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 by 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 firm will still need to consider reporting provisions summarised in Section 8, e.g. where there is suspicion that payment for the service is made out of the proceeds of criminal conduct.
3. This section explains the measures required to demonstrate compliance with the requirement to scrutinise transactions and also sets a requirement to scrutinise client activity.
4. The requirement to keep documents, data and information up to date and relevant is discussed at Section 3.4 of this Handbook.

6.2 Obligation to Perform On-going Monitoring

Statutory Requirements

5. *Article 3(3) of the Money Laundering Order sets out what on-going monitoring is to involve:*
   - *Scrutinising transactions undertaken throughout the course of a business relationship to ensure that the transactions being conducted are consistent with the relevant person's knowledge of the customer, including the customer's business and risk profile. See Article 3(3)(a) of the Money Laundering Order.*
   - *Keeping documents, data or information up to date and relevant by undertaking reviews of existing records, particularly in relation to higher risk categories of 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:*
     a. *complex or unusually large transactions;*

Deleted: 24 March 2015

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 firm **monitors** all client transactions and activity in order to **recognise notable transactions or activity,** i.e. those that:

› are inconsistent with the firm's knowledge of the client;

› are complex or unusually large;

› form part of an unusual pattern; or

› present a higher risk of money laundering or the financing of terrorism.

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

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

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

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

15. **Unusual transactions or activity, unusually large transactions or activity, and unusual patterns of transactions or activity** may be recognised where transactions or activity are inconsistent with the expected pattern of transactions or expected activity for a particular client, or with the normal business activities for the type of service that is being delivered.

Deleted: s

Deleted: 24 March 2015

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

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

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

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

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

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

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

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

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

25. In order to recognise *money laundering* and the *financing of terrorism*, employees will need to have a good level of awareness of both and to have received training. Awareness raising and training are covered in Section 8 of this Handbook.

26. 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

Deleted: 24 March 2015

AML/CFT Codes of Practice

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

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

- complex or unusually large activity;
- unusual patterns of activity, which have no apparent economic or visible lawful purpose; and
- any other activity the nature of which causes the firm to regard it as particularly likely to be related to *money laundering* or the *financing of terrorism*.

29. As part of its examination of the above transactions, a firm must examine, as far as possible, their background and purpose and set forth its findings in writing. A firm must have *policies and procedures* in place to address any specific risks associated with client relationships established where the client is not physically present for identification purposes (i.e. non-face to face).

Guidance Notes

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

- its business risk assessment (including the size and complexity of its business);
- the nature of its accountancy business and services;
- whether it is possible to establish appropriate standardised parameters for automated monitoring; and
- the monitoring procedures that already exist to satisfy other business needs.

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

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

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

- reference to the client's business and risk profile;
- as far as possible, a review of the background and purpose of a transaction or activity (set in the context of the business and risk profile); and
- where necessary, the collection of further information needed to determine whether a transaction or activity has an apparent economic or visible lawful purpose.

Deleted: of

Deleted: 24 March 2015

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

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

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

Overview

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 is with a person connected with a country or territory:

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

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 country or territory**.

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

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 this Handbook.

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

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 firm 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 firm must examine, as far as possible, their background and purpose and set forth its findings in writing.

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

Deleted: 3A

Deleted: person

Deleted: 24 March 2015

Guidance Notes

42. A firm may demonstrate that *CDD policies and procedures* are appropriate where **scrutiny** of transactions and activity has regard to the following factors:
    - its business risk assessment (including the size and complexity of its business);
    - whether it is practicable to monitor transactions or activity in real time (i.e. before client instructions are put into effect); and
    - whether it is possible to establish appropriate standardised parameters for automated monitoring.
43. A firm may demonstrate that *CDD policies and procedures* are appropriate where the following are used to **recognise** connections with persons connected to enhanced risk states and sanctioned countries:
    - **All -** Client business and risk profile in line with Section 3.3.5 of this Handbook.
    - **Enhanced risk states** - Appendix D1 of the *AML/CFT Handbook*.
    - **Sanctioned countries** - Appendix D2 of the *AML/CFT Handbook* (Source 6 only).
44. A firm may demonstrate that *CDD policies and procedures* are appropriate if **examination** of transactions or activity recognised as being with a person connected with an enhanced risk state includes:
    - reference to the client's business and risk profile;
    - as far as possible, a review of the background and purpose of a transaction or activity (set in the context of the business and risk profile); and
    - where necessary, the collection of further information needed to determine whether a transaction or activity has an apparent economic or visible lawful purpose.
45. A firm may demonstrate that *CDD* and reporting *policies and procedures* are appropriate if **post-examination** of transactions or activity recognised as being with a person connected with an enhanced risk state it:
    - revises, as necessary, its client's business and risk profile;
    - adjusts, as necessary, its monitoring system e.g. refines monitoring parameters, enhances controls for more vulnerable services; and
    - considers whether it knows, suspects or has reasonable grounds for suspecting that another person is engaged in *money laundering* or the *financing of terrorism*, or that any property constitutes or represents the proceeds of criminal conduct.

