2 CORPORATE GOVERNANCE

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.

2.1 Overview of Section

1. Corporate governance is defined as the system by which enterprises are directed and controlled.
2. Under the general heading of corporate governance, this Section considers:
   - Board responsibilities for the prevention and detection of *money laundering* and the *financing of terrorism*;
   - requirements for *systems and controls*, training and awareness; and
   - the appointment of a Money Laundering Compliance Officer (the ***MLCO***) and Money Laundering Reporting Officer (the ***MLRO***).
3. This Handbook describes a *relevant person*'s general framework to combat *money laundering* and *the financing of terrorism* as its "***systems and controls***". This Handbook refers to the way in which those *systems and controls* are implemented into the day-to-day operation of a *relevant person* as its "***policies and procedures***".
4. Where a *relevant person* is not a company, but is, for example, a partnership, references in this section to "the Board" should be read as meaning the senior management function of that person. In the case of a sole trader[1], the Board will be the sole trader.

2.2 Measures to Prevent Money Laundering and the Financing of Terrorism

Statutory Requirements

5. *In accordance with Article 37 of the Proceeds of Crime Law, a relevant person must take prescribed measures to prevent and detect money laundering and the financing of terrorism. Failure to take such measures is a criminal offence and, where such an offence is proved to have been committed with the consent or connivance of, or to be attributable to neglect on the part of, a director or manager or officer of the relevant person, they too shall be deemed to have committed a criminal offence.*
6. *Article 37 of the Proceeds of Crime Law enables the Chief Minister to prescribe by Order the measures that must be taken by a relevant person. These measures are established in the Money Laundering Order.*

[1] "sole trader" is defined in Article 1(1) of the *Money Laundering Order*

2.3 Board Responsibilities

Overview

7. The key responsibilities of the Board are set out in further detail below. The Board is assisted in fulfilling these responsibilities by a *MLCO* and *MLRO*. Larger or more complex relevant persons may also require dedicated risk and internal audit functions to assist in the assessment and management of *money laundering* and the *financing of terrorism* risk.

Statutory Requirements

8. *Article 11(1) of the Money Laundering Order requires a relevant person to establish and maintain appropriate and consistent policies and procedures in respect of the person's financial services business, and financial services business carried on by a subsidiary, in order to prevent and detect money laundering and the financing of terrorism.*

9. *Article 11(9) of the Money Laundering Order requires a relevant person to take appropriate measures for the purpose of making employees whose duties relate to the provision of relevant services (**relevant employees**) aware of policies and procedures required under Article 11(1) of the Money Laundering Order and of Jersey's money laundering legislation. Article 11(10) of the Money Laundering Order requires a relevant person to provide relevant employees with training in the recognition and handling of transactions carried out by or on behalf of persons who are, or appear to be, engaged in money laundering or the financing of terrorism.*

10. *Article 11(11) of the Money Laundering Order requires a relevant person to establish and maintain adequate procedures for (i) monitoring compliance with, and testing the effectiveness of, its policies and procedures; and (ii) monitoring and testing the effectiveness of measures to promote AML/CFT awareness and training of relevant employees (see Section 6 of this Handbook).*

11. *Articles 7 and 8 of the Money Laundering Order require that a relevant person appoints a MLCO and a MLRO.*

AML/CFT Codes of Practice

12. The Board must conduct and record a business risk assessment. In particular, the Board must consider, on an on-going basis, its risk appetite, and the extent of its exposure to *money laundering* and the *financing of terrorism* risks "in the round" or as a whole by reference to its organisational structure, its customers, the countries and territories with which its customers are connected, its range of services, and how it delivers those services. The assessment must consider the cumulative effect of risks identified, which may exceed the sum of each individual risk element. The Board's assessment must be kept up to date (See Section 2.3.1).

13. On the basis of its business risk assessment, the Board must establish a formal strategy to counter *money laundering* and the *financing of terrorism*. Where a *relevant person* forms part of a group operating outside of the Island, that strategy may protect both its global reputation and its Jersey business.

14. Taking into account the conclusions of the business risk assessment, the Board must (i) organise and control its affairs in a way that effectively mitigates the risks that it has identified, including areas that are complex; and (ii) be able to demonstrate the existence of adequate and effective *systems and controls* (including *policies and procedures*) to counter *money laundering* and the *financing of terrorism* (see Section 2.4).

15. The Board must document its *systems and controls* (including *policies and procedures*) and clearly apportion responsibilities for countering *money laundering* and the *financing of terrorism*, and, in particular, responsibilities of the *MLCO* and *MLRO* (see Sections 2.5 and 2.6).

16. The Board must assess both the effectiveness of, and compliance with, *systems and controls* (including *policies and procedures*), and take prompt action necessary to address any deficiencies (see Sections 2.4.1 and 2.4.2).

17. The Board must consider what barriers (including cultural barriers) exist to prevent the operation of effective *systems and controls* (including *policies and procedures*) to counter *money laundering* and the *financing of terrorism*, and must take effective measures to address them (see Section 2.4.3).

18. The Board must notify the *Commission* immediately in writing of any material failures to comply with the requirements of the *Money Laundering Order* or of this Handbook. Refer to Part 3 of the *AML/CFT Handbook* for further information.

2.3.1 Business Risk Assessment

AML/CFT Codes of Practice

1. A *relevant person* must maintain appropriate policies and procedures to enable it, when requested by the JFSC, to make available to that authority a copy of its business risk assessment.

Guidance Notes

19. The Board of a *relevant person* may demonstrate that it has considered its exposure to *money laundering* and the *financing of terrorism* risk by:

- involving all members of the Board in determining the risks posed by *money laundering* and the *financing of terrorism* within those areas for which they have responsibility;
- considering organisational factors that may increase the level of exposure to the risk of *money laundering* and the *financing of terrorism*, e.g. business volumes and outsourced aspects of regulated activities or compliance functions;
- considering the nature, scale and complexity of its business, the diversity of its operations (including geographical diversity), the volume and size of any transactions, and the degree of risk associated with each area of its operation;
- considering who its customers are and what they do;
- considering whether any additional risks are posed by the countries or territories with which its customers are connected. Factors such as high levels of organised crime, increased vulnerabilities to corruption and inadequate frameworks to prevent and detect *money laundering* and the *financing of terrorism* will impact the risk posed by relationships connected with such countries and territories;
- considering the risk that is involved in placing reliance on *obliged person*s to apply *reliance identification measures*;
- considering the characteristics of its service areas and assessing the associated vulnerabilities posed by each service area. For example:
  - assessing how legal entities and structures might be used to mask the identities of the underlying beneficial owners; and
  - considering how it establishes and delivers services to its customers. For example, risks are likely to be greater where relationships may be established remotely (non-face to face); and
- considering the accumulation of risk for more complex customers.

