CHAPTER 6

SUSPICIOUS ACTIVITIES, REPORTING AND DATA PROTECTION

- **Relevant law/regulation**
  - Regulations ~~20(1)(b)~~19(3)(c), (4)(d) ~~and (2)(d) ,and~~ 21(5)and 24
  - POCA ss327-340
  - SI2006/1070 (Exceptions to overseas conduct defence)
  - Terrorism Act, ss21, 39
  - Data Protection Act 1998, s7, s29
  - Financial sanctions legislation
- **Core obligations**
  - All staff must raise an internal report where they have knowledge or suspicion, or where there are reasonable grounds for having knowledge or suspicion, that another person is engaged in money laundering, or that terrorist property exists
  - The firm's nominated officer (or their appointed alternate) must consider all internal reports
  - The firm's nominated officer (or their appointed alternate) must make an external report to the National Crime Agency (NCA) as soon as is practicable if he considers that there is knowledge, suspicion, or reasonable grounds for knowledge or suspicion, that another person is engaged in money laundering, or that terrorist property exists
  - The firm must seek consent from the NCA before proceeding with a suspicious transaction or entering into arrangements
  - Firms must freeze funds if a customer is identified as being on the Consolidated List on the HM Treasury website of suspected terrorists or sanctioned individuals and entities, and make an external report to HM Treasury
  - It is a criminal offence for anyone, following a disclosure to a nominated officer or to the NCA, to do or say anything that might either 'tip off' another person that a disclosure has been made or prejudice an investigation
  - The firm's nominated officer (or their appointed alternate) must report suspicious approaches, even if no transaction takes place
- **Actions required, to be kept under regular review**
  - Enquiries made in respect of disclosures must be documented
  - The reasons why a Suspicious Activity Report (SAR) was, or was not, submitted should be recorded
  - Any communications made with or received from the authorities, including the NCA, in relation to a SAR should be maintained on file
  - In cases where advance notice of a transaction or of arrangements is given, the need for prior consent before it is allowed to proceed should be considered

General legal and regulatory obligations

POCA ss 330, 331
Terrorism Act s 21A

6.1 Persons in the regulated sector are required to make a report in respect of information that comes to them within the course of a business in the regulated sector:

- where they *know* or
- where they *suspect* or
- where they *have reasonable grounds for knowing or suspecting*

that a person is engaged in, or attempting, money laundering or terrorist financing. Within this guidance, the above obligations are collectively referred to as "grounds for knowledge or suspicion".

Regulation ~~20(2)(d)~~19(4)(d)
POCA s 330

6.2 In order to provide a framework within which suspicion reports may be raised and considered:

- each firm must ensure that any member of staff reports to the firm's nominated officer or their appointed alternate[1] (who may also be the MLRO in an FCA-regulated firm), where they have grounds for knowledge or suspicion that a person or customer is engaged in, or attempting, money laundering or terrorist financing;
- the firm's nominated officer must consider each such report, and determine whether it gives grounds for knowledge or suspicion;
- firms should ensure that staff are appropriately trained in their obligations, and in the requirements for making reports to their nominated officer.

Regulation ~~21~~ 21(5)

Regulation 24

POCA, s 331
Terrorism Act s 21A

6.3 If the nominated officer determines that a report does give rise to grounds for knowledge or suspicion, he must report the matter to the NCA. Under POCA, the nominated officer is required to make a report to the NCA as soon as is practicable if he has grounds for suspicion that another person, whether or not a customer, is engaged in money laundering. Under the Terrorism Act, similar conditions apply in relation to disclosure where there are grounds for suspicion of terrorist financing.

6.4 A sole trader with no employees who knows or suspects, or where there are reasonable grounds to know or suspect, that a customer of his, or the person on whose behalf the customer is acting, is or has been engaged in, or attempting, money laundering or terrorist financing, must make a report promptly to the NCA.

POCA ss 333A -334
Terrorism Act ss 21D-H, 39

6.5 It is a criminal offence for any person, following a disclosure to a nominated officer or to the NCA, to release information that might 'tip off' another person that a disclosure has been made if the disclosure is likely to prejudice an investigation, if the information released came to that person in the course of a business in the UK regulated sector. It is also an offence for a person to disclose that an investigation into allegations that an offence has been committed is being contemplated or is being carried out; the disclosure is likely to prejudice that investigation and the information on which the disclosure is based came to the person in the course of a business in the regulated sector. It is also an offence for a person to disclose to another anything which is likely to prejudice an investigation resulting from a disclosure, or where the person knows or has reasonable cause to suspect that a disclosure has been or will be made.

Financial sanctions legislation

6.6 It is a criminal offence to make funds, economic resources or, in certain circumstances, financial services available to those persons or entities listed as the targets of financial sanctions legislation (see Part III, section 4). There is also a requirement to report to HM Treasury both details of funds frozen and where firms have knowledge or suspicion that a customer of the firm or a person with whom the firm

[1] References in this chapter to 'nominated officer' should be taken to include 'or their appointed alternate' where applicable.

has had business dealings is a listed person or entity, a person acting on behalf of a listed person or entity or has committed an offence under the sanctions legislation.

Attempted offences

POCA, s 330

Terrorism Act s21A(2)

6.7 POCA and the Terrorism Act provide that a disclosure must be made where there are grounds for suspicion that a person is engaged in money laundering or terrorist financing. "Money laundering" is defined in POCA to include an attempt to commit an offence under s327-329 of POCA. Similarly, under the Terrorism Act a disclosure must be made where a person has knowledge or suspicion that 'another person had committed *or attempted to commit* an offence under any of the sections 15-18'. There is no duty under s330 of POCA or s21A of the Terrorism Act to disclose information about the person who unsuccessfully attempts to commit fraud. This is because the attempt was to commit fraud, rather than to commit an offence under those Acts.

6.8 However, as soon as the firm has reasonable grounds to know or suspect that any benefit has been acquired, whether by the fraudster himself or by any third party, so that there is criminal property or terrorist property in existence, then, subject to paragraph 6.9, knowledge or suspicion of money laundering or terrorist financing must be reported to the NCA (see paragraphs 6.40ff). Who carried out the criminal conduct, and who benefited from it, or whether the conduct occurred before or after the passing of POCA, is immaterial to the obligation to disclose, but should be reported if known.

POCA, s330(3A)

6.9 In circumstances where neither the identity of the fraudster, nor the location of any related criminal property, is known nor is likely to be discovered, limited useable information is, however, available for disclosure. An example of such circumstances would be the theft of a chequebook, debit card, credit card, or charge card, which can lead to multiple low-value fraudulent transactions over a short, medium, or long term. In such instances, there is no obligation to make a report to the NCA where none of the following is known or suspected:

- the identity of the person who is engaged in money laundering;
- the whereabouts of any of the laundered property;
- that any of the information that is available would assist in identifying that person, or the whereabouts of the laundered property.

What is meant by "knowledge" and "suspicion"?

POCA, s 330 (2),(3), s 331 (2), (3)
Terrorism Act ss21A, 21ZA, 21ZB

6.10 Having knowledge means actually knowing something to be true. In a criminal court, it must be proved that the individual *in fact* knew that a person was engaged in money laundering. That said, knowledge can be *inferred* from the surrounding circumstances; so, for example, a failure to ask obvious questions may be relied upon by a jury to imply knowledge. The knowledge must, however, have

come to the firm (or to the member of staff) in the course of business, or (in the case of a nominated officer) as a consequence of a disclosure under s 330 of POCA or s 21A of the Terrorism Act. Information that comes to the firm or staff member in other circumstances does not come within the scope of the regulated sector obligation to make a report. This does not preclude a report being made should staff choose to do so, or are obligated to do so by other parts of these Acts.

6.11 Suspicion is more subjective and falls short of proof based on firm evidence. Suspicion has been defined by the courts as being beyond mere speculation and based on some foundation, for example:

> *"A degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not";* and
>
> *"Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation."*

6.12 A transaction which appears unusual is not necessarily suspicious. Even customers with a stable and predictable transactions profile will have periodic transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. So the unusual is, in the first instance, only a basis for further enquiry, which may in turn require judgement as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.