6.3 Automated Monitoring Methods

Overview

46. 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 client's business and risk profile.
48. Large or more complex firms may also use automated monitoring methods to facilitate the monitoring of significant volumes of transactions, or - in an e-commerce environment - where the opportunity for human scrutiny of individual transactions is limited.

Deleted: As noted in paragraph above,

Deleted: 24 March 2015

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

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

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

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

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 clients may be particularly effective. However, where a firm uses group screening arrangements, it will need to be satisfied that it provides adequate mitigation of risks applicable to the Jersey business. In all cases, it is important that a firm:

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

53. 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"

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

[2] http://www.jerseyfsc.org/pdf/Banking-AML-&-Sanctions-Summary-Findings-2014.pdf

Deleted: 24 March 2015

6.4 Money Laundering Warning Signs for the Accountancy Sector

Overview

55. Article 13 of the *Money Laundering Order* requires firms to conduct ongoing monitoring of business relationships and take steps to be aware of transactions with heightened *money laundering* risks. The *Proceeds of Crime Law* requires firms to report suspicious transactions and activity (see Section 8 of this Handbook).

56. This Section highlights a number of warning signs for accountants generally and for those working in specific business areas to help firms decide where there are reasons for concern or the basis for a reportable suspicion.

57. Because money launderers 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 client's risk profile, or give cause for concern.

6.4.1 Secretive Clients

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

6.4.2 Unusual Instructions

59. Instructions that are unusual in themselves, or that are unusual for the firm or the client 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, 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; and
- excessive use of off-balance sheet transactions or activity.

6.4.2.1 Instructions Outside the Firm's Area of Expertise

60. Taking on work which is outside the firm's normal range of expertise can present additional risks because a money launderer might be using the firm to avoid answering too many questions. An inexperienced accountant might be influenced into taking steps which a more experienced accountant would not contemplate. Accountants should be wary of highly paid niche areas of work in which the firm has no background, but in which the client claims to be an expert.

Deleted: 9

Deleted: 24 March 2015

61. If the client is based outside Jersey, firms should satisfy themselves that there is a genuine legitimate reason why they have been instructed. For example, have the firm's services been recommended by another client or is the matter based near your firm? Making these types of enquiries makes good business sense as well as being a sensible *AML/CFT* check.

6.4.2.2 Changing Instructions

62. Instructions that change unexpectedly might be suspicious, especially if there seems to be no logical reason for the changes.

63. The following situations could give rise to cause for concern:

- a client deposits funds into a firm's client account, but then ends the transaction for no apparent reason;
- a client advises that funds are coming from one source and at the last minute the source changes; and
- a client unexpectedly requests that money received into a firm's client account be sent back to its source, to the client or to a third party.

6.4.3 Use of Client Accounts

64. Client accounts should only be used to hold client money for legitimate transactions for clients, or for another proper legal purpose. Putting criminal money through a professional firm's client account can clean it, whether the money is sent back to the client, 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

65. If funding is from a source other than a client, firms may need to make further enquiries, especially if the client has not advised what they intend to do with the funds before depositing them into the firm's account. If it is decided to accept funds from a third party, perhaps because time is short, firms should ask how and why the third party is helping with the funding.

66. Enquiries do not need to be made into every source of funding from other parties. However, firms must always be alert to warning signs and in some cases will need to seek more information.

6.4.4 Accountancy and Audit Services

6.4.4.1 Intent

67. 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*.

68. If an individual or firm knows or believes that a client is acting in error, the client may be approached and the situation and legal risks explained to them. However, once the criminality of the conduct is explained to the client, 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 firm, clients should be referred to an appropriate specialist or legal adviser.

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

Deleted: '

Deleted: 24 March 2015

6.4.4.2 Holding of Funds

70. Firms who choose to hold funds as a stakeholder or escrow agent in commercial transactions 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.

71. 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 General Warning Signs

72. Any of the following general warning signs should prompt additional questions or investigation by those offering accountancy and *audit services*:

- use of many different firms of *auditor*s and advisers for connected companies and businesses;
- the client has a history of changing bookkeepers or accountants yearly; and
- company records consistently reflect sales at less than cost, thus putting the company into a loss position, but the company continues to operate without reasonable explanation of the continued loss.

