Financial Crime

1. Introduction

1.1. Chapter overview

You will recall that one of the four statutory objectives of the FCA is to reduce financial crime.

This chapter explains the different types of financial wrongdoing and the penalties incurred if someone is found to have breached the relevant law.

You will begin by looking at insider dealing (a criminal offence defined by the Criminal Justice Act 1993) - a serious offence but notoriously difficult to prosecute.

You will then read about two offences defined by FSMA 2000: misleading statements and practices (S397), and market abuse (S118) and the penalties incurred for non-compliance.

The chapter then moves on to discuss the Proceeds of Crime Act 2002 and the criminal offence of money laundering and the financing of terrorism.

1.2. Learning outcomes

On completion of this module you will:

Insider dealing

- 3.7.7 - Explain the offence of insider dealing covered by the CJA 1993
- 3.7.6 - Explain the meaning of 'inside information' covered by the Criminal Justice Act (CJA) 1993
- 3.7.8 - Identify the penalties for being found guilty of insider dealing
- 3.7.9 - Explain the FCA's powers to prosecute insider dealing

Market abuse (S118 FSMA 2000)

- 3.7.10 - Describe the behaviours defined as market abuse (MAR 1.3, 1.4, 1.5, 1.6, 1.7, 1.8 & 1.9)
- 3.7.11 - Explain the enforcement powers of the FCA relating to market abuse (MAR 1.1.4, 1.1.5 & 1.1.6)

Money laundering

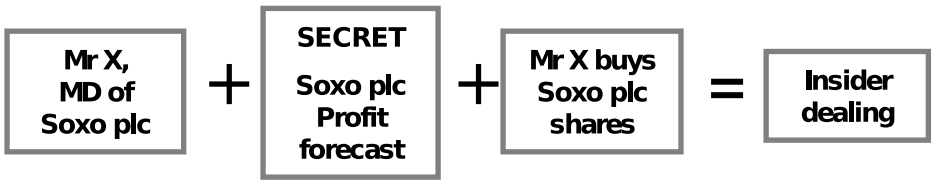
- 3.7.4 - Explain the three stages involved in the money laundering process
- 3.7.1 - Explain the various sources of money laundering and counter terrorism regulation and legislation (FCA rules, Money Laundering Regulations, Proceeds of Crime Act 2002)
- 3.7.2 - Explain the role of the Joint Money Laundering Steering Group (JMLSG)
- 3.7.3 - Explain the main features of the guidance provided by the JMLSG
- 3.7.5 - Explain the four offence categories under UK money laundering legislation

Bribery

- 3.7.12 - Explain the main features of the Bribery Act 2010

2. Insider dealing (Part V Criminal Justice Act 1993)

2.1. Introduction



Company directors and their professional advisors often have access to price-sensitive information about a company's results or prospects. It is a **criminal** offence for anyone to benefit from such information prior to its release to the market as a whole.

The Treasury oversees the insider dealing legislation contained within the Criminal Justice Act 1993.

2.2. Offences

The Criminal Justice Act defines three types of offence as 'insider dealing'. These are:

- **Dealing** on the strength of inside information either on a regulated market or through a professional intermediary
- **Encouraging** another person to deal on the strength of inside information with a reasonable belief that dealing would take place on a regulated market or through a professional intermediary
- **Disclosing** inside information to another person other than in the proper performance of one's duties

Note that disclosing information is only an offence when the person disclosing the information believes that the recipient is **likely** to deal on the strength of that information.

An offence is committed when one of the actions described above is taken and the person has information as an insider. This means that the person **knows** that it is inside information and **knows** that the information is from an inside source.

2.3. Inside information

Many types of information are covered, including financial results, takeover plans and news of the departure of key employees. Under the legislation, the information must have **all** of the following characteristics:

- It relates to a particular issuer (or issuers) of securities, or to a particular issue of securities
- It is specific or precise
- It has not been made public
- It must be likely to have a significant effect on the price once made public

Information that satisfies this definition is called **unpublished, price-sensitive information**.