6.13 A member of staff, including the nominated officer, who considers a transaction or activity to be suspicious, would not necessarily be expected either to know or to establish the exact nature of any underlying criminal offence, or that the particular funds or property were definitely those arising from a crime or terrorist financing.

6.14 Transactions, or proposed transactions, ~~as part of~~such as '419' scams, are attempted advance fee frauds, and not money laundering; they are therefore not reportable under POCA or the Terrorism Act, unless the fraud is successful, and the firm is aware of resulting criminal property.

What is meant by "reasonable grounds to know or suspect"?

POCA, s 330 (2)(b), s 331 (2)(b) Terrorism Act s 21A

6.15 In addition to establishing a criminal offence when suspicion or actual knowledge of money laundering/terrorist financing is proved, POCA and the Terrorism Act introduce criminal liability for failing to disclose information when reasonable grounds exist for knowing or suspecting that a person is engaged in money laundering/terrorist financing. This introduces an objective test of suspicion. The test would likely be met when there are demonstrated to be facts or circumstances, known to the member of staff, from which a reasonable person engaged in a business subject to the ML Regulations would

have inferred knowledge, or formed the suspicion, that another person was engaged in money laundering or terrorist financing.

6.16 To defend themselves against a charge that they failed to meet the objective test of suspicion, staff within financial sector firms would need to be able to demonstrate that they took reasonable steps in the particular circumstances, in the context of a risk-based approach, to know the customer and the rationale for the transaction, activity or instruction. It is important to bear in mind that, in practice, members of a jury may decide, with the benefit of hindsight, whether the objective test has been met.

6.17 Depending on the circumstances, a firm being served with a court order in relation to a customer may give rise to reasonable grounds for suspicion in relation to that customer. In such an event, firms should review the information it holds about that customer across the firm, in order to determine whether or not such grounds exist.

Internal reporting

Regulation ~~20(2)(d)(ii)~~ 19(4)(d)
POCA s 330(5)

6.18 The obligation to report to the nominated officer within the firm where they have grounds for knowledge or suspicion of money laundering or terrorist financing is placed on all relevant employees in the regulated sector. All financial sector firms therefore need to ensure that all relevant employees know who they should report suspicions to.

6.19 Firms may wish to set up internal systems that allow staff to consult with their line manager before sending a report to the nominated officer. The obligation under POCA is to report 'as soon as is reasonably practicable', and so any such consultations should take this into account. Where a firm sets up such systems it should ensure that they are not used to prevent reports reaching the nominated officer whenever staff have stated that they have knowledge or suspicion that a transaction or activity may involve money laundering or terrorist financing.

6.20 Whether or not a member of staff consults colleagues, the legal obligation remains with the staff member to decide for himself whether a report should be made; he must not allow colleagues to decide for him. Where a colleague has been consulted, he himself will then have knowledge on the basis of which he must consider whether a report to the nominated officer is necessary. In such circumstances, firms should make arrangements such that the nominated officer only receives one report in respect of the same information giving rise to knowledge or suspicion.

6.21 Short reporting lines, with a minimum number of people between the person with the knowledge or suspicion and the nominated officer, will ensure speed, confidentiality and swift access to the nominated officer.

6.22 All suspicions reported to the nominated officer should be documented, or recorded electronically. The report should include full

details of the customer who is the subject of concern and as full a statement as possible of the information giving rise to the knowledge or suspicion. All internal enquiries made in relation to the report should also be documented, or recorded electronically. This information may be required to supplement the initial report or as evidence of good practice and best endeavours if, at some future date, there is an investigation and the suspicions are confirmed or disproved.

6.23 Once an employee has reported his suspicion in an appropriate manner to the nominated officer, or to an individual to whom the nominated officer has delegated the responsibility to receive such internal reports, he has fully satisfied his statutory obligation.

6.24 Until the nominated officer advises the member of staff making an internal report that no report to the NCA is to be made, further transactions or activity in respect of that customer, whether of the same nature or different from that giving rise to the previous suspicion, should be reported to the nominated officer as they arise.

Non-UK offences

POCA, s 340 (2), (11)
SOCPA, s 102

6.25 The offence of money laundering, and the duty to report under POCA, apply in relation to the proceeds of any criminal activity, wherever conducted (including abroad), that would constitute an offence if it took place in the UK. However, this broad scope excludes activity (other than those referred to in paragraph 6.26) which the firm, staff member or nominated officer knows, or believes on reasonable grounds, to have been committed in a country or territory outside the UK and the activity was not unlawful under the criminal law then applying in the country or territory concerned. Firms may nevertheless have an obligation to report in that overseas country or territory, through an appropriate overseas reporting officer.

SI 2006/1070
1968 c 65
1976 c 32
2000 c 8

6.26 Offences committed overseas which the Secretary of State has prescribed by order as remaining within the scope of the duty to report under POCA are those which are punishable by imprisonment for a maximum term in excess of 12 months in any part of the United Kingdom if they occurred there, other than:

- an offence under the Gaming Act 1968;
- an offence under the Lotteries and Amusements Act 1976; or
- an offence under ss 23 or 25 of FSMA

Terrorism Act
s21A(11)

6.27 The duty to report under the Terrorism Act applies in relation to taking any action, or being in possession of a thing, that is unlawful under ss 15-18 of that Act, that would have been an offence under these sections of the Act had it occurred in the UK.

POCA s 331
POCA ss 327-329
Terrorism Act s 21A

6.28 The obligation to consider reporting to the NCA applies only when the nominated officer has received a report made by someone working within the UK regulated sector, or when he himself becomes aware of such a matter in the course of relevant business (which may come from overseas, or from a person overseas). The nominated officer is not, therefore, obliged to report everything that comes to his attention from outside of the UK, although he would be prudent to exercise his

judgement in relation to information that comes to his attention from non-business sources. In reaching a decision on whether to make a disclosure, the nominated officer must bear in mind the need to avoid involvement in an offence under ss327-329 of POCA.

Evaluation and determination by the nominated officer

Regulation ~~20(2)(d)~~21(5)

6.29 The firm's nominated officer must consider each report and determine whether it gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion. The firm must permit the nominated officer to have access to any information, including 'know your customer' information, in the firm's possession which could be relevant. The nominated officer may also require further information to be obtained, from the customer if necessary, or from an intermediary who introduced the customer to the firm, to the extent that the introducer still holds the information (bearing in mind his own record keeping requirements). Any approach to the customer or to the intermediary should be made sensitively, and probably by someone other than the nominated officer, to minimise the risk of alerting the customer or an intermediary that a disclosure to the NCA may be being considered.

6.30 When considering an internal suspicion report, the nominated officer, taking account of the risk posed by the transaction or activity being addressed, will need to strike the appropriate balance between the requirement to make a timely disclosure to the NCA, especially if consent is required, and any delays that might arise in searching a number of unlinked systems and records that might hold relevant information.

6.31 As part of the review, other known connected accounts or relationships may need to be examined. Connectivity can arise commercially (through linked accounts, introducers, etc.), or through individuals (third parties, controllers, signatories etc.). Given the need for timely reporting, it may be prudent for the nominated officer to consider making an initial report to the NCA prior to completing a full review of linked or connected relationships, which may or may not subsequently need to be reported to the NCA.

6.32 If the nominated officer decides not to make a report to the NCA, the reasons for not doing so should be clearly documented, or recorded electronically, and retained with the internal suspicion report.

External reporting

Regulation ~~20(2)(d)~~19(4)(d)
POCA, s 331
Terrorism Act, s 21A

6.33 The firm's nominated officer must report to the NCA any transaction or activity that, after his evaluation, he knows or suspects, or has reasonable grounds to know or suspect, may be linked to money laundering or terrorist financing, or to attempted money laundering or terrorist financing. Such reports must be made as soon as is

reasonably practicable after the information comes to him.

POCA, s 339

6.34 POCA provides that the Secretary of State may by order prescribe the form and manner in which a disclosure under s330, s331, s332 or s338 may be made. Although a consultation paper on the form and manner of reporting was issued by the Home Office in the summer of 2007, the Home Office decided, on a recommendation from the NCA, not to proceed with the introduction of such an order.