20. In the case of a *relevant person* that is dynamic and growing, the Board may demonstrate that its business risk assessment is kept up to date where it is reviewed annually. In some other cases, this may be too often e.g. a *relevant person* with stable services or smaller well-established business. In all cases, the Board may demonstrate that its business risk assessment is kept up to date where it is reviewed when events (internal and external) occur that may materially change *money laundering* and the *financing of terrorism* risk.

2.3.1.1 Considering and Assessing Service Area Vulnerabilities and Warning Signs

Estate Agents

Overview

21. Criminal conduct generates huge amounts of illicit capital and these criminal proceeds need to be integrated into personal lifestyles and business operations. Law enforcement agencies advise that property purchases are one of the most frequently identified methods of laundering money. Property can be used either as a vehicle for laundering money or as a means of investing laundered funds.

22. Criminals will buy property both for their own use, e.g. as principal residencies or second homes, business or warehouse premises, and as investment vehicles to provide additional income. The Serious Organised Crime Agency in the UK advises that real property arises in over 85% of all confiscation cases and at least 25% of those investigated hold five or more properties both residential and commercial.

Criminal use of conveyancing services

23. The estate agent is but one of the professionals who will be involved in a property transaction. Every property transaction requires a legal practitioner to undertake the conveyancing and this is one of the criminal's most frequently utilised functions. Conveyancing is a comparatively easy and efficient means to launder money with relatively large amounts of criminal monies cleaned in one transaction. In a stable or rising property market, the launderer will incur no financial loss except fees. Whilst many legal practitioners will be unwitting accomplices, some corrupt legal practitioners will provide deliberate assistance and estate agents should be vigilant for any signs that this is occurring.

24. The purchase of real estate is commonly used as part of the last stage of *money laundering*. Such a purchase offers the criminal an investment which gives the appearance of financial stability. The purchase of a hotel, for example, offers particular advantages, as it is often a cash-intensive business. Cash remains the mainstay of much serious organised criminal activity. It has the obvious advantage that it leaves no audit trail and is the most reliable form of payment, as well as the most flexible.

1. Case Study: Drug trafficking funds a hotel purchase

A financial intelligence unit received information that a previously convicted drug trafficker had made several investments in real estate and was planning to buy a hotel. An assessment of his financial situation did not reveal any legal source of income, and he was subsequently arrested and charged with an offence of *money laundering*. Further investigation substantiated the charge that part of the invested funds were proceeds of his own drug trafficking. He was charged with substantive drug trafficking, drug *money laundering* and other offences.

The criminal's lawyer received the equivalent of approximately US$70,000 cash from his customer, placed this money in his customer's bank account and later made payments and investments on the customer's instructions. He was charged with *money laundering* in relation to these transactions.

The drug trafficker was convicted of drug trafficking, sentenced to seven-and-a-half years imprisonment, and a confiscation order was made for US$450,000. The lawyer was convicted and sentenced to 10 months imprisonment.

25. Retail businesses provide a good front for criminal funds where legitimate earnings can be mixed with the proceeds of crime.

2. Case Study: Tobacco smuggling funds a property empire

In June 2005 the Northern Ireland Assets Recovery Agency was granted an Interim Receiving Order at the Belfast High Court for assets valued at an estimated £1.4 million.

The assets in question were held by Stephen Baxter and his wife Denise. In its application to the High Court, the Agency evidenced that Mr Baxter purported to trade as an ice cream salesman with two vans. However, no street trading licence had ever been granted making the vans recoverable property. The Agency also showed that on a number of occasions police had detected Mr Baxter selling smuggled tobacco from his vans. His lifestyle and property acquisitions appeared to be far in excess of his lawful means.

The assets included:

- a principal residence in Belfast;
- two apartments in Belfast city centre;
- an interest in a further eight building developments; and
- a planned apartment in a prestige Belfast development.

The Agency advised that they had intervened to prevent Mr Baxter from extending his property portfolio shortly before the hearing.

The total value of the property subject to the restraint order was estimated to be £1.4 million.

Recognising suspicious behaviour and unusual instructions

26. The following are examples of potentially suspicious events, both prior to and during the life of the property transaction.

Secretive customers

27. Whilst face-to-face contact with customers is not always necessary, it is unusual for there not to be such contact. Estate agents should satisfy themselves that the absence of a face-to-face meeting is not designed to assist a prospective customer to present a false identity.

28. An excessively obstructive or secretive customer may also be a cause for concern. For example, is the customer reluctant to answer the due diligence questions or provide evidence of their identity or the identity of underlying beneficial owners? Is the customer trying to use external parties to protect their identity or to hide their involvement?

Absence of normal commercial rationale

29. Activity that does not appear to make good business sense may indicate that it is linked to criminal activity. For example, where the prospective purchaser is willing to pay significantly over the market value for a property, particularly where the purchase is being undertaken by a cash-rich company.

30. A property sale or purchase that is subject to any last minute changes of significance may indicate that there is an attempt to confuse the customer due diligence (***CDD***) information.

31. A customer that has no apparent reason for using a *relevant person* (for example the location of the property or type of business) where another business would be better placed to act, may indicate that the customer is trying to make it harder for *CDD* measures to be completed. Alternatively the customer may hope that if the transaction is outside the normal size that you handle, or that it is particularly lucrative, you may turn a blind eye to any unusual or suspicious activity.

32. Where a customer has declined services that you would normally expect them to use, or shows little interest in the transaction, this may indicate that the property deal is a sham and merely being used to confuse the audit trail for criminal money (i.e. part of the layering stage of the laundering proceeds).

Ownership issues

33. Properties owned by nominee companies or those with complex structures may be used as *money laundering* vehicles to disguise the true owner and/or confuse the audit trail. In such cases, verifying the identity of the ultimate beneficial owner of the corporate structure is vital.

34. Last minute changes of instructions concerning the identity of the prospective purchaser in whose name the property is to be registered should give rise to additional due diligence.

35. Changes in the beneficial ownership of a company owning and managing a property where the new beneficial owners' *source of funds* for the company purchase is unclear or dubious may indicate that criminal funds have been injected into the company. This risk is heightened if known, reputable lawyers have not been appointed by either or both sides to act for them.

Property values

36. A significant discrepancy between the sale price and what would be considered to be normal for such a property may indicate fraud or *money laundering*.

37. Properties sold below the market value to an associate may have the objective of obscuring the title to the property while the original owner still maintains the beneficial ownership.

