5.6 ON-GOING MONITORING OF TRANSACTIONS & ACTIVITY

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. This section explains the measures required to demonstrate compliance with the requirement to scrutinise transactions and also sets a requirement to scrutinise customer activity.

3. 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

4. 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. See Article 3(3)(b) of the Money Laundering Order.

5. Article 13 of the Money Laundering Order requires a relevant person to apply on-going monitoring throughout the course of a business relationship.

6. Article 11(1) and (2) 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:
     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 that does not apply, or insufficiently applies, the FATF Recommendations [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 connected with a country or territory that is subject to measures 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 UN.

7. 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

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

9. 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.

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

11. In addition to the scrutiny of transactions, as required by the Money Laundering Order, this section introduces a general requirement 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.

12. 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.

13. 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 develop, prepare and record a customer **business and risk profile** of expected activity to which will provide a basis for recognising unusual activity and **notable transactions** and identify unusual activity or transactions, which may indicate money laundering or financing of terrorism or activity.

14. This section requires a relevant person to monitor business relationships and to apply scrutiny to unusual and higher risk activity or **Unusual transactions** and also to specific higher risk activity, so that money laundering or the financing of terrorism may be identified and, where possible, prevented. An effective monitoring system requires a relevant person to identify unusual and higher risk activity, to maintain up to date customer due diligence information and to scrutinise transactions to determine whether there is a rational explanation for the activity or **activity, unusually large transactions** identified. The scrutiny of activity and unusual patterns of transactions may involve requesting additional customer due diligence information.

15. For some customers, a complete customer profile and appropriate risk assessment may only become evident once the relationship has been established, making monitoring of customer activity and **or activity may be recognised where** transactions key to obtaining a complete understanding of business relationships.

16. Unusual activity or transactions may be identified as activity that is inconsistent with the expected pattern of **transactions or expected activity** within for a particular relationship/customer, or with the normal business activities for the type of product or service that is being delivered.

17. Where a relevant person’s customer base is homogeneous, and where the products and services provided to customers result in uniform patterns of **activity or 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 identification 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.
16. **Monitoring procedures**. **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).

17. **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).

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

19. 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.

20. **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.

21. Scrutiny may involve both **real time** and **post event** monitoring. Real time monitoring will focus on activity and 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 activity and transactions and activity. Real time monitoring of transactions and activity will be more effective at reducing terrorism risk. Post event monitoring may be more effective at identifying unusual patterns of customer activity.

22. Monitoring may involve **manual** and **automated** procedures. Automated monitoring procedures may add value to manual procedures (particularly for businesses with large volumes of customer transactions) by producing exception reports identifying transactions or activity that fall outside a set of parameters for usual activity. This will be particularly so where a relevant person processes large volumes of customer transactions which are not subject to daily oversight. However, automated monitoring procedures will depend on the relevance of the parameters to the nature undertaken by a relevant person’s 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.

23. Unusual or higher risk activity may indicate money laundering or financing terrorism activity where there is no apparent economic or visible lawful purpose.

24. Where monitoring indicates possible money laundering or financing terrorism activity, and the process of undertaking identification procedures is managed without due care, contact between a relevant person and an employee (or his advisors) could unintentionally lead to records.

9. Reporting of knowledge, suspicion, or reasonable grounds for knowledge or suspicion of money laundering and financing of terrorism is addressed in...

10. **Sufficient guidance and training of staff** is essential to enable them to recognise notable transactions and activity. 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 notable transactions and activity.
In order to recognise money laundering and financing terrorism activity, requirements for terrorism, employees will need to have a good level of awareness of both and to have received training. Awareness raising and training in the recognition and handling of suspicious activity are covered in .

This section should be read and understood in conjunction with , , .

### 6.2 OBLIGATION TO MONITOR

**SECTION 9 STATUTORY REQUIREMENTS**

25. of the Money Laundering Order requires a relevant person to scrutinise transactions undertaken throughout .

**AML/CFT CODES OF PRACTICE**

26. In addition to , scrutiny of transactions on-going monitoring must also involve scrutinising activity in respect 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.