The following categories of information are deemed to be **published** information:

- Published information, for example:
  - Information from a regulatory information service or financial press
  - Information from public records
  - Information published overseas
  - Information selectively published
- Information that can only be acquired by expertise or by payment of a fee
- Information that can be acquired by observation e.g. news broadcasts

2.4. Primary and secondary insiders

A person is defined as an insider if he/she has information that he/she **knows** is inside information and he/she **knows** that it is from an inside source.

Insiders could include directors, employees, shareholders, and anyone obtaining information because of their employment or profession. Such insiders are known as **primary** insiders as they have acquired their information due to their connection with the company. A **secondary** insider (sometimes known as a 'tippee') is anyone who came across inside information, directly or indirectly, from a primary insider. Both types of insider can be guilty of insider dealing.

2.5. Securities affected

Insider dealing legislation relates specifically to abuses of information in respect of financial securities. It therefore includes instruments based on securities, such as stock index futures, share warrants, depositary receipts and equity options. The main **exclusions** are:

- Assets with no secondary market, such as units in **unit trusts** and shares in investment companies with variable capital (ICVCs)
- Commodities and commodity derivatives, e.g. copper options
- Over-the-counter (OTC) markets, such as foreign exchange forward contracts
- Insurance products

2.6. Transactions affected

Only transactions on an exchange or via a professional intermediary (such as a stockbroker) are covered. Thus, a private sale from one investor directly to another is not subject to the legislation.

2.7. Defences

General defences

The following constitute a valid defence to the charge of insider dealing:

- Information was being passed on in the proper course of employment
- The person who passed on the information did not expect the recipient to deal
- The information was already publicly available: this is a very wide-ranging defence since, under the legislation, information disclosed to a 'section' of the public is deemed to be publicly available
- The person would have behaved in the same way even if he/she was not in possession of the inside information

Special defences

There are three further defences relevant to market professionals:

1. **Stabilisation** - a procedure used to maintain the price of new issues, carried out under strict rules.
2. Recipients of **market information** - this is designed to protect market participants where they have knowledge of transactions that have taken place, or are to take place, or that a transaction will not take place.
    - Market information refers to information that market professionals may hear about and it would be unreasonable to prevent them from using. The criteria the court will apply is that 'it was reasonable for an individual in their position to have acted as they did despite having that information as an insider'
    - For example where a market professional knows of the client's intention to enter into a large transaction, then the firm can continue to act on behalf of other clients or deal with them provided that it is reasonable to do so
    - This defence allows a company planning a takeover of another to buy shares in the target company before announcing its full intentions. Although it has price-sensitive information of its own intentions at the time, it will not be found guilty of insider dealing. This defence is called 'bid facilitation'
3. **Market makers** acting in the ordinary course of business - they are duty bound to buy and sell securities.

2.8. Enforcement

The market operations division of the London Stock Exchange (LSE) monitors transactions on the LSE in order to identify possible abuses. Suspicions are passed on to the FCA for investigation and prosecution. The FCA has operating arrangements in place with the Recognised Investment Exchanges (RIEs) which set out the responsibilities of the FCA and the market operators for monitoring, investigation and prosecution.

The FCA also has responsibility for prosecutions.

2.9. Penalties

In a Magistrate's Court the maximum penalty is a fine of £5,000 and six months in jail.

In a Crown Court the maximum penalty is an unlimited fine and seven years in jail.

3. Market abuse (S118 FSMA 2000)

3.1. The offence

Basic offence

Market abuse is a **civil offence** under S118 FSMA 2000.

The rules were amended in 2005 on adoption of the EU Market Abuse Directive (MAD).

The offence applies in addition to the criminal offences of insider dealing and misleading statements and practices and is easier to prove as the burden of proof in civil law is based on the balance of probabilities.

The FCA issues a 'Code of Market Conduct' which forms part of the FCA Handbook. The Code provides guidance on what does and does not constitute market abuse.