Valuations and surveys

38. When estate agents provide a valuation service prior to being instructed as selling agents, or when they are providing a service as surveyors, it is important that they are vigilant. If there is any indication that the property is being used for criminal conduct, a disclosure report must be made to the *MLRO*. A roomful of randomly stacked high value goods or a greenhouse filled with cannabis cannot be ignored.

3.	**Case Study: A lucrative farming enterprise**
	In September 2006, a Cannabis Farm was discovered by Dyfed Powys Police. Officers found a large and sophisticated infrastructure for growing cannabis which could have produced close to £2.5 million pounds worth of cannabis over the previous four years. The owner, who was convicted of producing cannabis with intent to supply, was imprisoned for three years and had £375,000 of his assets confiscated.

Funding issues

39. Whilst lawyers and advocates will normally handle the funds provided for a property purchase, or the sale proceeds, estate agents will often become aware of the funding arrangements. Suspicions should not be ignored merely because a lawyer is also involved and the sale or purchase funds are not passing through the estate agent's client account.

40. For example, a customer who advises that the funds from the sale will be going overseas and paid to an unrelated third party may indicate that the funds are being laundered on behalf of that third party. Similarly, where the source of funding for a purchase is obscure or appears to be unusual, this may indicate laundering of criminal funds, particularly if the funds are offered in cash or are coming in from an overseas bank account that is unconnected to the purchaser.

41. A cash deposit paid to an estate agent as part of a large property transaction, which is also to be settled in cash, may indicate tax evasion or that criminal proceeds are being used to fund the transaction. Cash is the principal currency of the criminals and should always be subject to further enquiries.

42. Situations where a potential purchaser you are assisting requests you, as the estate agent, to hold the potential purchase funds in your client account must be treated with extreme caution. Because large amounts of cash cannot normally be banked without suspicions being raised, criminals will use other professionals as 'gatekeepers'. Placing cash into the banking system through customer accounts of professional firms is a classic *money laundering* technique. As lawyers tighten up on the circumstances in which they will hold customer money, other targets will be sought. Where a customer withdraws from a transaction after paying money into a client account, the customer receives a cheque (or electronic transfer) from the lawyer or estate agent which makes the funds appear to be legitimate.

Mortgage fraud and money laundering

43. Where prospective property purchasers overstate or misrepresent their income in an attempt to mislead mortgage lenders, this falls within the definition of mortgage fraud. Alternatively, the value of the property may be inflated with a view to obtaining a mortgage for the full inflated value. Estate agents must avoid becoming complicit in such criminal arrangements. Mortgage fraud itself is a criminal offence, but the estate agent is also entering into an arrangement to further a criminal act and obtain funds for laundering.

44. Unexplained changes in ownership may indicate 'flipping' where property has been purchased using someone else's identity and the proceeds of crime are mixed with mortgage funds for the purchase.

45. Fraudulent borrowers will often seek to build a portfolio of properties by obtaining many mortgages with several lenders, either using fictitious names or using real names. The portfolio is then used for various purposes such as:

- Organised letting (particularly using assisted housing schemes);
- Property development of a site or individual properties; and
- 'Rollover', where the entrepreneur sells the properties to him/herself (in various guises) at inflated prices.

46. Collusive mortgage fraud has become a significant problem in many countries with agents, valuers and legal professionals acting in concert to provide all concerned with maximum benefit.

4.	**Case Study: Operation Trooper**
	A ring of 43 professionals, including several fraudulent valuers, was broken as a result of the largest mortgage fraud investigation ever undertaken in the UK. The fraudsters bought over 200 properties, falsely inflated their values, and sold them amongst themselves, fraudulently obtaining mortgages from most of the large lenders. No repayments were ever made on any of the mortgages which totalled £35 million.

Buy to let

47. Buy to let properties are particularly vulnerable to *money laundering*, and especially so when linked to self-certification of income by the purchaser. Terrorist organisations may also purchase multi-tenanted property to provide safe haven accommodation for the operatives within their cells. Consequently, the receipt of substantial payments of rent in cash increases the vulnerabilities of letting agents. To safeguard the position of letting agents who deal with buy to let properties or wish to receive payments of rent in cash, the Association of Residential Letting Agents recommends that they voluntarily adopt the *AML/CFT systems and controls* that are applicable to estate agents.

5.	**Case Study: Operation Verge**
	In February 2004, following an investigation by the National Crime Squad and Her Majesty's Revenue and Customs in the UK, four people were arrested for importing cannabis resin concealed in machines from Spain. One of the defendants offered to plead guilty if no confiscation order was brought against him. The investigation which spanned several jurisdictions in Europe had uncovered a property portfolio the defendant wanted to protect. The defendant had purchased several new apartments in various developments to launder the money and rent out the properties. A confiscation order was raised against the defendant amounting to around £2.7m.

High Value Dealers

Overview

Cash as criminal currency

48. Cash remains the mainstay of much serious organised criminal activity. It has the obvious advantage that it leaves no audit trail and is the most reliable form of payment, as well as the most flexible.

49. As illustrated in the following case study, the €500 note has become the bank note of choice for criminals, replacing the $100 note. Consequently, businesses should always exercise additional vigilance when accepting a large number of €500 notes from any one customer.

6. Case Study: €500 Spanish Bin Ladens

In 2005 the Bank of Spain advised that €500 notes were increasingly being drawn from high street banks and then disappearing. In March 2006, 100 million more notes were issued to Spanish high street banks than were handed in by them. This was of significant concern because Spain uses 26% of all €500 notes that are issued within the 12 eurozones.

In response to the Central Bank's concern, an investigation was launched by the Spanish Government into the missing notes. The result was that the Spanish Treasury identified 13,500 suspicious transactions totalling €6 billion that had taken place between 2003 and 2006 using €500 notes.

By way of example, the deputy mayor of Marbella was found to have €378,000 in €500 notes in her safe when she was arrested by police in April 2006 during the investigation of eastern European crime groups operating on the Costa del Sol.

In Spain the €500 notes are popularly known as Bin Ladens; like the Al-Qa'ida leader, everyone knows that they are around, but hardly anyone has seen them.

50. Those in receipt of large sums of cash have the problem of how to dispose of it. The objective of the first stage of *money laundering* – placement – is to move the criminal cash into the financial system. It is extremely difficult to place large amounts of cash into the banking system without raising suspicions. Serious organised criminals frequently launder cash through legitimate and quasi legitimate businesses, typically those with a high cash turnover. The businesses are often owned or part–owned by the criminals or by close associates, although legitimate businesses may also be duped into providing the means for laundering criminal proceeds. Retail businesses that genuinely accumulate and bank large amounts of cash are natural targets for laundering the cash though genuine purchases.