6.35 The NCA prefers that SARs are submitted electronically via the secure internet system SAR~~s~~ Online, or via a dedicated bulk reporting facility. Information about access to and guidance on the use of SAR~~s~~ Online can be found at. http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu/how-to-report-sars ~~www.ukciu.gov.uk/(nrajwkjokzajrk3t3e0g41rw)/saronline.aspx~~.

6.36 In order that an informed overview of the situation may be maintained, all contact between particular departments/branches and law enforcement agencies should be controlled through, or reported back to a single contact point, which will typically be the nominated officer. In the alternative, it may be appropriate to route communications through an appropriate member of staff in the firm's legal or compliance department.

6.37 A SAR's intelligence value is related to the quality of information it contains. A firm needs to have good base data from which to draw the information to be included in the SAR; there needs to be a system to enable the relevant information to be produced in hard copy for the law enforcement agencies, if requested under a court order.

6.38 Firms should include in each SAR as much relevant information about the customer, transaction or activity that it has in its records. In particular, the law enforcement agencies have indicated that details of an individual's occupation/company's business and National Insurance number are valuable in enabling them to access other relevant information about the customer. As there is no obligation to collect this information (other than in very specific cases), a firm may not hold these details for all its customers; where it has obtained this information in the course of normal business, however, it would be helpful to include it as part of a SAR made by the firm. The NCA's website (http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu/how-to-report-sars) contains guidance on completing SARs in a way that gives most assistance to law enforcement. In particular, the NCA has published a glossary of terms, and find it helpful if firms use these terms when completing a SAR. NCA also publish, from time to time, guides to reporting entities.

Financial sanctions legislation

6.39 Firms must report to HM Treasury details of funds frozen under financial sanctions legislation and where the firm has knowledge or a suspicion that the financial sanctions measures have been or are being contravened, or that a customer is a listed person or entity, or a person acting on behalf of a listed person or entity. The firm may also need to consider whether the firm has an obligation also to report under POCA or the Terrorism Act.

Where to report

6.40 To avoid committing a failure to report offence, nominated officers must make their disclosures to the NCA. The national reception point for disclosure of suspicions, and for seeking consent to continue to proceed with the transaction or activity, is the UKFIU within the NCA

6.41 The UKFIU address is PO Box 8000, London, SE11 5EN and it can be contacted during office hours on: 020 7238 8282. Urgent disclosures, i.e., those requiring consent, should be transmitted electronically over a previously agreed secure link or, if secure electronic methods are not available, by fax, as specified on the NCA website at www.~~soca~~nationalcrimeagency.gov.uk. Speed of response is assisted if the appropriate consent request is clearly mentioned in the title of any faxed report (http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu/how-to-report-sars). ~~www.ukciu.gov.uk/(nrajwkjokzajrk3t3e0g41rw)/saronline.aspx).~~

6.42 To avoid committing a failure to report offence under financial sanctions legislation, firms must make their reports to HM Treasury. The relevant unit is the Office of Financial Sanctions Implementation, HM Treasury, 1 Horse Guards Road, London SW1A 2HQ. Reports can be submitted electronically at ofsi@hmtreasury.gsi.gov.uk and the Unit can be contacted by telephone on 020 7270 5454.

Sanctions and penalties

POCA s334
Terrorism Act s21A

6.43 Where a person fails to comply with the obligation under POCA or the Terrorism Act to make disclosures to a nominated officer and/or the NCA as soon as practicable after the information giving rise to the knowledge or suspicion comes to the member of staff, a firm is open to criminal prosecution or regulatory censure. The criminal sanction, under POCA or the Terrorism Act, is a prison term of up to five years, and/or a fine.

Financial sanctions legislation

6.44 Where a firm fails to comply with the obligations to freeze funds, not to make funds, economic resources and, in relation to suspected terrorists, financial services, available to listed persons or entities or to report knowledge or suspicion, it is open to prosecution.

Consent

6.45 Care should be taken that the requirement to obtain consent for a particular transaction does not lead to the unnecessary freezing of a customer's account, thus affecting other, non-suspicious transactions.

Consent under POCA

POCA s 336

6.46 Reporting before or reporting after the event are not equal options which a firm can choose between. Where a customer instruction is

received prior to a transaction or activity taking place, or arrangements being put in place, and there are grounds for knowledge or suspicion that the transaction, arrangements, or the funds/property involved, may relate to money laundering, a report must be made to the NCA and consent sought to proceed with that transaction or activity. In such circumstances, it is an offence for a nominated officer to consent to a transaction or activity going ahead within the seven working day notice period from the working day following the date of disclosure, unless the NCA gives consent. Where urgent consent is required, use should be made of the process referred to in paragraph 6.41 above.

POCA ss 330 (6)(a), 331(6), 338 (3)(b)

6.47 When a transaction which gives rise to concern is already within an automated clearing or settlement system, where a delay would lead to a breach of a contractual obligation, or where it would breach market settlement or clearing rules, the nominated officer may need to let the transaction proceed and report it later. Where the nominated officer intends to make a report, but delays doing so for such reasons, POCA provides a defence from making a report where there is a reasonable excuse for not doing so. However, it should be noted that this defence is untested by case law, and would need to be considered on a case-by-case basis.

6.48 When consent is needed to undertake a future transaction or activity, or to enter into an arrangement, the disclosure should be sent electronically (ensuring that the tick box for a consent request is marked) or, if electronic methods are not available, faxed to the NCA UKFIU Consent Desk immediately the suspicion is identified. Consent requests should not be sent by post due to the timings involved, and additional postal copies are not required following submission by electronic means or fax. Further information is available on the NCA website ~~www.soca.gov.uk.~~www.nationalcrimeagency.gov.uk. The Consent Desk will apply NCA policy to each submission, carrying out the necessary internal enquiries, and will contact the appropriate law enforcement agency, where necessary, for a consent recommendation. Once the NCA's decision has been reached, the disclosing firm will be informed of the decision by telephone, and be given a consent number, which should be recorded. A formal consent letter will follow.

POCA, s 335

6.49 In the event that the NCA does not refuse consent within seven working days following the working day after the disclosure is made, the firm may process the transaction or activity, subject to normal commercial considerations. If, however, consent is refused within that period, a restraint order must be obtained by the authorities within a further 31 calendar days (the moratorium period[2]) from the day consent is refused, if they wish to prevent the transaction going ahead after that date. In cases where consent is refused, the law enforcement agency refusing consent should be consulted to establish what information can be provided to the customer.

POCA, s 335(1)(b)

6.50 Consent from the NCA (referred to as a 'notice' in POCA), or the absence of a refusal of consent within seven working days following

[2] The Criminal Finances Bill currently before Parliament proposes changes to this regime.

the working day after the disclosure is made, provides the person handling the transaction or carrying out the activity, or the nominated officer of the reporting firm, with a defence against a possible later charge of laundering the proceeds of crime in respect of that transaction or activity if it proceeds.

Consent under Terrorism Act

Terrorism Act s21ZA

6.51 A person does not commit an offence under the Terrorism Act where, before becoming involved in a transaction or arrangement relating to money or other property which he suspects or believes is terrorist property, a report is made to the NCA and consent sought to proceed with that transaction or arrangement. In such circumstances, it is an offence for an authorised officer to consent to a transaction or arrangement going ahead within the seven working day notice period from the working day following the date of disclosure to the NCA, unless the NCA gives consent. [Where urgent consent is required, use should be made of the process referred to in paragraph 6.41 above.]

Formatted: Highlight

Terrorism Act s21ZB

6.52 When a transaction which gives rise to concern is already within an automated clearing or settlement system, where a delay would lead to a breach of a contractual obligation, or where it would breach market settlement or clearing rules, the authorised officer may need to let the transaction proceed and report it later. Where the nominated officer intends to make a report, but delays doing so for such reasons, the Terrorism Act provides a defence from making a report where there is a reasonable excuse for not doing so, so long as the report is made on his own initiative and as soon as it is reasonably practical for the person to make it. However, it should be noted that this defence is untested by case law, and would need to be considered on a case-by-case basis.