Market abuse offences

There are seven types of behaviour in relation to qualifying investments trading or to be traded on a prescribed market which are deemed to be market abuse.

1. Insider dealing

2. Improper disclosure

3. Misuse of information

4. Manipulating transactions

5. Manipulating devices

6. Dissemination

7. Misleading behaviour and distortion

Qualifying investments and prescribed markets

Behaviour will be deemed to constitute market abuse if it occurs in the UK or in relation to qualifying investments traded on a prescribed market.

The Code refers to behaviour as this includes action and inaction.

A prescribed market is:

- Any UK market regulated by an RIE (including AIM) and any regulated market as defined in the Markets in Financial Investments Directive (MiFID)

A qualifying investment is:

- Any investment handled on a UK RIE

For the offences of 'misuse of information' and 'misleading behaviour and distortion', the definition of prescribed markets excludes non-UK regulated markets. This means that these offences are only relevant for UK markets (they are not covered by MAD, but they existed in the UK before MAD and they have been carried forward).

The behaviour must be in relation to qualifying investments. However, 'in relation to' means that the offence can apply to off-exchange dealings too.

Intention

The statutory definition of market abuse does not require the person engaging in the behaviour to have intended to abuse the market. It is the **effect**, rather than the intention of the person, that is important in determining whether market abuse has occurred or not.

3.2. Code of Market Conduct

Background

FSMA defines only the outer limits of what can constitute market abuse. Under S119 FSMA 2000, the FCA has a duty to compile the Code of Market Conduct to 'give appropriate guidance to those determining whether or not behaviour amounts to market abuse'. This Code allows the FCA flexibility to adapt and amend its rules in the face of rapidly changing market practices.

The Code of Market Conduct is contained within the Business Standards block of the FCA Handbook.

Guidance contained within the Code has the authority of an evidential provision. Breach of the Code therefore does not automatically constitute market abuse, but it can be used as evidence towards demonstrating that market abuse has taken place.

Market abuse behaviours

Market abuse is behaviour by one person alone or two or more people jointly or in concert which occurs in relation to:

- Qualifying investments traded on a prescribed market
- Qualifying investments in respect of which a request for trading on a prescribed market has been made
- Related investments of a qualifying investment

The behaviour must be included in one of the seven types of behaviour described below:

1. Insider dealing

This is where an insider deals, or attempts to deal, in a qualifying investment or related investment on the basis of inside information.

An insider is someone who has inside information as a result of:

- Membership of administration, management or supervisory body of an issuer
- Holding capital in an issuer
- Their employment, profession or duties
- Criminal activities
- Obtaining information by other means which he/she knows, or could reasonably be expect to know, is inside information

2. Improper disclosure

This is where an insider discloses inside information to another person other than in the proper course of the exercise of his/her employment, profession or duties.

3. Misuse of information

The behaviour does not fall into Type 1 or 2, but it is based on information which is not generally available to those using the market and which a regular user would regard as relevant, and the behaviour would be regarded as a failure to observe the standards of behaviour reasonably expected.

A regular user is:

- A hypothetical, reasonable person
- Someone who regularly deals on the market and in the investments of the kind in question

4. Manipulating transactions

This is behaviour which consists of effecting transactions or orders to trade that are not for legitimate reasons or in conformity with accepted market practices and which:

- Give, or are likely to give, a false or misleading impression as to the supply of, or demand for, or as to the price of, the qualifying investment
- Secure the price of such investments at an abnormal or artificial level

5. Manipulating devices

Behaviour that consists of effecting transactions or orders to trade which employ fictitious devices or any other form of deception or contrivance.

6. Dissemination

This behaviour consists of the dissemination of information by any means which gives, or is likely to give, a false or misleading impression as to a qualifying investment by a person who knew, or could reasonably be expected to have known, that the information was false or misleading.