6.4.4.4 Factors Arising from Action by the Entity or its Directors

73. Where an entity is actively involved in *money laundering*, the signs are likely to be similar to those where there is a risk of fraud, and 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);
- 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.

6.4.4.5 Where the Client May Be Unknowingly a Party to Money Laundering

74. There may be occasions where the client has been duped by its own customers or clients into providing assistance or a vehicle for laundering criminal funds. Warning signs may be:

- unusual transactions without an explanation or a pattern of trading with one customer that is different from the norm;
- request for settlement of sales in cash;
- a client setting up a transaction that appears to be of no commercial advantage or logic;

Deleted: or

Deleted: 24 March 2015

- a client requesting special arrangements for vague purposes;
- unusual transactions with companies registered overseas;
- 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

75. 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 low risk of *money laundering* for those working in this area.

76. When winding up an estate, there is no blanket requirement that firms should be satisfied about the history of all of the funds which make up the estate under administration. However, firms 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, firms 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 territory, firms may need to make further checks about the source of those funds.

77. Firms 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.

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

79. If firms 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.

80. 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. Firms should remain alert to warning signs, for example if the deceased or their business interests are based in a higher risk jurisdiction.

81. If the deceased person is from another jurisdiction and a lawyer is dealing with the matter in the home country, firms may find it helpful to ask that person 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

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

83. Firms acting for charities should consider its purpose and the organisations it is 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, firms should be alert to unusual circumstances, including large sums of money.

Deleted: 24 March 2015

6.4.7 Taxation Services

84. There are a number of tax offences which can give rise to the proceeds of crime and the need to submit a *SAR* to the *JFCU*. A tax practitioner is not required to be an expert in criminal law, but they would be expected to be aware of the boundaries between deliberate understatement or other tax evasion and simple cases of error or genuine differences in the interpretation of tax law, and be able to identify conduct in relation to direct and indirect taxation which is punishable by the criminal law.

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

86. The main areas where offences may arise in 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

Deleted: negligence

87. It is not uncommon for tax practitioners to become aware of errors or omissions, in current or past years, from clients' tax returns, or any calculations or statements appertaining to any liability, or an underpayment of tax, for example, because a payment date has been missed. If the tax practitioner has no cause to doubt that these came about as a result of an innocent mistake or negligence, then they will not have formed a suspicion. However, in some cases the tax practitioner may form a suspicion that the original irregularity was criminal in nature and this will then become a reportable suspicion.

6.4.7.2 Unwillingness or Refusal to Disclose to the Tax Authorities

88. Where a client indicates that they are unwilling, or refuse, to disclose the matter to the tax authorities in order to avoid paying the tax due, the client appears to have formed a criminal intent and therefore the reporting obligation arises. The tax practitioner should also consider whether they can continue to act and should consult their professional body's guidance on such matters. This paragraph applies equally to potential clients for whom the tax practitioner has declined to act.

6.4.7.3 Adjusting Subsequent Returns

89. Where the legislation permits the correction of small errors by subsequent tax adjustments, and the original error was not attributable to any criminal conduct, then the adjustment itself will not give rise to the need to report, since no crime will have been committed.

6.4.7.4 Intention to Underpay

90. A client 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 tax practitioner can and should apply their professional body's normal ethical guidance to persuade the client to comply with the legislation. Should the client's intention in this regard still remain in doubt, the tax practitioner 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 once there are proceeds of crime.

Deleted: 24 March 2015

6.4.7.5 Offences Applicable to Value Added Tax

91. A business client who is resident in the UK or another *EU* Member State will normally be subject to *VAT*. Guidance on the offences applicable to *VAT*, for example, fraudulent evasion of *VAT* and production or sending of false documents or statements, is set out in the supplementary guidance for the tax practitioner produced as an appendix to the *AML/CFT* guidance released by the UK Consultative Committee of Accountancy Bodies.

6.4.8 Business Recovery or Receiverships

92. *Insolvency practitioners* will often encounter criminal activity when winding up or effecting recovery for a business. Serious fraud which has resulted in benefit either for the business or an individual will be reportable to the *JFCU* as will incidences where the business has been used to launder the proceeds of crime. Examples may be where:

- fraud has caused or contributed to the failure of the business;
- there has been illegal siphoning off or transfer of assets by directors/shareholders;
- false accounting or misrepresentation of profits has been applied to maintain share value;
- the Directors or members of senior management have been guilty of illegal trading or market abuse;
- tax fraud has been committed by reducing income or profits; or
- a white knight has invested criminal funds.

6.4.8.1 Observation of Unlawful Conduct Resulting in Advice

93. 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.

94. Examples of unlawful behaviour which may be observed, and may well result in advice to a client to correct an issue, 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, firms 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 client 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: 24 March 2015