51. Businesses who find themselves in financial difficulties may also be targeted by the criminals. Cash may be placed into the banking system by persuading the owners or managers to deposit criminal money along with their normal takings. The business then transfers the criminal money to the money launderer's account, taking a cut along the way.

7. Case Study: Cash will do nicely

A number of banks in Madrid were surprised to be visited by their local drug squad.

Accounts had been opened for companies running cash based businesses that received cash from customers and paid suppliers in cash.

The businesses even arranged to deliver cash to the bank in small denomination notes, which would be exchanged for the large €500 notes. The €500 notes were then either paid into other bank accounts or smuggled out of Spain. Needless to say, no suspicious transaction reports had been made by any of the banks concerned.

Recognising stolen cash

52. Stolen cash is frequently laundered through retail outlets. GB pounds sterling, and many euro banknotes, become stained with dye when cash boxes are stolen and opened during bank or cash in transit robberies. Frequently criminals attempt to clean them, but the process damages foil and other security features.

High value cash transactions

53. Money Launderers normally want to move funds quickly in order to avoid detection. This is more easily done in large one-off transactions. The purchase of high value goods, with good portability, paid for in cash, represents an attractive target for money launderers. Luxury goods paid for with cash that can easily be sold on (even at a loss) for "clean money" are especially attractive.

54. Equally an asset may be purchased to support a certain lifestyle (e.g. a high performance car or a yacht). Alternatively an asset may be purchased as a form of long term investment (e.g. jewellery an antique or work of art etc).

8.	**Case Study: A high value lifestyle**
	In August 2007, a record £2.8 million was seized from two criminal families who made a fortune from car crime and tax evasion. The Biddies and the Strettons lived a life of luxury, shopping at Harrods and wearing designer clothes and jewellery and driving top of the range cars. However, it was all paid for through crime. The families made their money by dishonest car dealing – turning back the mileages of cars and then selling them on – and by selling stolen caravans. The scam involved forged documents, altered MOT certificates and fake service histories. The gang of eleven, none of whom had legitimate jobs, then made the money disappear by splashing out on luxury cars, designer jewellery, clothes, perfumes, priceless china and other antiques. When the homes of the gang were raided by 350 officers from four UK police forces, almost £1 million in cash, mostly in £50 notes, was found to be buried in the grounds or hidden around the various houses. Members of the gang pleaded guilty to *money laundering*, criminal conspiracy, obtaining money by deception and possessing criminal property.

Gold and Precious Metals

55. Criminal funds can be used to purchase gold which is then exported to other jurisdictions and sold, thus legitimising the funds as the proceeds of sale. The use of gold is attractive for many reasons; it is the only raw material comparable to money. It is a universally accepted medium of exchange which is traded on world markets and the launderer can remain anonymous.

9.	**Case Study: A rich horde of tools**
	A New York gold refinery owner was found guilty of laundering money for Colombian drug traffickers by selling them gold moulded into tools, screws and other bulk items that could be shipped to Colombia undetected.

56. Sometimes the jewellery trade will also becoming involved in the laundering exercise.

10.	Case Study: Operation Meltdown

Operation Meltdown was a three-year investigation into drug *money laundering* in Manhattan's diamond district. Dealers agreed to trade 220 pounds of gold and diamonds for more than US$1 million in cash. The probe resulted in 23 arrests, including 11 jewellers and the seizure of more than US$1.5 million in cash, US$1.3 million in gold and 118 kilograms of cocaine.

One jeweller was charged with agreeing to exchange diamonds and gold for US$600,000 in cash. He was murdered in June 2004 less than one month before his trial.

Precious Stones and Jewellery

57. Precious stones and jewellery are easily transportable and highly concentrated forms of wealth.

11.	Case Study: Laundering through diamonds

A Singapore couple deposited a reported US$8 million into a lawyer's client account. The deposit was made pending the completion of a real estate transaction, but the lawyer defrauded his clients, stole the money and disappeared. However, before fleeing Singapore in June 2006, the lawyer bought jewellery to the value of a few million Singapore dollars from a local jeweller with whom he had no apparent prior dealings. The purchase was enormous for the size of the jewellery store, being the equivalent of one half year's turnover. However, the owner of the store did not request to meet the client and was not involved in providing any advice on the purchases. Sales staff at the jewellery store noted that the lawyer was going on a vacation with his family at the end of the week and needed the jewellery for investment purposes.

A Singapore Police Advisory Notice issued by the Commercial Affairs Department and circulated to participants in the Singapore diamond market indicated that between 31 May and 2 June, the lawyer bought a handful of good quality fancy yellow diamonds, some 10 carats each, which the trade would sell for between S$8,500 and S$12,500 per carat, several other pieces of cheaper jewellery and two large blue sapphires. He allegedly asked for, and received, a total price for the entire purchase and then bargained on the amount payable. Notwithstanding the 'investment purchase excuse' the invoices did not provide the individual prices for the loose and certified diamonds. According to industry sources, some of the fancy yellow diamonds were bought without even being seen.

Multiple payments were made, including a wire transfer to the jeweller's bank account for an amount greater than the total value of the purchase which was drawn on the lawyer's client account. The refund (approximately S$20,000) was requested to be made in cash. This was followed by an additional payment by cheque made out to cash (for additional goods) also drawn from the lawyer's client account. The owner of the jewellery store cashed the cheque himself.

The motor trade

58. Vehicles may be either the source of the laundered money or the means by which other illegal income is laundered. Money launderers often make contacts within trades in which the use of cash is accepted, such as dealers in expensive cars.

12. Case Study: The four-wheel laundry

The financial intelligence unit of Country R received a suspicious transaction report on large purchases of Country F currency totalling US$263,000 and carried out by a citizen of Country R.

The funds in Country F currency were used for the purchase of new motor vehicles in Country F. However, the transactions detected appeared to include only part of the funds moved by the individual and his associates.

Indeed, the organisation to which the individual belonged regularly acquired new motor vehicles in Country R for payments in cash from a large dealership – which was either in collusion with the organisation or turning a blind eye to the activity.

The purchased vehicles (for around US$30,900 each in the verified cases) were delivered and then driven to a neighbouring country where they were received by a close relation of the main individual in the scheme and known by authorities to be involved in narcotics trafficking. The vehicles were then exchanged for large quantities of drugs that were to be resold in Country R. Investigations revealed that the total amount of money involved in the scheme was in excess of US$355,000.