6.53 When consent is needed to undertake a future transaction or activity, or to enter into an arrangement, the disclosure should be sent electronically (ensuring that the tick box for a consent request is marked) or, if secure electronic methods are not available, faxed to the NCA UKFIU Consent Desk immediately the suspicion is identified. Consent requests should not be sent by post due to the timings involved, and additional postal copies are not required following submission by electronic means or fax. Further information is available on the NCA website www.~~soca~~nationalcrimeagency.gov.uk. The Consent Desk will carry out the necessary internal enquiries, and will contact the appropriate law enforcement agency, where necessary, for a consent recommendation. Once the NCA's decision has been reached, the disclosing firm will be informed of the decision by telephone, and be given a consent number, which should be recorded. A formal consent letter will follow.

Terrorism Act s21ZA(2)

6.54 In the event that the NCA does not refuse consent within seven working days following the working day after the disclosure is made, the firm may proceed with the transaction or arrangement, subject to normal commercial considerations. In cases where consent is refused, the law enforcement agency refusing consent should be consulted to establish what information can be provided to the customer.

Terrorism Act S21ZA(1)-(3)

6.55 Consent from the NCA (referred to as a 'notice' in the Terrorism Act), or the absence of a refusal of consent within seven working days following the working day after the disclosure is made, provides the person handling the transaction or arrangement, or the nominated officer of the reporting firm, with a defence against a possible later charge under the Terrorism Act in respect of that transaction or arrangement if it proceeds.

General

6.56 The consent provisions can only apply where there is prior notice to the NCA of the transaction or activity; the NCA cannot provide consent after the transaction or activity has occurred. The receipt of a SAR after the transaction or activity has taken place will be dealt with as an ordinary standard SAR, and in the absence of any instruction to the contrary, a firm will be free to operate the customer's account under normal commercial considerations until such time as the LEA determines otherwise through its investigation.

6.57 Where there is a need to take urgent action in respect of an account, and the seven working day consent notice period applies, the NCA will endeavour to provide a response in the shortest timeframe, taking into consideration the circumstances of the particular case. Where possible, this will be sooner than the seven working day time limit. If the customer makes strong demands for the transaction/activity to proceed, the NCA will put the firm in touch with the investigating law enforcement agency for guidance, in order to prevent the customer being alerted to the fact of suspicion and that a disclosure has been made. In these circumstances, each case will be dealt with on its merits.

6.58 In order to provide a defence against future prosecution for failing to report, the reasons for any conscious decision not to report should be documented, or recorded electronically. An appropriate report should be made as soon as is practicable after the event, including full details of the transaction, the circumstances precluding advance notice, and to where any money or assets were transferred.

6.59 The consent regime as it currently operates in the UK is a difficult one for financial practitioners to work with, and continues to be a matter of discussion between the industry and the authorities. There are operational challenges and legal uncertainties concerning what can realistically constitute a 'pre-event' transaction. There are customer service implications - the potentially litigious consequences of declining a customer's instructions, the inability to give an explanation because of the risk of tipping-off and the problematic requirement referred to in 6.73 for (in particular, large) deposit-taking institutions to seek consent for all post-disclosure transactions over £250.

Tipping off, and prejudicing an investigation

POCA s 333A (1), (3)
Terrorism Act, s 21D

6.60 POCA and the Terrorism Act each contains two separate offences of tipping off and prejudicing an investigation. The first offence relates to disclosing that an internal or external report has been made; the second relates to disclosing that an investigation is being contemplated or is being carried out. These offences are similar and overlapping, but there are also significant differences between them. It is important for those working in the regulated sector to be aware of the conditions precedent for each offence. Each offence relates to situations where the information on which the disclosure was based came to the person making the disclosure in the course of a business in the regulated sector. There are a number of permitted disclosures that do not give rise to these offences (see paragraphs 6.63 to 6.66).

POCA ss 333A (1), 333D(3)
Terrorism Act,
ss 21D(1), 21G(3)

6.61 Once an internal or external suspicion report has been made, it is a criminal offence for anyone to disclose information about that report which is likely to prejudice an investigation that might be conducted following that disclosure. An offence is not committed if the person does not know or suspect that the disclosure is likely to prejudice such an investigation, or if the disclosure is a permitted disclosure under POCA or the Terrorism Act. Reasonable enquiries of a customer, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is prudent practice, forms an integral part of CDD measures, and should not give rise to the tipping off offence.

POCA, ss 333A(3), 333D(4)
Terrorism Act,
ss 21D(3), 21G(4)

6.62 Where a money laundering investigation is being contemplated, or being carried out, it is a criminal offence for anyone to disclose this fact if that disclosure is likely to prejudice that investigation. An offence is not committed if the person does not know or suspect that the disclosure is likely to prejudice such an investigation, or if the disclosure is a permitted disclosure under POCA or the Terrorism Act

Permitted disclosures

POCA s 333D(1)
Terrorism Act,
s 21G(1)

6.63 An offence is not committed if the disclosure is made to the FCA (or other relevant supervisor) for the purpose of:

- the detection, investigation or prosecution of a criminal offence (whether in the UK or elsewhere);
- an investigation under POCA; or
- the enforcement of any order of a court under POCA.

POCA, s 333B(1)
Terrorism Act,
Ss 21A, 21E(1)

6.64 An employee, officer or partner of a firm does not commit an offence under POCA, s333A, or the Terrorism Act, s 21A, if the disclosure is to an employee, officer or partner of the same firm.

POCA, s 333B(2)
Terrorism Act,
s 21E(2)

6.65 A person does not commit an offence if the firm making the disclosure and the firm to which it is made belong to the same group (as defined in directive 2002/87/EC), and:

- the disclosure is to a credit institution or a financial institution: and
- the firm to which the disclosure is made is situated in an EEA State, or a country imposing equivalent money laundering requirements.

POCA s 333C Terrorism Act, s 21F

6.66 A firm does not commit an offence under POCA, s333A or the Terrorism Act s21D, if the disclosure is from one credit institution to another, or from one financial institution to another, and:

- the disclosure relates to
  - a customer or former customer of the firm making the disclosure and of the firm to which the disclosure is made; or
  - a transaction involving them both; or
  - the provision of a service involving them both.
- the disclosure is for the purpose only of preventing an offence under Part 7 of POCA or under Part III of the Terrorism Act;
- the firm to which the disclosure is made is situated in an EEA State or in a country imposing equivalent money laundering requirements; and
- the firm making the disclosure and the one to which it is made are subject to equivalent duties of protection of personal data (within the meaning of the Data Protection Act 1998).

POCA, ss 335, 336 Terrorism Act, ss21ZA, ZB

6.67 The fact that a transaction is notified to the NCA before the event, and the NCA does not refuse consent within seven working days following the day after the authorized disclosure is made, or a restraint order is not obtained within the 31 day moratorium period, does not alter the position so far as 'tipping off' is concerned.

6.68 This means that a firm:

- cannot, at the time, tell a customer that a transaction is being delayed because a report is awaiting consent from the NCA;
- cannot later – unless law enforcement/the NCA agrees, or a court order is obtained permitting disclosure – tell a customer that a transaction or activity was delayed because a report had been made under POCA or the Terrorism Act; and
- cannot tell the customer that law enforcement is conducting an investigation.

6.69 The judgement in K v Natwest [2006] EWCA Civ 1039 confirmed the application of these provisions. The judgement in this case also dealt with the issue of suspicion stating that the "The existence of suspicion is a subjective fact. There is no legal requirement that there should be reasonable grounds for the suspicion. The relevant bank employee either suspects or he does not. If he does suspect, he must (either himself or through the Bank's nominated officer) inform the authorities." It was further observed that the "truth is that Parliament has struck a precise and workable balance of conflicting interests in the 2002 Act". The Court appears to have approved of the 7 and 31 day scheme and said that in relation to the limited interference with private rights that this scheme entails "many people would think that a reasonable balance has been struck". A full copy of the judgement is ~~available~~ at http://www.bailii.org/ew/cases/EWCA/Civ/2006/1039.html The court's view in this case was upheld in Shah and another v HSBC Private Bank Ltd [2012] EWHC 1283 (QB). This judgement is ~~available~~ at http://www.bailii.org/ew/cases/EWHC/QB/2012/1283.html.

