

6 ONGOING MONITORING – SCRUTINY OF TRANSACTIONS & ACTIVITY

6.1 Overview

1. This section outlines the statutory provisions concerning 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 *supervised person* will still need to consider reporting provisions summarised in Section 8 of this Handbook. For example 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 sets a requirement to scrutinise *customer* activity.
4. The requirement to keep documents, data or information up-to-date and relevant is covered at Section 3.4 of this Handbook.

6.2 Obligation to perform on-going monitoring

Statutory requirements (paraphrased wording)

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 of the Money Laundering Order requires a relevant person to 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: <#>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](#).

Deleted: of Section

Deleted: ;

Deleted: relevant

Deleted: , e.g.

Deleted: also

Deleted: discussed

Deleted: the AML/CFT

Deleted:

Deleted: .

Deleted: (1)

Deleted: establish and

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(3)(a), "scrutiny" includes scrutinising the background and purpose of transactions and activities.

Deleted: Handbook for regulated financial services businesses¶
Part 1: Section 6 – On-going monitoring: scrutiny of transactions and activity¶

Deleted:

Deleted: ;

Deleted: ;

Deleted: ;

Deleted: ,

Deleted: ,

Deleted: 1

6.2.1 Scrutiny of transactions and activity

B

Overview

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

10. **Firstly**, a supervised person monitors all customer transactions and activity in order to recognise notable transactions or activity, i.e. those that:

are inconsistent with the supervised 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 the financing of terrorism.

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

12. In addition to the scrutiny of transactions as required by the Money Laundering Order, AML/CFT Codes of Practice in this section also require a supervised person to scrutinise customer activity. This is not just relevant to transaction-based business relationships, but also to business relationships that do not involve transactions, e.g. where a supervised person gives investment advice, or acts as a director to a company.

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

Deleted: :

Deleted: relevant

Deleted: relevant

Deleted: activity);

Deleted: ;

Deleted: ;

Deleted: , including the background and purpose of such transactions and activity.

Deleted: ,

Deleted: set

Deleted: requires

Deleted: relevant

Deleted: also

Deleted: (though this will already be the effect of policies and procedures required by Article 11(3)(a)(iii) of the Money Laundering Order).

Deleted: particularly

Deleted: where a

Deleted: relationship does

Deleted: relevant

Deleted: , but will be relevant also in a transaction-based business relationship.

Deleted: relevant

Deleted: and

Deleted: and

Deleted: or

Deleted: This version is effective from: 12 February 2020

14. Sections 3 and 4 of this Handbook address the capturing of sufficient information about a customer, allowing a supervised person to record a **customer business and risk profile** which provides a basis for recognising notable transactions/activity, which may indicate money laundering or the financing of terrorism.
15. Additional or more frequent monitoring is required for relationships that have been designated as carrying a higher risk of money laundering or the financing of terrorism.
16. With reference to what has been recorded in the customer business and risk profile, unusual transactions/activity, unusually large transactions/activity, and unusual patterns of transactions/activity may be recognised where transactions or activity are inconsistent with the expected pattern of transactions, the expected activity for a particular customer, or the normal business activities for the type of product or service that is being delivered.
17. Where a supervised person's customer base is homogeneous, and where the products and services provided to customers result in uniform patterns of transactions or activity, it may be easier to establish parameters to identify usual transactions/activity. For example when dealing with local property transactions being passed before the Royal Court or undertaking deposit-taking activities.
18. Where each customer is unique, and where the product or service is bespoke, a supervised 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.
19. For some customers, additional information may only become evident during the course of the business relationship (i.e. whilst acting for the customer), leading to a revised profile and risk assessment. This requires particular diligence and care when updating documents, data or information and when scrutinising and monitoring customer activity and transactions. In these cases, appropriate staff training in the recognition of unusual transactions and activity is vital, as are relevant systems and controls.
20. **Higher risk transactions/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 supervised person's understanding of its business, products and customers (i.e. the outcome of its business risk assessment – Section 2.3.1).
21. **Complex transactions/activity** may be recognised by developing a set of indicators, based on a supervised person's understanding of its business, its products and its customers (i.e. the outcome of its business risk assessment – Section 2.3.1).
22. External data sources and media reports may also assist with the identification of notable transactions and activity.
23. Where notable transactions or activity are **recognised**, they 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. 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 and on occasion this examination will involve requesting additional information from a customer.