13. Case Study: The tax evading car importer

Mr Renucci bought and sold Porsche, BMW, Mercedes and other high value vehicles. He ordered the cars from the continent and created a network of false identities and addresses to avoid paying import tax on the vehicles. Import documents gave false details and he built up a portfolio of false names and addresses from vehicle registration centres around the country. Police investigators traced the cars back to the importers. They found that numerous individuals had been paid £10 each to receive the vehicle registration documents through the post. Many of the cars were sold for cash to the travelling community and consequently were untraceable.

As a result of the investigations, Cumbria Police secured £1 million in assets following the conviction of Renucci who was jailed for two and a half years for *money laundering* and conspiracy to defraud the Revenue Authorities.

Outstanding finance

59. Outstanding finance is a big risk faced by dealers who buy in second hand cars. HPI Limited advise that 24 out of every 100 cars offered for sale that are checked by them are still subject to a finance agreement. If the loan remains unpaid when the vehicle is purchased, the dealer and any subsequent buyer will not acquire good title to it.

Recognising suspicious behaviour and unusual instructions

60. The following are examples of potentially suspicious transactions:

- reluctance to make personal contact;
- reluctance to provide the required identification information or evidence of identity;
- the size of purchase is out of line with the appearance/age of the customer;
- customers who initially indicate that they will be paying for goods over €15,000 by credit card/cheque and then at the last minute present cash as the means of payment;
- there appear to be no genuine reasons for paying large sums of money in cash;
- cash is unusual for that type of customer;

- customers purchasing goods which are available nearer home at a similar price;
- purchases by businesses where the level of cash activity is higher than the underlying business would justify; and
- the customer is paying in small denomination used notes.

Goods that are returned for refund

61. Returning high value goods paid for in cash and obtaining a refund by way of a cheque enables the laundering of the "dirty money" by exchanging it for a legitimate retailer's cheque. Suspicions may be raised in the following circumstances:

- the customer enquires about the business's refund policy prior to purchasing;
- the customer seeks a refund for spurious reasons; or
- the customer seeks the repayment in the form of a cheque when the purchase or a deposit was made in cash.

14. Case Study: The cash deposit scam

A professional criminal money launderer developed a simple technique of going into a number of high-priced West End jewellers and asking to inspect very expensive pieces of jewellery, saying that he was looking for a present for his wife. Dressed expensively and presenting himself well, he would choose various pieces, and then ask to see the manager. Explaining that he wanted to give his wife the opportunity to choose for herself, he asked if the shop would be prepared to take the items off display, and hold them for his wife's inspection. He explained that he would be prepared to deposit significant sums of cash to be held by the shop as a deposit for the items chosen, and that once his wife had chosen the item she wished, he would pay the balance. He also explained that any sums uncollected could be returned to him in the form of a cheque made payable to one of his corporate entities.

On five separate occasions he placed significant sums of cash, a total in excess of £100,000, as 'deposits' for items of valuable jewellery. On each occasion, his 'wife' then went into the shop on the following day and inspected the relevant items. Finding nothing to her taste, she then asked the store to make a cheque payable to her husband's business as previously instructed.

Both husband and wife were later arrested after one store learned about the unusual couple with so much money to spend but with such particular tastes. They shared the information among their trade members and discovered that the tactic had been used on a number of previous occasions. Then they alerted the police.

15. Case Study: Cash into wine

A similar technique was discovered by a leading wine trade company who discovered that a number of apparently wealthy Russian businessmen were asking to buy significant volumes of high-value wine, and keeping it held in 'bond' by the firm. The businessmen paid for their purchases in cash, but did not ask for the wine to be released from the bonded warehouse. This was not considered unusual as many wine buyers purchase investment wines in this way. Later, upon request, the businessmen asked for their wines to be re-sold back to the company, sometimes at enhanced rates, depending upon the prevailing sale-room price.

Buying second hand goods

62. High value dealers who buy-in high value second hand items for trading on should be vigilant to avoid handling stolen property. A money launderer who has exchanged criminal cash for a high value asset and then trades it in has a cheque that can be paid into *his* bank account. He has therefore effectively 'placed' and 'integrated' the laundered money. Jewellers, art and antique dealers should use their networking to exchange information when stolen goods are being offered around for sale.

2.4 Adequate and effective systems and controls

Overview

63. For *systems and controls* (including *policies and procedures*) to be adequate and effective in preventing and detecting *money laundering* and the *financing of terrorism*, they will need to be appropriate to the circumstances of the *relevant person*.

Statutory Requirements

64. *Article 11(1) of the Money Laundering Order requires a relevant person to establish and maintain appropriate and consistent policies and procedures in respect of the person's financial services business, and financial services business carried on by a subsidiary, in order to prevent and detect money laundering and* the *financing of terrorism.*

65. *Parts 3, 3A, 4 and 5 of the Money Laundering Order set out the measures that are to be applied in respect of customer due diligence, record keeping and reporting.*

66. *Article 11(2) of the Money Laundering Order requires that policies and procedures established and maintained under Article 11(1) are appropriate having regard to the degree of risk of money laundering and the financing of terrorism taking into account: (i) the level of risk identified in a national or sector-specific risk assessment in relation to money laundering carried out in respect of Jersey; and (ii) the type of customers, business relationships, products and transactions with which the relevant person's business is concerned.*

67. *Article 11(3) lists a number of policies and procedures that must be established and maintained.*

68. *Article 11(9) of the Money Laundering Order requires a relevant person to take appropriate measures for the purpose of making employees whose duties relate to the provision of financial services ("relevant employees") aware of policies and procedures under Article 11(1) and of legislation in Jersey to counter money laundering and the financing of terrorism. Article 11(10) of the Money Laundering Order requires a relevant person to provide relevant employees with training in the recognition and handling of transactions carried out by or on behalf of persons who are, or appear to be, engaged in money laundering or financing terrorism.*

69. *Article 11(11) of the Money Laundering Order requires a relevant person to establish and maintain policies and procedures for: (i) monitoring compliance with, and testing the effectiveness of, its policies and procedures; and (ii) monitoring and testing the effectiveness of measures to promote awareness and training of relevant employees.*

70. *When considering the type and extent of testing to be carried out under Article 11(11) of the Money Laundering Order, Article 11(12) requires a relevant person to have regard to the risk of money laundering or the financing of terrorism and matters that have an impact on that risk, such as the size and structure of the relevant person.*

71. *Article 11(8) requires that a relevant person operating through branches or subsidiaries, which carry on financial services business, must communicate its policies and procedures, maintained in accordance with Article 11(1), to those branches or subsidiaries. In addition, Article 11A requires group programmes for information sharing (see 2.7)*