6.70 If a firm receives a complaint in these circumstances, it may be unable to provide a satisfactory explanation to the customer, who may then bring a complaint to the Financial Ombudsman Service (FOS). If a firm receives an approach from a FOS casehandler about such a case, the firm should contact a member of the FOS legal department immediately.

6.71 The NCA has confirmed that, in such cases, a firm may tell the FOS's legal department about a report to the NCA and the outcome, on the basis that the FOS will keep the information confidential (which they must do, to avoid any 'tipping off'). A firm may, however, wish to take legal advice about what information it should pass on. The FOS's legal department will then ensure that the case is handled appropriately in these difficult circumstances – liaising as necessary with the NCA. FOS's communications with the customer will still be in the name of a casehandler/ombudsman, so that the customer is not alerted.

Transactions following a disclosure

6.72 Firms must remain vigilant for any additional transactions by, or instructions from, any customer or account in respect of which a disclosure has been made, and should submit further disclosures, and consent applications, to the NCA, as appropriate, if the suspicion remains.

POCA s 339A

6.73 In the case of deposit-taking institutions alone, following the reporting of a suspicion, any subsequent transactions (including 'lifestyle' payments) involving the customer or account which was the subject of the original report may only proceed if it meets the 'threshold' requirement of £250 or less; where the proposed transaction exceeds £250, permission to vary the 'threshold' payment is required from the NCA before it may proceed.

POCA s339A

6.74 If regular transactions are over this £250 threshold, the deposit taker can apply to the NCA for a Threshold Variation, and seek permission to impose a higher threshold on the account for regular payments. When seeking such a variation, the NCA requires the deposit taker to specify what 'lifestyle' payments are to be paid, which named account they are coming from and going to, and to specify the amount for each transaction.

~~The significant practical difficulties involved in meeting the legal requirements set out in paragraph 6.73 are the subject of continuing discussions with the authorities.~~

POCA, ss 337 (1), 338(4)
Terrorism Act s 21B

6.75 The disclosure provisions within POCA and the Terrorism Act protect persons making SARs from any potential breaches of confidentiality, whether imposed under contract, statute (for example, the Data Protection Act), or common law. These provisions apply to those inside and outside the regulated sector, and include reports that are made voluntarily, in addition to reports made in order to fulfil reporting obligations. The NCA has established a SARs

Confidentiality Hotline (0800 234_6657) to report breaches from reporters and end-users alike.

6.76 The NCA's consent following a disclosure is given to the reporting institution solely in relation to the money laundering offences. Consent provides the staff involved with a defence against a charge of committing a money laundering offence under ss 327-329 of POCA or a terrorist finance offence under ss 15-18 of the Terrorism Act. It is not intended to override normal commercial judgement, and a firm is not committed to continuing the relationship with the customer if such action would place the reporting institution at commercial risk.

6.77 Whether to terminate a relationship is essentially a commercial decision, and firms must be free to make such judgements. However, in the circumstances envisaged here a firm should consider liaising with the law enforcement investigating officer to consider whether it is likely that termination would alert the customer or prejudice an investigation in any other way. If there is continuing suspicion about the customer or the transaction or activities, and there are funds which need to be returned to the customer at the end of the relationship, firms should ask the NCA for consent to repatriate the funds.

6.78 Where the firm knows that the funds in an account derive from criminal activity, or that they arise from fraudulent instructions, the account must be frozen. Where it is believed that the account holder may be involved in the fraudulent activity that is being reported, then the account may need to be frozen, but the need to avoid tipping off would have to be considered.

6.79 When an enquiry is under investigation, the investigating officer may contact the nominated officer to ensure that he has all the relevant information which supports the original disclosure. This contact may also include seeking supplementary information or documentation from the reporting firm and from other sources by way of a court order. The investigating officer will therefore work closely with the nominated officer who will usually receive direct feedback on the stage reached in the investigation. There may, however, be cases when the nominated officer cannot be informed of the state of the investigation, either because of the confidential nature of the enquiry, or because it is sub judice.

6.80 Where the firm does not wish to make the payment requested by a customer, it should notify the NCA of this fact and request them to identify any information that they are prepared to allow the firm to disclose to the court and to the customer in any proceedings brought by the customer to enforce payment. The NCA should be reminded that:

- the court may ask him to appear before it to justify his position if he refuses to consent to adequate disclosure; and
- the refusal to allow adequate disclosure is likely to make it apparent to the customer that the firm's reasons for refusing payment are due to a law enforcement investigation.

6.81 If the investigating officer is able to consent to the disclosure of adequate information to permit the firm to defend itself against any proceedings brought by the customer, that information may be shown to the court and to the customer without a tipping off offence being committed. In the event that the firm and the investigating officer cannot reach agreement on the information to be disclosed, an application can be made to the court for directions and/or an interim declaration.

6.82 In any proceedings that might be brought by the customer, the firm may only disclose to the court and the other side such information as has been consented to by the investigating officer or the court.

Constructive trusts

6.83 The duty to report suspicious activity and to avoid tipping off could, in certain circumstances, lead to a potential conflict between the reporting firm's responsibilities under the criminal law and its obligations under the civil law, as a constructive trustee, to a victim of a fraud or other crimes.

6.84 A firm's liability as a constructive trustee under English law can arise when it either knows that the funds held by the firm do not belong to its customer, or is on notice that such funds may not belong to its customer. The firm will then take on the obligation of a constructive trustee for the rightful owner of the funds. If the firm pays the money away other than to the rightful owner, and it is deemed to have acted dishonestly in doing so, it may be held liable for knowingly assisting a breach of trust.

6.85 Having a suspicion that it considers necessary to report under the money laundering or terrorist financing legislation may, in certain circumstances, indicate that the firm knows that the funds do not belong to its customer, or is on notice that they may not belong to its customer. However, such suspicion may not itself be enough to cause a firm to become a constructive trustee. Case law suggests that a constructive trust will only arise when there is some evidence that the funds belong to someone other than the customer.

6.86 If, when making a suspicious activity report, a firm knows that the funds which are the subject of the report do not belong to its customer, or has doubts that they do, this fact, and details of the firm's proposed course of action, should form part of the report that is forwarded to the NCA.

6.87 If the customer wishes subsequently to withdraw or transfer the funds, the firm should, in the first instance, contact the NCA for consent. Consent from the NCA will, however, not necessarily protect the firm from the risk of committing a breach of constructive trust by transferring funds. In situations where the assistance of the court is necessary, it is open to a firm to apply to the court for directions as to whether the customer's request should be met. However, the powers of the court are discretionary, and should only be used in cases of real need. That said, it is unlikely that a firm acting upon the direction of a

court would later be held to have acted dishonestly such as to incur liability for breach of constructive trust.

6.88 Although each case must be considered on its facts, the effective use of customer information, and the identification of appropriate underlying beneficial owners, can help firms to guard against a potential constructive trust suit arising out of fraudulent misuse or misappropriation of funds.

6.89 It should be noted that constructive trust is not a concept recognised in Scots law.

Data Protection - Subject Access Requests, where a suspicion report has been made

6.90 Occasionally, a Subject Access Request under the Data Protection Act will include within its scope one or more money laundering/terrorist financing reports which have been submitted in relation to that customer. Although it might be instinctively assumed that to avoid tipping off there can be no question of ever including this information when responding to the customer, an automatic assumption to that effect must not be made, even though in practice it will only rarely be decided that it is appropriate to include it. However, all such requests must be carefully considered on their merits in line with the principles below.

6.91 The following guidance is drawn from guidance issued by HM Treasury in April 2002. This guidance – The UK's Anti-Money Laundering Legislation and the Data Protection Act 1998 – Guidance notes for the financial sector - is available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/271862/money_laundering_1_.pdf~~www.hm-treasury.gov.uk/documents/financial_services/fin_index.cfm~~.