Deleted: Handbook for regulated financial services businesses¶
Part 1: Section 6 – On-going monitoring: scrutiny of transactions and activity¶

Deleted: the AML/CFT

Deleted: that will allow a *relevant*

Deleted: prepare and

Deleted: will provide

Deleted: or activity.

Deleted: Unusual transactions

Deleted: or

Deleted: or

Deleted: or

Deleted: ,

Deleted: with

Deleted: *relevant*

Deleted: e.g. deposit-taking activity,

Deleted: will

Deleted: more straightforward

Deleted: and unusual activity. However,

Deleted: provided

Deleted: e.g. acting as trustee of an express trust,

Deleted: *relevant*

Deleted: 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.

Deleted: or

Deleted: “

Deleted: flags”

Deleted: *relevant*

Deleted: its

Deleted: its

Deleted: or

Deleted: *relevant*

Deleted: will

Deleted: such transactions or activity

Deleted: recognised

Deleted: , but

Deleted: occasions

Deleted: This version is effective from : 12 February 2020

24. 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*.
25. **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 *supervised person's* exposure to *money laundering* and *the financing of terrorism*. Post event monitoring may be more effective at identifying unusual patterns.
26. 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 *supervised person* processes large volumes of *customer* transactions which are not subject to day-to-day oversight. However, *where* automated monitoring procedures *are* not in place, *monitoring is likely to be most effective when undertaken on a case-by-case basis by customer facing staff, administration and accounts staff, whom* may be expected to *spot and* highlight notable transactions *or* activity.
27. The **examination** of notable transactions or activity may *also* be conducted either by *customer* facing employees, or by an independent reviewer. In any case, the examiner must have access to all *customer* records.
28. The results of an examination should be recorded and *appropriate* action taken. Refer to Section 10 of *this Handbook* for record-keeping requirements in relation to the examination of notable transactions and activity.
29. 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. *Refer to Section 9 of this Handbook for raising of awareness and training.*
30. *Where on-going monitoring indicates possible money laundering or the financing of 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

31. 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 *supervised person's* knowledge of the *customer*, including the *customer's* business and risk profile.
32. A *supervised 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 *supervised person* to regard it as particularly likely to be related to *money laundering* or the *financing of terrorism*.

Deleted: Handbook for regulated financial services businesses¶
 Part 1: Section 6 – On-going monitoring: scrutiny of transactions and activity¶

Deleted: the AML/CFT

Deleted: relevant

Deleted: relevant

Deleted: may

Deleted: be appropriate

Deleted: cases where there

Deleted: close day

Deleted: day overview of a business relationship, e.g. where a relevant person carries

Deleted: trust company business, where the subsequent preparation of financial statements

Deleted: periodic review of a business relationship

Deleted: and

Deleted: as appropriate.

Deleted: the AML/CFT

Deleted: some

Deleted: Awareness

Deleted: are covered

Deleted: 9

Deleted: the AML/CFT

Moved down [1]: AML/CFT Codes of Practice¶

Deleted: relevant

Deleted: relevant

Deleted: ;

Deleted: ;

Deleted: relevant

Deleted: This version is effective from: 12 February 2020

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

Guidance notes

34. A supervised 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);
 - the nature of its business and services
 - whether it is practicable to monitor transactions or activity in real time (i.e. before customer instructions are put into effect);
 - whether it is possible to establish appropriate standardised parameters for automated monitoring; and
 - the monitoring procedures that already exist to satisfy other business needs.
35. A supervised 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 this Handbook;
 - 'red flags' or indicators of higher risk – that reflect the risk that is present in the supervised person's customer base – based on its business risk assessment (refer to Section 2.3.1 of this Handbook), information published from time to time by the JFSC or 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 and activity - based on its business risk assessment (refer to Section 2.3.1 of this Handbook), information published from time to time by the JFSC or JFCU, e.g. findings of supervisory and themed examinations and typologies, and information published by reliable and independent third parties.
36. A supervised 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**.