AML/CFT Codes of Practice

72. A *relevant person* must establish and maintain appropriate and consistent *systems and controls* to prevent and detect *money laundering* and the *financing of terrorism*, that enable it to:

- apply the *policies and procedures* referred to in Article 11 of the *Money Laundering Order*.
- apply *CDD* measures – in line with Sections 3 to 7.
- report to the Joint Financial Crimes Unit (the ***JFCU***) when it knows, suspects or has reasonable grounds to know or suspect that another person is involved in *money laundering* or the *financing of terrorism*, including attempted transactions (in line with Section 8 of this Handbook);
- adequately screen *relevant employee*s when they are initially employed, make employees aware of certain matters and provide training - in line with Section 9 of this Handbook;
- keep complete records that may be accessed in a timely basis - in line with Section 10 of this Handbook;
- liaise closely with the *Commission* and the *JFCU* on matters concerning vigilance, *systems and controls* (including *policies and procedures*);
- communicate *policies and procedures* to overseas branches and subsidiaries, and monitor compliance therewith; and
- monitor and review instances where exemptions are granted to *policies and procedures*, or where controls are overridden.

73. In addition to those listed in Article 11(3) of the *Money Laundering Order*, a *relevant person*'s *policies and procedures* must include *policies and procedures* for:

- customer acceptance (and rejection), including approval levels for higher risk customers;
- the use of transaction limits and management approval for higher risk customers;
- placing reliance on *obliged person*s;
- applying exemptions from customer due diligence requirements under Part 3A of the *Money Laundering Order* and enhanced *CDD* measures under Articles 15, 15A and 15B;
- keeping documents, data or information obtained under *identification measures* up to date and relevant, including changes in beneficial ownership and control;
- taking action in response to notices highlighting countries and territories in relation to which the *FATF* has called for the application of countermeasures or enhanced *CDD* measures; and
- taking action to comply with *Terrorist Sanctions Measures* and the *Directions Law*.

74. In maintaining the required *systems and controls* (including *policies and procedures*), a *relevant person* must check that the *systems and controls* (including *policies and procedures*) are operating effectively and test that they are complied with.

2.4.1 Effectiveness of Systems and Controls

Guidance Notes

75. A *relevant person* may demonstrate that it checks that *systems and controls* (including *policies and procedures*) are adequate and operating effectively where the Board periodically considers the efficacy (capacity to have the desired outcome) of those *systems and controls* (including *policies and procedures*, and those in place at branches and in respect of subsidiaries) in light of:

- changes to its business activities or business risk assessment;
- information published from time to time by the *Commission* or *JFCU*, e.g. findings of supervisory and themed examinations and typologies;
- changes made or proposed in respect of new legislation, *AML/CFT Codes of Practice* issued under the Supervisory Bodies Law or guidance;
- resources available to comply with the money laundering legislation, the *Money Laundering Order* and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law*, in particular resources provided to the *MLCO* and *MLRO*, to apply enhanced *CDD* measures and to scrutinise transactions.

76. A *relevant person* may demonstrate that it checks that *systems and controls* (including *policies and procedures*) are operating effectively where the Board periodically considers the effect of those *systems and controls* (including *policies and procedures*, and those in place at branches and in respect of subsidiaries) in lights of the information that is available to it, including:

- reports presented by the *MLCO* and others (e.g., where appropriate, risk management and internal audit functions) on compliance matters and the *MLRO* on reporting;
- reports summarising findings from supervisory and themed examinations and action taken or being taken to address recommendations;
- the number and percentage of customers that have been assessed by the *relevant person* as presenting a higher risk;
- the number of applications to establish business relationships or carry out one-off transactions declined due to *CDD* issues, along with reasons;
- the number of business relationships terminated due to *CDD* issues, along with reasons;
- the number of "existing customers" that have still to be remediated under Section 4.7.2;
- details of failures by an *obliged person* or customer to provide information and evidence on demand and without delay under Articles 16, 16A and 17B-D of the *Money Laundering Order* and action taken;
- the number of alerts generated by automated on-going monitoring systems;
- the number of internal *SAR*s made to the *MLRO* (or *deputy MLRO*), the number of subsequent external *SAR*s submitted to the *JFCU*, and the timelines of reporting (by business area if appropriate);
- inquiries made by the *JFCU*, or production orders received, without issues having previously been identified by *CDD* or reporting *policies and procedures*, along with reasons;
- results of testing awareness of *relevant employee*s with *policies and procedures* and legislation;
- the number and scope of exemptions granted to *policies and procedures*, including at branches and subsidiaries, along with reasons.

2.4.2 Testing of Compliance with Systems and Controls

Guidance Notes

77. A *relevant person* may demonstrate that it has tested compliance with *systems and controls* (including *policies and procedures*) where the Board periodically considers the means by which compliance with its *systems and controls* (including *policies and procedures*) has been monitored, compliance deficiencies identified and details of action taken or proposed to address any such deficiencies.

78. A *relevant person* may demonstrate that it has tested compliance with *systems and controls* (including *policies and procedures*) where testing covers all of the *policies and procedures* maintained in line with Article 11(1) of the *Money Laundering Order* and paragraph 73 above, and in particular:

- the application of simplified and enhanced *CDD* measures;
- reliance placed on *obliged person*s under Article 16 of the *Money Laundering Order*;
- action taken in response to notices highlighting countries and territories in relation to which the *FATF* has called for the application of countermeasures or enhanced *CDD* measures;
- action taken to comply with *Terrorist Sanctions Measures* and the *Directions Law*;
- the number or type of employees who have received training, the methods of training and the nature of any significant issues arising from the training

2.4.3 Consideration of Cultural Barriers

Overview

79. The implementation of *systems and controls* (including *policies and procedures*) for the prevention and detection of *money laundering* and the *financing of terrorism* does not obviate the need for a *relevant person* to address cultural barriers that can prevent effective control. Human factors, such as the inter-relationships between different employees, and between employees and customers, can result in the creation of damaging barriers.

80. Unlike *systems and controls* (including *policies and procedures*), the prevailing culture of an organisation is intangible. As a result, its impact on a *relevant person* can sometimes be difficult to measure.