7. Misleading behaviour and distortion

The behaviour does not fall into Types 4, 5 or 6 but:

- It is likely to give a regular user of the market a false or misleading impression as to the supply of, demand for, or price or value of qualifying investments
- It would be regarded by a regular user of the market as behaviour that would distort the market in such an investment, and is likely to be regarded by a regular user of the market as a failure on the part of the person concerned to observe the standard of behaviour reasonably expected of a person in his/her position

Statutory exceptions (safe harbours)

The Code also identifies various **statutory exceptions** of behaviour. If a person behaves within one of the statutory exceptions then they are not committing market abuse.

The following are statutory exceptions:

- Conforming with the EU's Buy-back and Stabilisation Regulation

- Conforming with the Conduct of Business Rules
- Disclosures in accordance with the Disclosure Rules
- Conforming with specified rules in the Takeover Code

FSMA 2000 also provides the following additional defences:

- Believing on reasonable grounds that your behaviour does not constitute an offence
- Taking all reasonable precautions and exercising all due diligence to avoid behaving in a way that constitutes an offence (due diligence defence)

3.3. Penalties

Penalties for market abuse are outlined in Part VIII of the Act, with wrongdoers being subject to an unlimited fine.

Other penalties open to the FCA include seeking a restitution order, obtaining an injunction and issuing public statements of misconduct.

4. Money laundering (Proceeds of Crime Act 2002)

4.1. The Proceeds of Crime Act

The three stages

Money laundering is a very serious crime. It is the process by which criminals disguise the source of their criminal proceeds. The legislation on money laundering is the Proceeds of Crime Act (POCA) 2002, as amended by the Serious Organised Crime and Police Act (SOCPA) 2005. It relates to cash generated from any illegal activity – be it drugs, fraud, forgery or tax evasion.

The legislation refers to 'criminal property', which is property that has arisen from 'criminal activity'. Criminal activity is any conduct which:

- Is an offence in the UK
- Would constitute an offence if it had taken place in the UK. However, there is now a defence introduced by SOCPA where the relevant criminal conduct occurred outside the UK in a country where it was not at the time unlawful

The scope of 'relevant criminal conduct' in relation to money laundering is ultimately determined by the Secretary of State.

Money laundering is usually described in three stages: placement, layering and integration. Each stage is explained below:

Stage one: placement

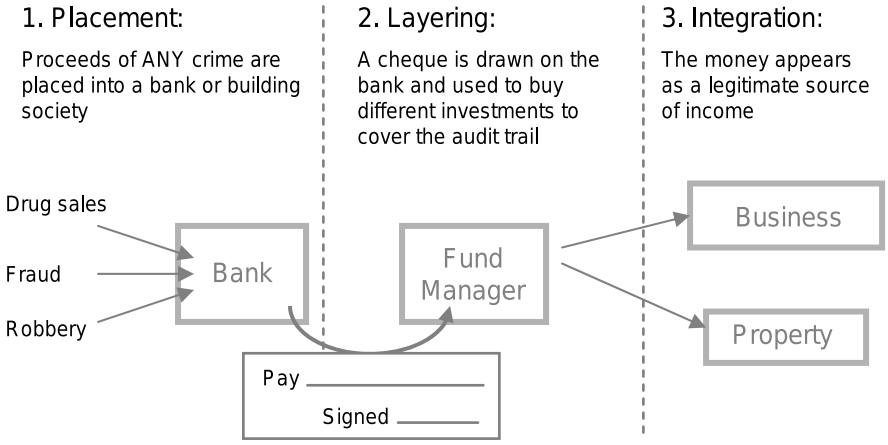
Placement involves the physical disposal of the illegal cash proceeds as a result of a criminal activity. For instance, an investor with illicit proceeds deposits £100,000 into a bank account.

Stage two: layering

Layering is the activity that separates the cash proceeds from their illegal source. For example, the criminal now draws a cheque to buy a range of investments (possibly through an authorised firm).