Case study:

- A supervised person may have a business relationship with a customer who previously advised that they had a modest source of funds.
- The customer then instructs the supervised person to purchase an asset, the value of which appears to be outside the means of the customer's source of funds, as currently understood.
- While the supervised person may be satisfied that it still knows the identity of the customer, as part of its on-going monitoring obligations, it would be appropriate to ask about the source

Deleted: Handbook for regulated financial services businesses¶
Part 1: Section 6 – On-going monitoring: scrutiny of transactions and activity¶

Deleted: *relevant*

Deleted: *relevant*

Deleted:);

Deleted:); and

Deleted: .

Deleted: *relevant*

Deleted: the AML/CFT

Deleted: .

Deleted: "Red flags"

Deleted: -

Deleted: *relevant*

Deleted: the AML/CFT

Deleted: *Commission*

Deleted: .

Deleted: "Red flags"

Deleted: the AML/CFT

Deleted: *Commission*

Deleted: *relevant*

Deleted: ;

Deleted:);

Deleted: *relevant*

Deleted: This version is effective from : 12 February 2020

of funds for this purchase. Depending on the customer's willingness to provide such information, and the answer that is provided, the supervised person's staff should also consider whether they:

are satisfied with the response

want further proof of the source of funds and/or

need to submit an internal SAR to the supervised person's MLRO.

37. A supervised 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. it refines monitoring parameters, enhances controls for more vulnerable products/services/business units 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 and transactions – Person connected with an enhanced risk state or sanctioned country

Overview

38. 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 one-off transaction is with a person or entity 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 UK, EU (in limited circumstances) or the UN,

39. 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 one-off transaction is with a person connected with an organisation subject to such measures or who is themselves subject to such measures.

40. As a part of its on-going monitoring procedures, a supervised person will establish and maintain appropriate policies and procedures to monitor all customer transactions and activity in order to recognise whether any business relationships or one-off transactions are directly or indirectly with such sanctioned persons, organisations or other parties.

41. 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.

Deleted: Handbook for regulated financial services businesses¶
Part 1: Section 6 – On-going monitoring: scrutiny of transactions and activity¶

Deleted: -

Deleted: .

Deleted: ;

Deleted: its

Deleted: -

Deleted: or Organization

Deleted: -

Deleted: ;

Deleted: EU

Deleted: - a sanctioned country or territory

Deleted: organization

Deleted: - a sanctioned person or organization.

Deleted: relevant

Deleted: with such a person

Deleted: the AML/CFT

Deleted: This version is effective from: 12 February 2020

42. There is not a statutory requirement to **examine**, or have *policies and procedures* in place to examine, *business relationships* or *one-off transactions* with a *designated person*, once they are recognised. This is because provisions in financial sanctions legislation must be followed. *Among other things*, such provisions may prohibit certain activities or require the property to be frozen. Further guidance is published on *the JFSC's website*.

AML/CFT Codes of Practice

43. On-going monitoring must involve **examining** transactions and activity recognised as being with a person connected with an *enhanced risk state*.
44. A *supervised 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*.
45. As part of its **examination** of the above transactions *and activity*, a *supervised person* must examine, as far as possible, their background and purpose and set forth its findings in writing.

Guidance notes

46. A *supervised 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)
 - the nature of its business and services*
 - whether it is practicable to monitor transactions or activity in real time (i.e. before *customer instructions* are put into effect)
 - whether it is possible to establish appropriate standardised parameters for automated monitoring *and*
 - the monitoring procedures that already exist to satisfy other business needs.*
47. A *supervised 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 *customers* – Business and risk profile in line with Section 3.3.5 of *this Handbook*
 - all *customers* – Adopting the UK's consolidated list as a comprehensive listing of *sanctions measures applicable in Jersey*
 - all *customers* – Considering methods of identifying possible indirect associations and connections that may exist between the *supervised person's customer* and any *sanctioned parties, and/or enhanced risk states, that will not immediately be obvious from screening of the UK's consolidated list*
 - enhanced risk states* - Appendix D1 of the *AML/CFT Handbook* *and*
 - sanctioned countries and territories* - Appendix D2 of the *AML/CFT Handbook* (Source 6 only).