Guidance Notes

81. A *relevant person* may demonstrate that it has considered whether cultural barriers might hinder the effective operation of *systems and controls* (including *policies and procedures*) to prevent and detect *money laundering* and the *financing of terrorism* where the Board considers the prevalence of the following factors:

- an unwillingness on the part of employees to subject high value (and therefore important) customers to effective *CDD* measures for commercial reasons;
- pressure applied by management or customer relationship managers outside Jersey upon employees in Jersey to transact without first conducting all relevant *CDD*;
- undue influence exerted by relatively large customers in order to circumvent *CDD* measures;
- excessive pressure applied on employees to meet aggressive revenue-based targets, or where employee or management remuneration or bonus schemes are exclusively linked to revenue-based targets;

- an excessive desire on the part of employees to provide a confidential and efficient customer service;
- design of the customer risk classification system in a way that avoids rating any customer as presenting higher risk;
- the inability of employees to understand the commercial rationale for business relationships, resulting in a failure to identify non-commercial and therefore potential *money laundering* and the *financing of terrorism* activity;
- negative handling by managerial staff of queries raised by more junior employees regarding unusual, complex or higher risk activity and transactions;
- an assumption on the part of more junior employees that their concerns or suspicions are of no consequence;
- a tendency for management to discourage employees from raising concerns due to lack of time and/or resources, preventing any such concerns from being addressed satisfactorily;
- dismissal of information concerning allegations of activities on the grounds that the customer has not been successfully prosecuted or lack of public information to verify the veracity of allegations;
- the familiarity of employees with certain customers resulting in unusual, complex, or higher risk activity and transactions within such relationships not being identified as such;
- little weight or significance is attributed to the role of the *MLCO* or *MLRO*, and little co-operation between these post-holders and customer-facing employees;
- actual practices applied by employees do not align with *policies and procedures*;
- employee feedback on problems encountered applying *policies and procedures* are ignored;
- non-attendance of senior employees at training sessions on the basis of mistaken belief that they cannot learn anything new or because they have too many other competing demands on their time.

2.4.4 Outsourcing

Overview

82. In a case where a *relevant person* outsources a particular activity, it bears the ultimate responsibility for the duties undertaken in its name. This will include the requirement to ensure that the external party has in place satisfactory *systems and controls* (including *policies and procedures*), and that those *systems and controls* (including *policies and procedures*) are kept up to date to reflect changes in requirements.

83. Depending on the nature and size of a *relevant person*, the roles of *MLCO* and *MLRO* may require additional support and resources. Where a *relevant person* elects to bring in additional support, or to delegate areas of the *MLCO* or *MLRO* functions to external parties, the *MLCO* or *MLRO* will remain directly responsible for the respective roles.

AML/CFT Codes of Practice

84. A *relevant person* must consider the effect that outsourcing has on *money laundering* and the *financing of terrorism* risk, in particular where a *MLCO* or *MLRO* is provided with additional support from other parties, either from within group or externally.

85. A *relevant person* must assess possible *money laundering* or the *financing of terrorism* risk associated with outsourced functions, record its assessment, and monitor any risk on an on-going basis.

86. Where an outsourced activity is a *financial services business* activity (including Schedule 2 business), then a *relevant person* must ensure that the provider of the outsourced services has in place *policies and procedures* that are consistent with those required under the *Money Laundering Order* and, by association, this Handbook.

87. In particular, a *relevant person* must ensure that knowledge, suspicion, or reasonable grounds for knowledge or suspicion of *money laundering* or the *financing of terrorism* activity are reported by the third party to the *relevant person*'s *MLRO* (or *deputy MLRO*).

2.5 The Money Laundering Compliance Officer ("MLCO")

Overview

88. The *Money Laundering Order* requires a *relevant person* to appoint an individual as *MLCO*, and tasks that individual with the function of monitoring its compliance with legislation in Jersey relating to *money laundering* and the *financing of terrorism* and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law*.

89. The *Money Laundering Order* also requires a *relevant person* to maintain adequate procedures for: (i) monitoring compliance with, and testing the effectiveness of, *policies and procedures*; and (ii) monitoring and testing the effectiveness of measures to raise awareness and training. When considering the type and extent of compliance testing to be carried out, a *relevant person* shall have regard to the risk of *money laundering* and the *financing of terrorism* and matters that have an impact on risk, such as size and structure of the *relevant person*'s business.

90. The *MLCO* may have a functional reporting line, e.g. to a group compliance function.

91. The *Money Laundering Order* does not rule out the possibility that the *MLCO* may also have other responsibilities. To the extent that the *MLCO* is also **responsible** for the development of *systems and controls* (including *policies and procedures*) as well as monitoring subsequent compliance with those *systems and controls* (including *policies and procedures*), some additional independent assessment of compliance will be needed from time to time to address this potential conflict. Such an independent assessment is unlikely to be needed where the role of the *MLCO* is limited to actively monitoring the development and implementation of such *systems and controls*.

Statutory Requirements

92. *Article 7 of the Money Laundering Order requires a relevant person to appoint a MLCO to monitor whether the enactments in Jersey relating to money laundering and the financing of terrorism and AML/CFT Codes of Practice are being complied with. The same person may be appointed as MLCO and MLRO.*

93. *Article 7(2A) of the Money Laundering Order requires a relevant person to ensure that the individual appointed is of an appropriate level of seniority and has timely access to all records that are necessary or expedient.*

94. *Article 7(6) of the Money Laundering Order requires a relevant person to notify the Commission in writing within one month when a person is approved as, or ceases to be a MLCO. However, Article 10 provides that the Commission may grant exemptions from this notification requirement by way of notice.*

AML/CFT Codes of Practice

95. A *relevant person* must appoint a *MLCO* that:

- is employed by the *relevant person*;

- is based in Jersey; and
- has sufficient experience and skills.

96. A *relevant person* must ensure that the *MLCO*;

- has appropriate independence, in particular from customer-facing, business development and system and control development roles;
- reports regularly and directly to the Board and has a sufficient level of authority within the *relevant person* so that the Board reacts to and acts upon reports made by the *MLCO*;
- has sufficient resources, including sufficient time and (if appropriate) a deputy *MLCO* and compliance support staff; and
- is fully aware of both their and the *relevant person*'s obligations under the *money laundering* legislation, the *Money Laundering Order* and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law*.

97. In the event that the position of *MLCO* is expected to fall vacant, to comply with the statutory requirement to have an individual appointed to the office of *MLCO* at all times, a *relevant person* must take action to appoint an appropriate member of the Board (or other appropriate member of senior management) to the position on a temporary basis.

98. If temporary circumstances arise where the *relevant person* has a limited or inexperienced compliance resource, it must ensure that this resource is supported as necessary.

99. When considering whether it is appropriate to appoint the same person as *MLCO* and *MLRO*, a *relevant person* must have regard to:

- the respective demands of the two roles, taking into account the size and nature of the *relevant person*'s activities; and
- whether the individual will have sufficient time and resources to fulfil both roles effectively.

