and risk profile, but on occasions this examination will involve requesting additional information from a customer.

21. Notable transactions or activity may indicate *money laundering* or *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 *financing of terrorism* is addressed in Section 8 of the *AML/CFT Handbook*.

22. Scrutiny may involve both **real time** and **post event** monitoring. Real time monitoring will focus on transactions and activity when information or instructions are received from a customer, before or as the instruction is processed. Post event monitoring may involve end of day, weekly, monthly or annual reviews of customer transactions and activity. Real time monitoring of transactions and activity will more effectively reduce a *relevant person's* exposure to *money laundering* and *financing of terrorism*. Post event monitoring may be more effective at identifying unusual patterns.

23. Monitoring may involve **manual** and **automated** procedures. Automated monitoring procedures may add value to manual procedures by recognising transactions or activity that fall outside set parameters. This will be particularly so where a *relevant person* processes large

Deleted: 12 June 2019

volumes of customer transactions which are not subject to day to day oversight. However, automated monitoring procedures may not be appropriate in cases where there is close day to day overview of a business relationship, e.g. where a *relevant person* carries on trust company business, where the subsequent preparation of financial statements and periodic review of a business relationship may be expected to highlight notable transactions and activity.

24. The examination of notable transactions or activity may be conducted either by customer facing employees, or by an independent reviewer. In any case, the examiner must have access to all customer records.

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

26. In order to recognise *money laundering* and *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 the *AML/CFT 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 *relevant person's* knowledge of the customer, including the customer's business and risk profile.

28. A *relevant person* 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 *relevant person* 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 *relevant person* must examine, as far as possible, their background and purpose and set forth its findings in writing.

Guidance Notes

30. A *relevant person* 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 customer instructions are put into effect); and
- Whether it is possible to establish appropriate standardised parameters for automated monitoring.

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

- **Customer business and risk profile** - see Section 3.3.5 of the *AML/CFT Handbook*.
- **"Red flags" or indicators of higher risk** - that reflect the risk that is present in the *relevant person's* customer base – based on its business risk assessment (refer to Section 2.3.1 of the *AML/CFT Handbook*), information published from time to time by the *Commission* or *JFCU*, e.g. findings of supervisory and themed examinations and typologies, and information published by reliable and independent third parties.

Deleted: 12 June 2019

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

32. A *relevant person* may demonstrate that *CDD policies and procedures* are appropriate if **examination** of notable transactions or activity includes:
    - Reference to the customer'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. A *relevant person* may demonstrate that *CDD* and reporting *policies and procedures* are effective if **post-examination** of notable transactions or activity it:
    - Revises, as necessary, its customer's business and risk profile.
    - Adjusts, as necessary, its monitoring system e.g. refines monitoring parameters, enhances controls for more vulnerable products/services/business units; and
    - Considers whether its knows, suspects or has reasonable grounds for suspecting that another person is engaged in *money laundering* or *financing of terrorism*, or that any property constitutes or represents the proceeds of criminal conduct.

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

Overview

34. 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 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 *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.**
35. 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 person or organization.**
36. As a part of its on-going monitoring procedures, a *relevant person* will establish appropriate procedures to **monitor** all customer transactions and activity in order to **recognise** whether any business relationships or one-off transactions are with such a person.
37. 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 the *AML/CFT Handbook*.
38. There is not a statutory requirement to **examine**, or have *policies and procedures* in place to examine, business relationships or transactions with a **sanctioned person, organization,**

Deleted: 3A)

Deleted: 12 June 2019

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.

AML/CFT Codes of Practice

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

40. A *relevant 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.

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

Guidance Notes

42. A *relevant person* 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 customer instructions are put into effect); and
- Whether it is possible to establish appropriate standardised parameters for automated monitoring.

43. A *relevant person* 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 -** Customer business and risk profile in line with Section 3.3.5 of the *AML/CFT Handbook*.
- **Enhanced risk states** - Appendix D1 of the *AML/CFT Handbook*.
- **Sanctioned countries** - Appendix D2 of the *AML/CFT Handbook* (Source 6 only).

44. A *relevant person* 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 customer'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.

45. A *relevant person* 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 customer's business and risk profile.
- Adjusts, as necessary, its monitoring system e.g. refines monitoring parameters, enhances controls for more vulnerable products/services/business units; and

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

Deleted: 12 June 2019

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

6.3 Automated Monitoring Methods

Overview

46. As noted in paragraph 23 above, 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.

47. **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 customer's business and risk profile.

48. Large or more complex *relevant persons* 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.

49. What constitutes unusual behaviour by a customer 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 *relevant person*.

50. Where an automated monitoring method (group or otherwise) is used, a *relevant person* 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).

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

52. 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 customers may be particularly effective. However, where a *relevant person* 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 *relevant person*:

› 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.

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

Deleted: 12 June 2019

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"

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

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

Deleted: 12 June 2019