Stage three: integration

The third and final stage is integration. This stage is an attempt to lose the audit trail even further by re-investing cash proceeds from a seemingly legitimate source back into the financial system. For example, the investments purchased in the layering stage are now sold and the proceeds are reinvested into a business and/or property and real estate.



Relevance to the industry

Firms must maintain a sufficient audit trail of records and documents so that it can be used by the authorities should a suspicious chain of events come to light.

Each firm, no matter how small, must appoint a Money Laundering Reporting Officer (MLRO) to whom suspicions should be reported. The MLRO will then, if appropriate, speak to the relevant authority, which is the National Crime Agency (NCA), formerly known as SOCA.

The MLRO is a required controlled function and therefore must be a senior member of the firm with approved person status. Other conditions for an MLRO are:

- Expected to be based in the UK
- Be sufficiently independent
- Have sufficient resources at his/her disposal

4.2. The Money Laundering Regulations 2007

Application

The Money Laundering Regulations, issued by the Treasury and approved by Parliament, set down detailed procedures on what a firm should do to protect itself against money laundering. They are based on and implement the Money Laundering Directive.

A breach of the Regulations can be committed **whether or not** any money laundering actually takes place. The maximum penalty is a two-year jail sentence and an unlimited fine.

The Regulations apply to:

- Banks, building societies and other credit institutions
- Individuals and firms engaging in investment business within the meaning of the FSMA 2000
- Insurance companies covered by the EU Life Directives, including the life business of Lloyd's of London
- Bureau de change, cheque encashment centres and money transmission services
- Other relevant businesses including lawyers, casinos, estate agents and dealers in high value goods

A risk-based approach to identification

The approach to identifying clients and performing customer due diligence is risk-based. Where there is greater risk of money laundering, there needs to be enhanced due diligence. Where there is less risk of money laundering, simplified due diligence can be used.

Increased emphasis on due diligence

The third and most recent version of the Money Laundering Regulations (2007) has increased the emphasis on obligations regarding due diligence; for example:

- Explicit requirements for firms to undertake ongoing monitoring of business relationships
- Firms being required to identify not just the client, but the beneficial owner underlying the client

It requires firms to take enhanced customer due diligence measures in higher risk situations, while allowing firms to take reduced identification measures for specific situations with a lower risk of money laundering.

It also allows firms to rely on certain other firms for undertaking customer identification.

Simplified due diligence

Identification procedures are not required in the following circumstances:

- Credit or financial institutions subject to the Third Money Laundering Directive
- Supervised credit or financial institutions in states with comparable controls
- Listed companies on regulated markets with specified disclosure obligations
- The beneficiaries of solicitor's accounts
- Certain defined public authorities
- Certain insurance products and pension schemes
- Certain other types of defined products, such as child trust funds

Enhanced due diligence

Note that a firm should carry out identification checks, even on those persons where it is not usually required to do so, if:

- Business is conducted on a non-face to face basis
- A situation presents a higher risk of money laundering or terrorist financing
- The customer is a politically exposed person (PEP)

PEPs are clients who hold or have held public office or have gained a high political profile which could make them vulnerable to corruption. The enhanced due diligence applies to PEPs, their families and associates.

A firm is obliged to have in place procedures to ascertain whether an individual is a PEP. The 2007 regulations provide that a firm has to have in place:

- A requirement that all PEP relationships must be approved by senior management
- Adequate measures to establish source of funds and source of wealth

- Enhanced ongoing monitoring procedures

The FCA rules

FSMA 2000 sets the FCA the objective of reducing financial crime, of which money laundering is a part.

With a view to simplifying the structure and content of the Handbook, the FCA decided to delete the Money Laundering Sourcebook in its entirety and replace it with simpler and more general provisions in Senior Management Arrangements, Systems and Controls (SYSC).

To supplement this, the FCA have also produced a regulatory guide called “Financial Crime: a guide to firms” and also emphasises the guidance available from the Joint Money Laundering Steering Group. These guidance notes are considered when the FCA is assessing whether a firm has met the appropriate requirements in the systems and controls of the firm for mitigating money laundering and the terrorist financing risk.