Data Protection Act, s 7

6.92 On making a request in writing (a Subject Access Request) to a data controller (i.e. any organisation that holds personal data), an individual is normally entitled to:

- be informed whether the data controller is processing (which includes merely holding) his personal data; and if so
- be given a description of that data, the purposes for which they are being processed and to whom they are or may be disclosed; and
- have communicated to him in an intelligible form all the information that constitutes his personal data and any information available to the data controller as to the source of that data.

Data Protection Act, s 29

6.93 Section 29 of the Data Protection Act provides that personal data are exempt from disclosure under section 7 of the Act in any case where the application of that provision would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. However, even when relying on an exemption, data controllers (i.e., firms) should provide as much information as they can in response to a Subject Access Request.

6.94 Where a firm withholds a piece of information in reliance on the section 29 exemption, it is not obliged to tell the individual that any information has been withheld. The information in question can simply be omitted and no reference made to it when responding to the individual who has made the request.

6.95 To establish whether disclosure would be likely to prejudice an investigation or a potential investigation, firms should approach the NCA for guidance; the NCA will usually discuss this with past or present investigating agencies/officers. This may also involve cases that are closed, but where related investigations may still be continuing.

6.96 Each Subject Access Request must be considered on its own merits in determining whether, in a particular case, the disclosure of a suspicion report is likely to prejudice an investigation and, consequently, constitute a tipping-off offence. In determining whether the section 29 exemption applies, it is legitimate to take account of the fact that although the disclosure does not, in itself, provide clear evidence of criminal conduct when viewed in isolation, it might ultimately form part of a larger jigsaw of evidence in relation to a particular crime. It is also legitimate to take account generally of the confidential nature of suspicious activity reports when considering whether or not the exemption under section 29 might apply.

6.97 In cases where the fact that a disclosure had been made had previously been reported in legal proceedings, or in a previous investigation, and the full contents of such a disclosure had been revealed, then it is less likely that the exemption under section 29 would apply. However, caution should be exercised when considering disclosures that have been made in legal proceedings for the purposes of the section 29 exemption, as often the disclosure will have been limited strictly to matters relevant to those proceedings, and other information contained in the original report may not have been revealed.

6.98 To guard against a tipping-off offence, nominated officers should ensure that no information relating to SARs is released to any person without the nominated officer's authorisation. Further consideration may need to be given to suspicion reports received internally that have not been submitted to the NCA. A record should be kept of the steps that have been taken in determining whether disclosure of a report would involve tipping off and/or the availability of the section 29 exemption.

Data Protection Act s 7(8)

6.99 Firms should bear in mind that there is a statutory deadline for responding to Subject Access Requests of 40 days from their receipt by the firm. The timing of enquiries to the NCA, or any other party, to obtain further information, or for guidance on whether disclosure would be likely to prejudice an investigation, should be made with this deadline in mind.

CHAPTER 7

STAFF AWARENESS, TRAINING AND ALERTNESS

- **Relevant law/regulation**
  - Regulation 21, ~~21~~ 24
  - POCA ss 327-329, 330 (6),(7), 333, 334(2)
  - Terrorism Act ss 18, 21A
  - SYSC 6.3.7 (1) G
  - TC, Chapter 1
  - Financial sanctions legislation
- **Core obligations**
  - Relevant employees should be
    - made aware of the risks of money laundering and terrorist financing, the relevant legislation, and their obligations under that legislation
    - made aware of the identity and responsibilities of the firm's nominated officer and MLRO
    - trained in the firm's procedures and in how to recognise and deal with potential money laundering or terrorist financing transactions or activity
  - Staff training should be given at regular intervals, and details recorded
  - MLRO is responsible for oversight of the firm's compliance with its requirements in respect of staff training
  - The relevant director or senior manager has overall responsibility for the establishment and maintenance of effective training arrangements
- **Actions required, to be kept under regular review**
  - Provide appropriate training to make relevant employees aware of money laundering and terrorist financing issues, including how these crimes operate and how they might take place through the firm
  - Ensure that relevant employees are provided with information on, and understand, the legal position of the firm and of individual members of staff, and of changes to these legal positions
  - Consider providing relevant employees with case studies and examples related to the firm's business
  - Train relevant employees in how to operate a risk-based approach to AML/CFT

Why focus on staff awareness and training?

7.1 One of the most important controls over the prevention and detection of money laundering is to have staff who are alert to the risks of money laundering/terrorist financing and well trained in the identification of unusual activities or transactions which may prove to be suspicious.

7.2 The effective application of even the best designed control systems can be quickly compromised if the staff applying the systems are not adequately trained. The effectiveness of the training will therefore be important to the success of the firm's AML/CTF strategy.

7.3 It is essential that firms implement a clear and well-articulated policy for ensuring that relevant employees are aware of their obligations in respect of the prevention of money laundering and terrorist financing and for training them in the identification and reporting of anything that gives grounds for suspicion. This is especially important for staff

who handle customer transactions or instructions. Temporary and contract staff carrying out such functions should also be covered by these training programmes.

POCA ss 327-329, 334 (2)
Terrorism Act ss 18, 21A

7.4 Under POCA and the Terrorism Act, individual members of staff face criminal penalties if they are involved in money laundering or terrorist financing, or if they do not report their knowledge or suspicion of money laundering or terrorist financing where there are reasonable grounds for their knowing or suspecting such activity. It is important, therefore, that staff are made aware of these obligations, and are given training in how to discharge them.

General legal and regulatory obligations

SYSC 3.1.6 R
SYSC 5.1.1 R

7.5 The FCA requires authorised firms to employ personnel with the skills, knowledge and expertise necessary for the discharge of the responsibilities allocated to them.

TC 2.1
SYSC 3.1.9 G
SYSC 5.1.4A G

7.6 Firms carrying out retail activities that are subject to TC are responsible for ensuring that

- its employees are competent;
- its employees remain competent for the work they do;
- its employees are appropriately supervised;
- its employees' competence is regularly reviewed; and
- the level of competence is appropriate to the nature of the business.

Other firms may nevertheless wish to take TC into account in complying with the high-level training and competence requirement in SYSC.

Regulation 21(1)

7.6A Where appropriate with regard to the size and nature of its business, a firm must carry out screening of relevant employees and agents appointed by the firm, both before the appointment is made, and at regular intervals during the course of the appointment;

Regulation 21(2)(a)

7.6B Screening of relevant employees means an assessment of:

- the skills, knowledge and expertise of the individual to carry out their functions effectively; and
- the conduct and integrity of the individual.

Regulation 21(2)(b)

7.6C A relevant employee is one whose work is –

- relevant to the firm's compliance with any requirement in the ML Regulations; or
- otherwise capable of contributing to the
  - identification or mitigation of the risks of ML/TF to which the firm is subject; or
  - prevention or detection of ML/TF in relation to the firm's business.

	7.6D	Where an employee is found to have breached the firm's internal rules, or the FCA's Conduct Rules, there may be an obligation on the firm to report such a breach to the FCA, rather than only dealing with the matter internally.
Regulation ~~16~~24	7.7	The obligations on senior management and the firm in relation to staff awareness and staff training address each requirement separately. ML Regulations require firms to take appropriate measures to ensure ~~so~~ that ~~all relevant~~ relevant employees and agents are made aware of the law relating to money laundering and terrorist financing (and to data protection), and that they are regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.
Regulation 24(3)(a)	7.7A	In determining its training measures, firms must take account of the nature and size of its business, and the nature and extent of the risks of money laundering and terrorist financing to which its business is subject.
SYSC 6.3.9 (1) R SYSC 6.3.7 (1) G	7.8	The FCA specifically requires the MLRO to have responsibility for oversight of the firm's AML systems and controls, which include appropriate training for the firm's employees in relation to money laundering.
POCA, s 330 (6) and (7)	7.9	Where a staff member is found to have had reasonable grounds for knowing or suspecting money laundering, but failed to make a disclosure, he will have a defence under POCA if he does not know or suspect, and has not been provided with AML training by his employer. No such defence is available under the Terrorism Act.
Regulation ~~16~~24	7.10	A successful defence by a staff member under POCA may leave the firm open to prosecution or regulatory sanction for not having adequate training and awareness arrangements. Firms should therefore not only obtain acknowledgement from the individual that they have received the necessary training, but should also take steps to assess its effectiveness.