27. provides that policies for the application of customer due diligence procedures are appropriate having regard to the degree of risk of money laundering. The policies referred to include those:

- Which provide for the identification and scrutiny of:
  a. Complex or unusually large transactions;
  b. Unusual patterns of transactions, which have no apparent economic or lawful purpose;
  c. Business relationships and transactions connected with jurisdictions that do not, or insufficiently, apply the FATF Recommendations;
  d. Business relationships and transactions with persons or jurisdictions that are subject to UN or EU sanctions and measures or measures imposed by one or more countries for insufficient or non-existent application of FATF Recommendations; or
  e. 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 specify additional procedures where products and transactions are susceptible to anonymity and;

- Which determine whether a customer is a PEP.

28. The monitoring procedures must require more intensive identification and scrutiny of higher risk customers (including PEPs) and higher-risk products/services:

29. The monitoring procedures must:

### REGULATORY REQUIREMENTS

15. A relevant person must, as a part of its ongoing identification procedures, establish and maintain appropriate customer activity and transaction monitoring consistent policies and procedures that scrutinise which provide for the activity and transactions of its customers.

16. The monitoring procedures must require more intensive identification and scrutiny of higher-risk customers (including PEPs) and higher-risk products/services.

17. The monitoring procedures must:
Part 1: Section 6 – On-going monitoring: scrutiny of transactions and activity

- involve a relevant person applying its understanding of its business (i.e. the outcome of its business risk assessment) to determine the nature of usual activity and its expectations for unusual and higher risk activity and transactions;

- be designed to result in the identification of unusual and higher risk activity or transactions;

- require that, in particular, special attention is paid to specific higher risk activity and transactions (see 18 below);

- require the examination of any unusual or higher risk activity or transaction by an appropriate person to determine the background and purpose of the activity or transaction;

- in connection with the above examination, involve the collection of additional information (where appropriate);

- establish whether there is a rational explanation (an apparent economic or visible lawful purpose) for the unusual or higher risk activity or transaction and document these findings in writing; and

- result in appropriate action being taken as a result of the findings of the above procedures.

18. When conducting monitoring procedures, the following are to be considered to be higher risk activity and transactions:

- complex transactions;

- unusual large transactions;

- Complex or unusually large activity;

- Unusual patterns of transaction activity, which have no apparent economic or visible lawful purpose; and

- Any other activity and transactions: (i) connected with jurisdictions which do not, or insufficiently apply, the FATF Recommendations; or (ii) nature of which are causes, the subject of UN or EU countermeasures; and

- activity and transactions that may be conducted with persons who are the subject of UN or EU sanctions and measures.

19. A relevant person must have policies and procedures in place to address any specific risks associated with customer relationships established where the customer was not physically present for identification purposes (i.e. non-face-to-face). Be related to money laundering or the financing of terrorism.

GUIDANCE NOTES

20. Appropriate monitoring systems. In determining the nature of the monitoring, a relevant person may demonstrate that CDD policies and procedures are appropriate for a business, a relevant person may have where scrutiny of transactions and activity has regard to the following factors:

- Its business risk assessment:
  - (including the size and complexity of its business);
  - its ability 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 unusual activity; and
  - the automated monitoring procedures that already exist to satisfy other business needs.
30. Identifying unusual activity: A relevant person may demonstrate that CDD policies and procedures are appropriate where the following are used to recognise notable transactions. Appropriate factors to consider 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 determining whether activity or 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.

21. “Red flags” or indicators of complex transactions are unusual include: 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.

- The expected frequency, size, volume and origin/destination of customer funds whether specific to an individual customer, or for a generic customer type or product type; and

- The presence of risk factors specific to the nature of the activity and customer base of the relevant person. A relevant person should determine risk factors based on its knowledge of its customer base (refer to ) and should have regard to typologies (whether external or developed from its own experiences) relevant to the nature of business activities.