Deleted: Handbook for regulated financial services businesses¶
Part 1: Section 6 – On-going monitoring: scrutiny of transactions and activity¶

Deleted: sanctioned

Deleted: , organization, country or territory

Deleted: Inter alia

Deleted: of listed persons

Deleted: ¹

Deleted: the Commission's website.

Deleted: AML/CFT Codes of Practice¶

Moved (insertion) [1]

Deleted: relevant

Deleted: relevant

Deleted: relevant

Deleted:);

Deleted:); and

Deleted: .

Deleted: relevant

Deleted: - Customer

Deleted: the AML/CFT

Deleted: .

Deleted: - Appendix D1

Deleted: .

Deleted: - Appendix D2

Deleted: This version is effective from : 12 February 2020

48. A supervised 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.
49. A supervised 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
 - 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.

Deleted: Handbook for regulated financial services businesses¶
Part 1: Section 6 – On-going monitoring: scrutiny of transactions and activity¶

Deleted: relevant

Deleted: ;

Deleted:);

Deleted: relevant

Deleted: .

Deleted: ;

6.3 Automated monitoring methods

Overview

50. Automated monitoring methods may be effective in recognising notable transactions and activity, and *business relationships* and *one-off transactions* with persons connected to *enhanced risk states* and sanctioned countries, territories and other sanctioned parties.
51. **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.
52. Large or more complex supervised persons may also use automated monitoring methods to facilitate the monitoring of significant volumes of transactions, or such as in an e-commerce environment, where the opportunity for human scrutiny of individual transactions is limited.
53. What constitutes unusual behaviour by a *customer* is often defined by the automated monitoring system selected by the supervised person. It is important that the system selected has an appropriate definition of 'unusual' and is in line with the nature of business conducted by the supervised person.
54. Where an automated monitoring method (group or otherwise) is used, a supervised 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)

Deleted: As noted in paragraph above,

Deleted: and

Deleted: .

Deleted: -

Deleted: -

Deleted: relevant

Deleted: -

Deleted: -

Deleted: system.

Deleted: will be

Deleted: one that

Deleted: relevant

Deleted: relevant

Deleted: ;

Deleted:);

Deleted: This version is effective from: 12 February 2020

how to use the system, e.g. making full use of guidance and the nature of its output (exceptions, alerts etc.).

55. Use of automated monitoring methods does not remove the need for a supervised 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.

56. 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 supervised 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 supervised person: understands which business relationships and transaction types are screened, understands the system's capacity for fuzzy matching (a 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 and records the basis for discounting alerts (e.g. false positives) to provide an audit trail.

57. 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"

58. Further information on screening practices may be found in reports published by the JFSC in August 2014 and May 2021. Additional guidance is also available on the JFSC's website.

6.4 Money laundering warning signs

Overview

59. Article 13 of the Money Laundering Order requires a supervised person 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 a supervised person to report suspicious transactions and activity (see Section 8 of this Handbook).

Deleted: Handbook for regulated financial services businesses¶
Part 1: Section 6 – On-going monitoring: scrutiny of transactions and activity¶

Deleted: ;

Deleted:).

Deleted: relevant

Deleted: ,

Deleted: relevant

Deleted: relevant

Deleted: .

Deleted: "

Deleted: " (

Deleted:).

Deleted: .

Deleted: "

Deleted: "

Deleted: a report

Deleted: Commission

Deleted: August 2014²

Deleted: This version is effective from : 12 February 2020

Deleted: Handbook for regulated financial services businesses¶
Part 1: Section 6 – On-going monitoring: scrutiny of transactions and activity¶

60. This section highlights a number of general warning signs for supervised persons to help them decide whether there may be reasons for concern or the basis for a reportable suspicion.