Guidance Notes

100. A *relevant person* may demonstrate that its *MLCO* is monitoring whether enactments and *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law* are being complied with where he or she:

- regularly monitors and tests compliance with *systems and controls* (including *policies and procedures*) in place to prevent and detect *money laundering* and the *financing of terrorism* – supported as necessary by a compliance or internal audit function;
- reports periodically, as appropriate, to the Board on compliance with the *relevant person*'s *systems and controls* (including *policies and procedures*) and issues that need to be brought to its attention; and
- responds promptly to requests for information made by the *Commission* and the *JFCU*.

101. In a case where the *MLCO* is also **responsible** for the development of *systems and controls* (including *policies and procedures*) in line with evolving requirements, a *relevant person* may demonstrate that the *MLCO* has appropriate independence where such *systems and controls* are subject to periodic independent scrutiny.

2.6 The Money Laundering Reporting Officer ("MLRO")

Overview

102. Whilst the *Money Laundering Order* requires one individual to be appointed as *MLRO*, it recognises that, given the size and complexity of operations of many enterprises, it may be appropriate to designate additional persons (***deputy MLROs***) to whom *SAR*s may be made.

Statutory Requirements

103. *Article 8 of the Money Laundering Order requires a relevant person to appoint a MLRO. The MLRO's function is to receive and consider internal SARs in accordance with internal reporting procedures. The same person may be appointed as both MLCO and MLRO.*

104. *Article 8(2A) of the Money Laundering Order requires a relevant person to ensure that the individual appointed is of an appropriate level of seniority and has timely access to all records that are necessary or expedient.*

105. *Article 8(4) of the Money Laundering Order requires a relevant person to notify the Commission in writing within one month when a person is appointed as, or ceases to be a MLRO. However, Article 10 provides that the Commission may grant exemptions from this notification requirement by way of notice.*

106. *Article 9 of the Money Laundering Order allows a relevant person to designate one or more persons (deputy MLROs), in addition to the MLRO, to whom internal SARs may be made.*

AML/CFT Codes of Practice

107. A *relevant person* must appoint a *MLRO* that:

- is employed by the *relevant person*;
- is based in Jersey; and
- has sufficient experience and skills;

108. A *relevant person* must ensure that the *MLRO*:

- has appropriate independence, in particular from customer-facing and business development roles;
- has a sufficient level of authority within the *relevant person*;
- has sufficient resources, including sufficient time, and (if appropriate) is supported by *deputy MLRO*s;
- is able to raise issues directly with the Board; and
- is fully aware of both their and the *relevant person*'s obligations under the *money laundering* legislation and the *Money Laundering Order* (and by extension, also this Handbook).

109. Where a *relevant person* has appointed one or more *deputy MLRO*s the requirements set out above for the *MLRO* must also be applied to any *deputy MLRO*s.

110. Where a *relevant person* has appointed one or more *deputy MLRO*s, it must provide that the *MLRO*:

- keeps a record of all *deputy MLRO*s;
- provides support to, and routinely monitors the performance of, each *deputy MLRO*; and
- considers and determines that *SAR*s are being handled in an appropriate and consistent manner.

111. In the event that the position of *MLRO* is expected to fall vacant, to comply with the statutory requirement to have an individual appointed to the office of *MLRO* at all times, a *relevant person* must take action to appoint a member of the Board (or other appropriate member of senior management) to the position on a temporary basis.

112. If temporary circumstances arise where a *relevant person* has a limited or inexperienced reporting resource, the *relevant person* must ensure that this resource is supported as necessary.

Guidance Notes

113. A *relevant person* may demonstrate that its *MLRO* (and any *deputy MLRO*) is receiving and considering *SAR*s in accordance with Article 21 of the *Money Laundering Order* where, inter alia, its *MLRO*:

- maintains a record of all requests for information from law enforcement authorities and records relating to all internal and external *SAR*s (Section 8);
- manages relationships effectively post disclosure to avoid tipping off any external parties; and
- acts as the liaison point with the *Commission* and the *JFCU* and in any other external enquiries in relation to *money laundering* or the *financing of terrorism*.

114. A *relevant person* may demonstrate routine monitoring of the performance of any *deputy MLRO*s by requiring the *MLRO* to review:

- samples of records containing internal *SAR*s and supporting information and documentation;
- decisions of the *deputy MLRO* concerning whether to make an external *SAR*; and
- the bases for decisions taken.

2.7 Financial Groups

Overview

115. A Financial Group of which a firm is a member must maintain a group programme for the sharing of AML/CFT information. In addition, as explained in Section 1.4.3, where a company incorporated in Jersey carries on a *financial services business* through an overseas branch, it must comply with *AML/CFT Codes of Practice* issued under the *Supervisory Bodies Law* in respect of that business, irrespective of whether it also carries on *financial services business* in or from within Jersey.

Statutory Requirements

116. *Article 11A of the Money Laundering Order applies to a financial group of which a relevant person is a member*

117. *Article 11A (2) of the Money Laundering Order requires a financial group to maintain a programme to prevent and detect money laundering and the financing of terrorism that includes:*

- *policies and procedures by which a relevant person within a financial group, which carries on financial services business or equivalent business, may disclose information to a member of the same financial group, but only where such disclosure is appropriate for the purpose of preventing and detecting money laundering or managing money laundering risks;*
- *adequate safeguards for confidentiality and use of any such information;*

- *the monitoring and management of compliance with, and the internal communication of such policies and procedures (including the appointment of a compliance officer for the financial group); and*
- *the screening of employees.*

118. *Under Article 11A (3) of the Money Laundering Order "information" includes the following:*

- *information or evidence obtained from applying identification measures;*
- *customer, account and transaction information;*
- *information relating to the analysis of transactions that are considered unusual.*

AML/CFT Codes of Practice

119. A person that is a Jersey incorporated company must ensure that any subsidiary applies measures that are at least equivalent to *AML/CFT Codes of Practice* in respect of any *financial services business* carried on outside Jersey by that subsidiary.

120. A person who:

- is a legal person registered, incorporated or otherwise established under Jersey law, but who is not a Jersey incorporated company; and
- carries on a *financial services business* in or from within Jersey,

must apply measures that are at least equivalent to *AML/CFT Codes of Practice* in respect of any *financial services business* carried on by that person through an overseas branch/office.

121. Where overseas legislation prohibits compliance with an *AML/CFT Code of Practice* (or measures that are at least equivalent) then the *AML/CFT Codes of Practice* do not apply and the *Commission* must be informed that this is the case. In such circumstances, a *relevant person* must take other reasonable steps to effectively deal with the risk of *money laundering* and the *financing of terrorism*.