4.3. The Joint Money Laundering Steering Group (JMLSG)

Introduction

The JMLSG produces Guidance Notes for financial institutions on fulfilling their duties in relation to money laundering and money laundering for terrorist activities. The JMLSG is made up of the leading trade associations in the financial services sector (such as the British Bankers' Association).

In particular, the JMLSG set out the standards expected in relation to senior management's responsibility to control risks that could lead to the firm furthering financial crime. To do this the firm should adopt a risk-based approach.

Risk-based approach

- Senior management roles should include an MLRO and a senior manager responsible for the direction and oversight of anti-money laundering and combating the financing of terrorism (AML/CFT).
- Adequate documentation should be produced, including the policy and procedures of the firm to implement AML/CFT. This documentation must include a named employee responsible for its implementation and an assessment of the firm's risks. These documents must be specific to the firm's business and customer risks - a generic document is not adequate.
- As part of the risk-based approach, the JMLSG also identifies low risk clients. These are clients with a regular income, clients who have had a long-term active relationship with the firm and clients who have court approval; for example, the executors of a will.

Application of the Guidance Notes is not mandatory, and failing to comply with them does not mean that a breach of the Regulations or the FCA rules has occurred. However, they do provide a good indication of the behaviour expected of financial sector firms and are a safe harbour in respect of the Regulations.

POCA 2002 and the Terrorism Act 2000 also require the courts to take account of Guidance that has been approved by HM Treasury when considering whether a person within the financial sector has committed an offence of not reporting. The JMLSG Guidance Notes have received Treasury approval.

Requirements

Internal controls

Under the Regulations, firms must ensure that they set up **appropriate** internal controls and institute a programme of staff training.

A Money Laundering Reporting Officer (MLRO) **must be appointed** to act as an internal and external point of contact for matters arising in relation to money laundering.

An MLRO is also required under the FCA's rules and, as a 'required controlled function', needs FCA approval.

Once a member of staff has reported his/her suspicions to the firm's MLRO he/she has discharged his/her statutory duty and cannot face any criminal liability in respect of the reported transaction.

Education and training

Staff must be **trained to recognise** suspicious transactions. Suspicious transactions would include those which are unusual in size or in timing for the investor, the security or the market.

To facilitate this, firms should set out detailed training schedules on anti-money laundering (AML) awareness for employees.

Identification procedures

The basic requirement

Firms are obliged to verify the identity of new clients as part of customer due diligence (CDD). Unless satisfactory evidence of identity is obtained **in a timely manner**, the business must not proceed (unless a report has been made to NCA).

Firms are **required** to carry out identification procedures on new customers in the following circumstances:

- Where a new business relationship is to be established
- Where the value of the transaction exceeds €15,000
- Where there are suspicions

Firms must:

- Identify the customer and verify the customer's identity on the basis of documents, data or information obtained from a reliable and independent source
- Identify the beneficial owner and take adequate measures on a risk-sensitive basis to verify their identity, so that the firm is satisfied that it knows who the beneficial owner is
- Obtain information on the purpose and intended nature of the business relationship
- Keep the documents, etc, obtained for the purpose of applying CDD up to date
- Conduct ongoing monitoring of the business relationship

Reporting suspicions

Under the Regulations, employees are required to report suspicious transactions **as soon as possible** to the MLRO, who will in turn refer the matter to the NCA. Once an employee has reported his/her suspicion he/she has no further reporting obligation.

Examples when a firm may be suspicious of the motives of a new/existing client include:

- A reluctance of a new client to provide identification documents
- The unnecessary use of a third party to act as an intermediary

- Continual patterns of unusual trading
- A request for non-market price transactions
- The constant use and transfer of bearer securities
- An introduction from a suspicious party or jurisdiction
- Where the client has no obvious reason to use the firm's services
- Unusual and/or frequent payment to third parties

POCA 2002 also has implications for reporting suspicions (see below).