61. In relation to on-going monitoring, a supervised person should have regard both to the warning signs contained in the relevant sector-specific sections of this Handbook and the general indicators set out below, where they may become vulnerable to money laundering or the financing of terrorism. These warning signs apply to on-going relationships just as much as to circumstances that may arise at the start of a business relationship.

62. Because money launderers and terrorist financiers are always developing new techniques, no list of examples can be fully comprehensive. However, the following are some key factors indicating activity or transactions which might heighten a customer's risk profile, or give cause for concern.

6.4.1 Secretive customers

B

63. Whilst face-to-face contact with customers is not always possible, an excessively obstructive or secretive customer may be a cause for concern. Consideration should be given as to whether customers who demand strict confidentiality relating to their financial and business affairs, or are reluctant to answer due diligence questions are evading tax or seeking to mask the true beneficial ownership of their assets.

6.4.2 Unusual instructions

B

64. Instructions that are unusual in themselves, or that are unusual for the supervised person or the customer may give rise to concern, particularly where no rational or logical explanation can be given. Be wary of:

loss-making transactions where the loss is avoidable

dealing with money or property when there are suspicions that it is being transferred to avoid the attention of either a trust in a bankruptcy case, a revenue authority (e.g. HMRC, Revenue Jersey etc), or a law enforcement agency

complex or unusually large transactions, particularly where underlying beneficial ownership is difficult to ascertain and/or where the underlying transactions have been conducted in cash

unusual patterns of transactions which have no apparent economic purpose particularly those where a number of jurisdictions and different entities are involved for no logical business reason

funds that are being switched between investments or jurisdictions for no apparent reason

use of shell companies, blind trusts or other structures that are merely being used as a front for other activities

excessive use of off-balance sheet transactions or activity.

Deleted: This version is effective from: 12 February 2020

6.4.2.1 Instructions outside the supervised person's area of expertise

65. Taking on work which is outside the supervised person's normal range of expertise can present additional risks because a money launderer or terrorist financier might be using the supervised person to avoid answering too many questions. A supervised person inexperienced in the provision of a particular product or service might be influenced into taking steps which a more experienced business would not contemplate. Supervised persons should be wary of highly paid niche areas of work in which they have no background, but in which the customer claims to be an expert.
66. If the customer is not resident in Jersey, supervised persons should satisfy themselves that there is a genuine legitimate reason why they have been approached. For example, have the supervised person's services been recommended by another customer? Making these types of enquiries makes good business sense, as well as being a sensible AML/CFT check.

6.4.2.2 Changing instructions

67. Instructions that change unexpectedly or significantly might be suspicious, especially if there seems to be no logical reason for the changes. This may also be the case where the person making the instruction changes. The obligation to re-conduct CDD may well arise.
68. The following situations could give rise to cause for concern:
- a customer deposits funds into a supervised person's client account for a transaction, but then ends the transaction for no apparent reason
 - a customer advises that funds are coming from one source and at the last minute the source changes and
 - a customer unexpectedly requests that money received into a supervised person's client account be sent back to its source, to the customer or to a third party.

6.4.3 Use of client accounts

69. Client accounts should only be used to hold customer money for legitimate transactions for customers, or for another proper legal purpose. Putting criminal money through a supervised person's client account can make it appear clean, whether the money is sent back to the customer, on to a third party, or invested in some way. Introducing cash into the banking system can become part of the placement stage of money laundering. Therefore, the use of cash for non-cash based businesses is often a warning sign.

6.4.3.1 Source of funds

70. If funding is from a source other than the customer, supervised persons may need to make further enquiries, especially if the customer has not previously advised that a third party would be involved. When considering whether to accept funds from a third party, supervised persons should ask how and why the third party is helping with the funding.

Deleted: Handbook for regulated financial services businesses¶
Part 1: Section 6 – On-going monitoring: scrutiny of transactions and activity¶

71. A supervised person must always be alert to warning signs and in some cases will need to seek more information.

6.4.4 Money laundering offences factors

B

6.4.4.1 Intent

B

72. Except for certain strict liability offences, criminal conduct requires an element of criminal intent which means that an offender must know or suspect that an action or property is criminal. Conduct which is an innocent error or mistake may be criminal where it constitutes a strict liability offence, but will not also be money laundering.