Responsibilities of the firm, and its staff

Responsibilities of senior management

Regulation ~~20~~19	7.11	Senior management must be aware of their obligations under the ML Regulations to establish appropriate ~~systems~~ policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified in the firm's risk assessment~~forestall and prevent operations relating to money laundering and terrorist financing~~. It is an offence not to have appropriate ~~systems~~ policies, controls and procedures in place, whether or not money laundering or terrorist financing has taken place.
Regulation 21(1)(a)	7.11A	Where appropriate with regard to the size and nature of its business, a firm must appoint a member of its board of directors (or equivalent

management body) as the officer responsible for the firm's compliance with the ML Regulations.

Regulation 20SYSC 4.4.7(1)
SYSC 6.3.8 R
SYSC 6.3.9 R

7.12 The An relevant director or seniorSMF manager is allocated the prescribed responsibility for the firm's policies and procedures for countering the risk that the firm might be used to further financial crimehas overall responsibility for the establishment and maintenance of effective training arrangements. The MLRO is responsible for oversight of the firm's compliance with its requirements in respect of training, including taking reasonable steps to ensure that the firm's systems and controls include appropriate training for employees in relation to money laundering and terrorist financing. Awareness and training arrangements specifically for senior management, the MLRO and the nominated officer should therefore also be considered.

7.13 As noted in paragraph 1.31, the relationship between the MLRO and the director(s)/seniorSMF manager(s) allocated the prescribed responsibility for the firm's policies and procedures for countering the risk that the firm might be used to further financial crime allocated overall responsibility for the establishment and maintenance of the firm's AML/CTF systems is one of the keys to an successful effective AML/CTF regime. It is important that this relationship is clearly defined and documented, so that each knows the extent of his, and the other's, role and day to day responsibilities.

Regulation 21(1)(a) 7.13A Where the firm is required to appoint a board member as the officer responsible for the firm's compliance with the ML Regulations, it is important that this individual, the MLRO and the SMF Manager allocated the prescribed responsibility for the firm's policies and procedures are all clear as to the responsibilities of each. Firms should ensure, in consultation with their normal regulatory contact, that the FCA understands how particular responsibilities in this area are allocated or shared.

7.14 Firms should take reasonable steps to ensure that relevant employees are aware of:

- their responsibilities under the firm's arrangements for the prevention of money laundering and terrorist financing, including those for obtaining sufficient evidence of identity, recognising and reporting knowledge or suspicion of money laundering or terrorist financing;
- the identity and responsibilities of the nominated officer and the MLRO; and
- the potential effect on the firm, on its employees personally and on its clients, of any breach of that law.

7.15 The firm's approach to training should be built around ensuring that the content and frequency of training reflects the risk assessment of the products and services of the firm and the specific role of the individual.

Responsibilities of staff

7.16 Staff should be made aware of their personal responsibilities and those

of the firm at the start of their employment. These responsibilities should be documented in such a way as to enable staff to refer to them as and when appropriate throughout their employment. In addition, selected or relevant employees should be given regular appropriate training in order to be aware of:

- the criminal law relating to money laundering and terrorist financing;
- the ML Regulations;
- the FCA Rules;
- industry guidance;
- the risks money laundering and terrorist financing pose to the business;
- the vulnerabilities of the firm's products and services; and
- the firm's policies and procedures in relation to the prevention of money laundering and terrorist financing.

7.17 Where staff move between jobs, or change responsibilities, their training needs may change. Ongoing training should be given at appropriate intervals to all relevant employees.

Legal obligations on staff

POCA, ss327 – 329, 330-332
Terrorism Act ss18, 21A

7.18 There are several sets of offences under POCA and the Terrorism Act which directly affect staff – the various offences of money laundering or terrorist financing, failure to report possible money laundering or terrorist financing, tipping off, and prejudicing an investigation.

POCA, ss327 – 329
Terrorism Act s18

7.19 The offences of involvement in money laundering or terrorist financing apply to all staff, whether or not the firm is in the regulated sector. This would include staff of general insurance firms and mortgage intermediaries. The offences have no particular application to those engaged in specific customer-related activities – that is, they also apply to back office staff.

POCA ss330-332
Terrorism Act s21A

7.20 The offence under POCA and the Terrorism Act of failing to report applies to staff in the regulated sector, and to all nominated officers, whether in the regulated sector or not. Although general insurance firms and mortgage intermediaries are not in the regulated sector, if they have opted to appoint a nominated officer, the obligations on nominated officers apply to these appointees.

POCA s333

7.21 Once a report has been made to the firm's nominated officer, it is an offence to make any further disclosure that is likely to prejudice an investigation.

Training in the firm's procedures

7.22 The firm should train staff, in particular, on how its products and services may be used as a vehicle for money laundering or terrorist financing, and in the firm's procedures for managing this risk. They will also need information on how the firm may itself be at risk of prosecution if it processes transactions without the consent of the NCA where a SAR has been made.

7.23 Relevant employees should be trained in what they need to know in order to carry out their particular role. Staff involved in customer acceptance, in customer servicing, or in settlement functions will need different training, tailored to their particular function. This may involve making them aware of the importance of the "know your customer" requirements for money laundering prevention purposes, and of the respective importance of customer ID procedures, obtaining additional information and monitoring customer activity. The awareness raising and training in this respect should cover the need to verify the identity of the customer, and circumstances when it should be necessary to obtain appropriate additional customer information in the context of the nature of the transaction or business relationship concerned.

7.24 Relevant employees should also be made aware of the particular circumstances of customers who present a higher risk of money laundering or terrorist financing, or who are financially excluded. Training should include how identity should be verified in such cases, what additional steps should be taken, and/or what local checks can be made.

Staff alertness to specific situations

7.25 Sufficient training will need to be given to all relevant employees to enable them to recognise when a transaction is unusual or suspicious, or when they should have reasonable grounds to know or suspect that money laundering or terrorist financing is taking place.

7.26 The set of circumstances giving rise to an unusual transaction or arrangement, and which may provide reasonable grounds for concluding that it is suspicious (see paragraph 6.11), will depend on the customer and the product or service in question. Illustrations of the type of situation that may be unusual, and which in certain circumstances might give rise to reasonable grounds for suspicion, are:

- transactions which have no apparent purpose, or which make no obvious economic sense (including where a person makes a loss ~~against tax~~), or which involve apparently unnecessary complexity;
- the use of non-resident accounts, companies or structures in circumstances where the customer's needs do not appear to support such economic requirements;
- where the transaction being requested by the customer, or the size or pattern of transactions, is, without reasonable explanation, out of the ordinary range of services normally requested or is inconsistent with the experience of the firm in relation to the particular customer;
- dealing with customers not normally expected in that part of the business;
- transfers to and from high-risk jurisdictions, without reasonable explanation, which are not consistent with the customer's declared foreign business dealings or interests;

- where a series of transactions are structured just below a regulatory threshold;
- where a customer who has entered into a business relationship with the firm uses the relationship for a single transaction or for only a very short period of time;
- unnecessary routing of funds through third party accounts;
- unusual investment transactions without an apparently discernible profitable motive.

7.27 Issues around the customer identification process that may raise concerns include such matters as the following:

- Has the customer refused, or appeared particularly reluctant, to provide the information requested without reasonable explanation?
- Do you understand the legal and corporate structure of the client entity, and its ownership and control, and does the structure appear to make sense?
- Is the staff member aware of any inconsistencies between the information provided and what would be expected, given the location of the customer?
- Is the area of residence given consistent with other profile details, such as employment?
- Does an address appear vague or unusual – e.g., an accommodation agency, a professional 'registered office' or a trading address?
- Does it make sense for the customer to be opening the account or relationship in the jurisdiction that he is asking for?
- Is the information that the customer has provided consistent with the banking or other services or facilities that he is seeking?
- Does the supporting documentation add validity to the other information provided by the customer?
- Does the customer have other banking or financial relationships with the firm, and does the collected information on all these relationships appear consistent?
- Does the client want to conclude arrangements unusually urgently, against a promise to provide information at a later stage, which is not satisfactorily explained?
- Has the customer suggested changes to a proposed arrangement in order to avoid providing certain information?