Record keeping

The following records must be made and maintained:

- Evidence of identity: maintained for five years from the end of the firm's relationship with the client
- Transaction records: maintained for five years from the date when the transaction was completed

Records of the following should also be kept for five years:

- The dates when anti-money laundering training was given, the nature of the training and the names of the staff who received training
- Reports made by the MLRO to NCA, consideration of those reports and any action taken as a consequence

4.4. The penalties under the Proceeds of Crime Act 2002

The Proceeds of Crime Act (POCA) 2002, as amended by the Serious Organised Crime and Police Act (SOCPA) 2005, defines money laundering offences and defences.

Offences

Concealing, acquiring, possessing and assisting

The Act makes it an offence for any person to acquire or possess criminal property, or to assist another person engaging in or benefiting from criminal conduct.

The term 'criminal conduct' includes any conduct (wherever it takes place) that would constitute a criminal offence if committed in the UK. This not only includes serious criminal conduct, e.g. drug trafficking offences, terrorist activity, corruption, tax evasion, burglary and theft, fraud, forgery, counterfeiting, product piracy, illegal deposit taking, blackmail and extortion, but also any other offence regardless of size.

There is a **defence** when knowledge or suspicion of the offence is reported to the National Crime Agency (NCA) before the prohibited act is carried out, or as soon afterwards as reasonably practicable.

Failure to report

It is a criminal offence for any person within the regulated financial sector (i.e. anyone who falls within the scope of the Money Laundering Regulations) not to report his/her knowledge or suspicion that money laundering is taking place.

The Act introduces a new requirement to report **as soon as reasonably practicable** where there are 'reasonable grounds' to know or suspect that money laundering is taking place. This places an objective

test of suspicion on the regulated financial sector. If a report of a suspicion is not reported as soon as reasonably practicable, a criminal offence is committed.

An additional offence of **not reporting** has also been introduced for Money Laundering Reporting Officers (MLROs). The offence applies where an MLRO who has received an internal report does not make a report to the National Crime Agency (NCA) as soon as is practicable after the internal report was received.

It is a criminal offence to fail to be suspicious of behaviour that would ordinarily give rise to such suspicion.

Members of staff within the regulated financial sector are provided with a **defence** if their employer has not provided them with the training required under the Regulations to recognise and report suspicions or if they have a reasonable excuse for not reporting their suspicion.

Whether an excuse not to report a suspicion is reasonable will depend on the circumstances of the particular case. However, the burden of proof is that the person must demonstrate that he/she did have a reasonable excuse for not reporting their suspicion.

Note that, if an individual reports his/her suspicions regarding money laundering, he/she will **not** be in breach of any duty of confidentiality owed to a client.

Tipping off

A person commits an offence if he/she makes a disclosure which is likely to prejudice any investigation which might be conducted.

This includes disclosure to any third party no matter how small the crime may be.

It is a **defence** against this charge that a person can prove that they neither knew nor suspected that the disclosure would prejudice an investigation. Note that the burden of proof lies with the individual charged with the offence of tipping-off.

Failure to comply with the Money Laundering Regulations

Failure to comply with the Money Laundering Regulations is a criminal offence punishable by a jail term (see below).

Penalties

POCA 2002 defines the following maximum prison terms, all of which can be accompanied by an unlimited fine:

- Concealing, acquiring, possessing and assisting: 14 years
- Failure to report: five years
- Tipping off: two years
- Failure to comply with the Money Laundering Regulations: two years

FSMA 2000 grants the FCA the power to reprimand, fine and prosecute for money laundering offences under POCA 2002.

4.5. Terrorism (Terrorism Act 2000)

Introduction

In the UK, terrorism is defined by the Terrorism Act 2000 Part 1 and is a **criminal offence**.