73. If an individual or supervised person knows or believes that a customer is acting in error, the customer may be approached and the situation and legal risks explained to them. However, once the criminality of the conduct is explained to the customer, they must bring their conduct (including past conduct) promptly within the legislation to avoid a money laundering offence being committed. Where there is uncertainty about the legal issues that are outside the competence of the supervised person, customers should be referred to an appropriate specialist or legal adviser.

74. If there are reasonable grounds to suspect that a customer knew or suspected that their actions were criminal, a report must be made. Even if the customer does not have the relevant intent, but the supervised person is aware that there is criminal property, consideration needs to be given to whether a report has to be made to the JFCU.

75. In all circumstances, supervised persons should be mindful of committing a ‘tipping-off’ offence as set out at Article 35(4) of the Proceeds of Crime Law. See Section 8.5 of this Handbook for more information.

6.4.4.2 Holding of funds

B

76. Supervised persons who choose to hold funds on behalf of a customer should consider the checks to be made about the funds they intend to hold before the funds are received. Consideration should be given to conducting CDD measures on all those on whose behalf the funds are being held.

77. Particular consideration should be given to any proposal that funds are collected from a number of individuals whether for investment purposes or otherwise. This could lead to wide circulation of client account details and payments being received from unknown sources.

6.4.4.3 Factors arising from action by the customer or its controllers

B

78. Where a customer is actively involved in money laundering, the signs may include:
unusually complex corporate structure where complexity does not seem to be warranted
complex or unusual transactions, possibly with related parties
transactions with little commercial logic taking place in the normal course of business (such as selling and re-purchasing the same asset)

Deleted: This version is effective from: 12 February 2020

transactions conducted outside of the normal course of business or where the method of payment/receipt is not usual business practice, such as wire transfers or payments in foreign currency

transactions where there is a lack of information or explanation, or where explanations are unsatisfactory

transactions that are undervalued or overvalued, including double billing

transactions with companies whose identity or beneficial ownership is difficult to establish

abnormally extensive or unusual related party transactions

unusual numbers of cash transactions for substantial amounts or a large number of small transactions that add up to a substantial amount

payment for unspecified services or for general consultancy services and

long delays in the production of company or trust accounts for no apparent reason.

6.4.4.4 Where the customer may be unknowingly a party to money laundering

79. There may be occasions where **the customer has been duped by its own customer** into providing assistance or a vehicle for *money laundering* or the *financing of terrorism*. Warning signs may be:

unusual transactions without an explanation, or a pattern of trading with a customer of the supervised person's customer that is different from the norm

request for settlement of sales in cash

the customer's customer setting up a transaction that appears to be of no commercial advantage or logic

the customer's customer requesting special arrangements for vague purposes

unusual transactions with companies registered in other jurisdictions

request for settlement to bank accounts or jurisdictions which would be unusual for a normal commercial transaction or

excessive overpayment of accounts, subsequently requesting a refund.

6.4.5 Administration of estates

80. A deceased person's estate is very unlikely to be actively utilised by criminals as a means for *laundering* their funds; however, there is still a risk of *money laundering* for those working in this area.

81. When winding up an estate, there is no blanket requirement that *supervised persons* should be satisfied about the history of all of the funds which make up the estate under administration. However, *supervised persons* should be aware of the factors which can increase *money laundering* risks and consider the following:

where estate assets have been earned in a foreign jurisdiction, supervised persons should be aware of the wide definition of criminal conduct in the Proceeds of Crime Law and

where estate assets have been earned or are located in a higher risk country or territory, supervised persons may need to make further checks about the source of those funds.

82. Supervised persons should be alert from the outset and monitor throughout so that any disclosure can be considered as soon as knowledge or suspicion is formed and problems of delayed consent can be avoided.

83. Supervised persons should bear in mind that an estate may include criminal property. An extreme example would be where the supervised person knows or suspects that the deceased person was accused or convicted of acquisitive criminal conduct during their lifetime.