31. Examining unusual and higher risk activity. 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.

22. A relevant person may demonstrate that it is appropriately examining unusual and higher risk activity and transactions where it:

- Reviews the identified activity/transaction in light of the customer risk assessment and the customer due diligence information that it holds;

- Makes further enquires to obtain any further information required to enable a determination as to whether the activity/transaction has a rational explanation; and

- Considers the activity or transaction in the context of any other relationships connected with the customer.

23. The examination of unusual and higher risk activity or transactions may be conducted either by customer facing staff, or by an independent reviewer. In any case, the reviewer must have access to relevant customer due diligence information, and the enquiries made and the conclusions reached by the reviewer must be appropriate. Refer to for record keeping requirements in relation to the CDD and reporting policies and procedures are effective if post-examination of higher risk activity and notable transactions or activity it:

24. Appropriate follow up action may include:

- Updating customer due diligence information to record the results of the enquiries made;

- Reviewing the appropriateness of the customer risk assessment in light of the unusual activity and/or additional customer due diligence information obtained;
• Considering whether tuning of the Revises, as necessary, its customer’s business and risk profile.

• Adjusts, as necessary, its monitoring system to result in further staff training in the identification of unusual or higher risk activity and transactions, refinement of the monitoring system’s parameters, enhancements of controls for more vulnerable products/services/business units; and

• Applying increased levels of monitoring to particular relationships;

• Where the activity or transaction does not have a rational explanation, considering whether the circumstances require a suspicious activity report to be submitted to the relevant person’s MLRO.(

25. In line with enhanced due diligence requirements for higher risk customers (more intensive scrutiny of customer activity and transactions may involve, for example:

• More frequent review and updating of customer due diligence information;

• More regular review of customer activity and transactions against the customer’s expected activity profile;

• The application of lower thresholds for the monitoring of customer activity and transactions;

• Customer reviews being conducted by persons not directly involved in managing customer relationships.

6.2.1 Countries and territories that do not, or insufficiently, apply FATF Recommendations

OVERVIEW

• 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

OVERVIEW

33. The risk that a business relationship is tainted by funds that are the proceeds of crime or terrorist funding can enter the financial system, and remain undetected. For example, where the requirements for customer due diligence 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 transactions are with a person connected with such countries or territories.

34. As a part of crime or terrorist funding can enter the financial system, and remain undetected.
26. 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(3A) weak, or where there is an absence of the Money Laundering Order. See Section 7.5 of transparency or regulatory measures for express trusts, legal bodies or legal arrangements of the AML/CFT Handbook.

REGULATORY REQUIREMENT

36. Countries and territories in There is not a statutory requirement to examine, or have policies and procedures in place to examine, business relationships or transactions with a sanctioned 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 is published on the Commission’s website.

AML/CFT CODES OF PRACTICE

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

38. 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.

GUIDANCE NOTES

39. 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.

40. 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 are to be treated as countries and territories that do not apply, or insufficiently apply, the FATF Recommendations under Article 15 of the Money Laundering Order of the AML/CFT Handbook.
- Sanctioned countries - Appendix D2 of the AML/CFT Handbook (Source 6 only).

41. 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.

42. 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.

---

http://www.jerseyfsc.org/the_commission/sanctions/index.asp
• 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.

5.3
6.3 AUTOMATED MONITORING METHODS

OVERVIEW

28. As noted in paragraph 22 above, automated monitoring methods may be effective in
recognising unusual and higher risk activity or notable transactions and activity, and business
relationships and transactions with persons connected to enhanced risk states and sanctioned
countries and territories.

29. Exception procedures and 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 the nature of a customer’s
business and level of activity and the risk profiles of the relationships that are being monitored.

30. Large or more complex relevant persons may also use automated monitoring systems 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.

46. 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.

47. Where an automated monitoring system (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).

50. Use of automated monitoring methods does not remove the requirement 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 activity and transactions that do not seem to make sense, cannot be automated.

49. In the case of monitoring activity and transactions that may be conducted with individuals who are
the subject of countermeasures, applied under UN and EU sanctions and measures, 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.

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

<table>
<thead>
<tr>
<th>Variation</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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”


Name variations  “Chang” instead of “Jang”

51. Further information on screening practices may be found in a report published by the Commission in August 2014\(^2\).