The definition covers the use or threat of use of 'action' which is:

- Designed to influence the government (UK or overseas) or to intimidate the public (UK or overseas)
- Made for the purpose of advancing a political, religious or ideological cause

Action is relevant for the offence if it:

- Involves serious violence against a person
- Involves serious damage to property
- Endangers a person's life
- Creates a serious risk to the health or safety of the public
- Is designed to seriously interfere with or disrupt an electronic system

Laundering the proceeds of crime vs. financing terrorist acts

There are **two** major differences between the use of criminal and terrorist funds:

- Terrorists can be funded from **legitimate** funds. It is therefore difficult to identify precisely when the funds become terrorist assets.
- Only a small amount may be required to commit an act of terrorism, thus tracking funds can be difficult

Obligations on regulated firms under the Terrorism Act 2000

The Terrorism Act 2000 and the Anti-Terrorism, Crime and Security Act 2001 set out the statutory duties of regulated firms. Like money laundering, the JMLSG Guidance Notes support these obligations.

There is a statutory obligation to report any suspicion of terrorist financing arising in the regulated financial sector. As a result of this, a firm must disclose to the police and an employee must disclose internally if there is suspicion of an offence in respect of:

- Providing funds for terrorism
- Using and possessing terrorist funds
- Laundering money which is terrorist property

For staff working in an authorised firm, an offence is committed if suspicions are not reported where they had subjective suspicions (i.e. actual suspicions) or objective suspicions (i.e. reasonable grounds for being suspicious).

The penalty for failing to make a report is the same as the penalty for failing to disclose a suspicion of money laundering (i.e. a maximum of a five-year jail sentence and an unlimited fine).

5. UK Bribery Act 2010

The Bribery Act 2010 came into force in July 2011 and replaced the old laws on bribery with a more stringent set of anti-bribery rules.

5.1. Offences

Under the act it is an offence to:

- Pay bribes – it is illegal to give/offer a financial, or other, advantage with the intention of inducing a person to perform 'a relevant function or activity' improperly
- Receive bribes – it is illegal to receive a financial, or other, advantage in order to encourage the performance of 'a relevant function or activity' improperly
- To bribe foreign officials
- Fail as an organisation to prevent bribery

'Relevant function or activity' includes any function of a public nature and any activity connected with a business.

5.2. Impact on companies

Under previous laws it was unlikely for a company to be found guilty of bribery unless collusion of senior management could be proved. Therefore this is a significant change to previous legislation and a company could be found guilty without proven knowledge of the activity, but simply a lack of adequate prevention procedures. The government has published illustrative guidance on what amounts to 'adequate procedures'.

Penalties

- Individual – maximum jail sentence is ten years (increased from seven under this Act)
- Company – unlimited fine

6. Summary

6.1. Key concepts

Insider dealing

- 3.7.7 - The offence of insider dealing covered by the CJA 1993
- 3.7.6 - The meaning of 'inside information' covered by the Criminal Justice Act (CJA) 1993
- 3.7.8 - The penalties for being found guilty of insider dealing
- 3.7.9 - The FCA's powers to prosecute insider dealing

Market abuse (S118 FSMA 2000)

- 3.7.10 - The behaviours defined as market abuse (MAR 1.3, 1.4, 1.5, 1.6, 1.7, 1.8 & 1.9)
- 3.7.11 - The enforcement powers of the FCA relating to market abuse (MAR 1.1.4, 1.1.5 & 1.1.6)

Money laundering

- 3.7.4 - The three stages involved in the money laundering process
- 3.7.1 - The various sources of money laundering and counter terrorism regulation and legislation (FCA rules, Money Laundering Regulations, Proceeds of Crime Act 2002)
- 3.7.2 - The role of the Joint Money Laundering Steering Group (JMLSG)
- 3.7.3 - The main features of the guidance provided by the JMLSG
- 3.7.6 - The four offence categories under UK money laundering legislation

Bribery

- 3.7.12 - The main features of the Bribery Act 2010

Now you have finished this chapter you should attempt the chapter questions.