84. If supervised persons know or suspect that the deceased person improperly claimed welfare benefit or had evaded the due payment of tax during their lifetime, criminal property will be included in the estate and so a money laundering disclosure may be required.

85. Relevant local laws will apply before assets can be released. For example, a grant of probate will normally be required before UK assets can be released. Supervised persons should remain alert to warning signs, for example if the deceased or their business interests are based in a higher risk country or territory.

86. If the deceased person is from another jurisdiction and a lawyer is dealing with the matter in the home country, supervised persons may find it helpful to ask the lawyer for information about the deceased to gain some assurances that there are no suspicious circumstances surrounding the estate. The issue of the tax payable on the estate may depend on the jurisdiction concerned.

6.4.6 Charities

B

87. While the majority of charities are used for legitimate reasons, they can be used as vehicles for money laundering or the financing of terrorism.

88. Supervised persons acting for charities should consider their purpose and the organisations they are aligned with. If money is being received on the charity's behalf from an individual or a company donor, or a bequest from an estate, supervised persons should be alert to unusual circumstances, such as receipt of unexpectedly large sums of money.

6.4.7 Taxation matters

B

89. There are a number of tax offences which can give rise to the proceeds of crime and therefore require the submission of a SAR to the JFCU. A supervised person is not required to be an expert in criminal law, but they would be expected to recognise activity which might suggest the customer is involved in tax evasion.

90. There will, however, be no question of criminality where the customer has adopted in good faith, honestly and without mis-statement, a technical position with which a revenue authority disagrees.

91. The main areas where offences may arise in relation to direct tax are:

tax evasion, including making false returns (including supporting documents), accounts or financial statements or deliberate failure to submit returns and

deliberate refusal to correct known errors.

6.4.7.1 Innocent or negligent error

92. Where a *customer* indicates that they are unwilling, or refuse, to disclose an innocent mistake or negligent act to the *competent authority* in order to avoid paying the tax due, the *customer* appears to have formed a criminal intent and therefore a reporting obligation arises. The *supervised person* should also consider whether they can continue to act for the *customer*. This paragraph applies equally to potential *customers* for whom the *supervised person* has declined to act.

6.4.7.2 Intention to underpay

93. *Customers* may suggest that they will, in the future, underpay tax. This would be tax evasion and also a *money laundering* offence when it occurs. A *supervised person* can and should investigate whether the *customer* has understood their obligations under the relevant legislation. Should the *customer's* intention in this regard still remain in doubt, the *supervised person* should consider carefully whether they can commence or continue to act, and if in doubt should seek specialist legal advice. A SAR may well be required in such cases.

6.4.8 Observation of unlawful conduct

94. It should be borne in mind that for property to be criminal property, not only must it constitute a person's benefit from criminal conduct, but the alleged offender must know or suspect that the property constitutes such a benefit. This means, for example, that if someone has made an innocent error, even if such an error resulted in benefit and constituted a strict liability criminal offence, then the proceeds are not criminal property and no *money laundering* offence has arisen until the offender becomes aware of the error.

95. Examples of unlawful behaviour which may be observed, but which are not reportable as *money laundering*, are set out below:

offences where no proceeds or benefit results, such as the late filing of company accounts. However, *supervised persons* should be alert to the possibility that persistent failure to file accounts could represent part of a larger offence with proceeds, such as fraudulent trading or credit fraud involving the concealment of a poor financial position

mis-statements in tax returns, for whatever cause, but which are corrected before the date when the tax becomes due

attempted fraud where the attempt has failed and so no benefit has accrued (although this may still be an offence in some jurisdictions e.g. the UK) and

where a *customer* refuses to correct, or unreasonably delays in correcting, an innocent error that gave rise to proceeds and which was unlawful, firms should consider what that indicates about the client's intent and whether the property has now become criminal property.

Deleted: Handbook for regulated financial services businesses¶
Part 1: Section 6 – On-going monitoring: scrutiny of transactions and activity¶

Deleted: This version is effective from : 12 February 2020