7.28 Staff should also be on the lookout for such things as:

- sudden, substantial increases in cash deposits or levels of investment, without adequate explanation;
- transactions made through other banks or financial firms;
- regular large, or unexplained, transfers to and from countries known for money laundering, terrorism, corruption or drug trafficking;
- large numbers of electronic transfers into and out of the account;
- significant/unusual/inconsistent deposits by third parties; and
- reactivation of dormant account(s).

7.29 Staff awareness and training programmes may also include the nature of terrorism funding and terrorist activity, in order that staff are alert to customer transactions or activities that might be terrorist-related.

7.30 Examples of activity that might suggest to staff that there could be potential terrorist activity include:

- round sum deposits, followed by like-amount wire transfers;
- frequent international ATM activity;
- no known source of income;
- use of wire transfers and the internet to move funds to and from high-risk countries and geographic locations;
- frequent address changes;
- purchases of military items or technology; and
- media reports on suspected, arrested terrorists or groups.

7.31 It is important that staff are appropriately made aware of changing behaviour and practices amongst money launderers and those financing terrorism. As well as their regular series of publications on the typologies of financial crime, FATF's Guidance for Financial Institutions in Detecting Terrorist Financing issued in April 2002 contains an in-depth analysis of the methods used in the financing of terrorism and the types of financial activities constituting potential indicators of such activities. These documents are available at www.fatf-gafi.org.

7.33 Illustrations, based on real cases, of how individuals and organisations might raise funds and use financial sector products and services for money laundering or to finance terrorism, are also available on the FATF website at www.fatf-gafi.org

7.32 The NCA publishes a range of material at www.~~soca~~nationalcrimeagency.gov.uk, such as threat assessments and risk profiles, of which firms may wish to make their staff aware. The information on this website could usefully be incorporated into firms' training materials.

Staff based outside the UK

7.34 Where activities relating to UK business operations are undertaken by processing staff outside the UK, those staff must be made aware of and trained to follow the AML/CTF policies and procedures applicable to the UK operations. It is important that any local training and awareness obligations are also met, where relevant.

Training methods and assessment

7.35 There is no single solution when determining how to deliver training; a mix of training techniques may be appropriate. On-line learning systems can often provide an adequate solution for many employees, but there will be classes of employees for whom such an approach is not suitable. Focused classroom training for higher risk or minority areas can be more effective. Relevant videos always stimulate interest,

but continually re-showing the same video may produce diminishing returns.

7.36 Procedures manuals, whether paper or intranet based, are useful in raising staff awareness and in supplementing more dedicated forms of training, but their main purpose is to provide ongoing reference and they are not generally written as training material.

7.37 Ongoing training should be given at appropriate intervals to all relevant employees. Particularly in larger firms, this may take the form of a rolling programme.

7.38 Whatever the approach to training, it is vital to establish comprehensive records (see paragraph 8.21) to monitor who has been trained, when they received the training, the nature of the training given and its effectiveness.

CHAPTER 8

RECORD KEEPING

➢ **Relevant law/regulation** ▪ Data Protection Act 1998 ▪ Regulations 18, 19 and 38-40~~20~~ ▪ SYSC Chapter 3
➢ **Core obligations** ▪ Firms must retain: • copies of, or references to, the evidence they obtained of a customer's identity, for five years after the end of the customer relationship • details of customer transactions for five years from the date of the transaction ▪ Firms should retain: • details of actions taken in respect of internal and external suspicion reports • details of information considered by the nominated officer in respect of an internal report where no external report is made
➢ **Actions required, to be kept under regular review** ▪ Firms should maintain appropriate systems for retaining records ▪ Firms should maintain appropriate systems for making records available when required, within the specified timescales

General legal and regulatory requirements

Regulation ~~19~~19(1)(a)

8.1 This chapter provides guidance on appropriate record keeping procedures that will meet a firm's obligations in respect of the prevention of money laundering and terrorist financing. There are general obligations on firms to maintain appropriate records and controls more widely in relation to their business; this guidance is not intended to replace or interpret such wider obligations.

8.2 Record keeping is an essential component of the audit trail that the ML Regulations and FCA Rules seek to establish in order to assist in any financial investigation and to ensure that criminal funds are kept out of the financial system, or if not, that they may be detected and confiscated by the authorities.

Regulation 18(4), 19(1)(b), 38(2)(b)

8.2A As well as legislating for record keeping in relation to customer identification, and transactions with customers, there are obligations on firms to document their risk assessment, and their policies, controls and procedures. See paragraphs 1.41A and 2.2A. A firm is also required to have written arrangements with any third party on which they rely to apply customer due diligence measures.

Regulation ~~19~~39
SYSC 3.2.20R
SYSC 6.3.1 R

8.3 Firms must retain records concerning customer identification and transactions as evidence of the work they have undertaken in complying with their legal and regulatory obligations, as well as for use as evidence in any investigation conducted by law enforcement. FCA-regulated firms must take reasonable care to make and keep adequate records appropriate to the scale, nature and complexity of their businesses.

8.4 Where a firm has an appointed representative, it must ensure that the representative complies with the record keeping obligations under the ML Regulations. This principle would also apply where the record keeping is delegated in any way to a third party (such as to an administrator or an introducer).

What records have to be kept?

8.5 The precise nature of the records required is not specified in the legal and regulatory regime. The objective is to ensure that a firm meets its obligations and that, in so far as is practicable, in any subsequent investigation the firm can provide the authorities with its section of the audit trail.

8.6 The firm's records should cover:

- Customer information
- Transactions
- Internal and external suspicion reports
- MLRO annual (and other) reports
- Information not acted upon
- Training and compliance monitoring
- Information about the effectiveness of training

Customer information

Regulation ~~19~~39(2)

8.7 In relation to the evidence of a customer's identity, firms must keep a copy of~~,~~ any documents or information it obtained to satisfy the CDD measures required under the ML Regulations. ~~or the references to, the evidence of the customer's identity obtained during the application of CDD measures.~~ Where a firm has received a confirmation of identity certificate, this certificate will in practice be the evidence of identity that must be kept. Some documents which may be used for evidence of identification are more sensitive than others (for example, Armed Forces Cards and Firearms certificates – see paragraph 5.3.74), and firms should deal with such evidence with care.~~:~~
~~where originals of these documents are offered, firms should consider retaining only the reference numbers and dates of issue of such documents, rather than taking actual photocopies.~~

8.8 When a firm has concluded that it should treat a client as financially excluded for the purposes of customer identification, it should keep a record of the reasons for doing so.

8.9 A firm may often hold additional information in respect of a customer obtained for the purposes of enhanced customer due diligence or ongoing monitoring.

~~8.10~~ ~~Where the individual presents himself to the firm, or at one of its branches, he may produce the necessary evidence of identity for the firm to take and retain copies. In circumstances (such as where verification is carried out at a customer's home and photocopying facilities are not available) where it would not be possible to take a~~

~~copy of the evidence of identity, a record should be made of the type of document and its number, date and place of issue, so that, if necessary, the document may be re-obtained from its source of issue.~~

8.11 The Home Office current guidance on copying passports is available at http://www.nationalarchives.gov.uk/documents/information-management/reproduction-british-passport.pdf

Regulation ~~19(3)~~39(3)(b)(ii)

8.12 Records of identification evidence must be kept for a period of ~~at least~~ five years after the business relationship with the customer has ended, ~~. The date the relationship with the customer ends is the date:~~

~~an occasional transaction, or the last in a series of linked transactions, is carried out; or~~
~~the business relationship ended,~~ i.e. the closing of the account or accounts.

Regulation 39(4)

8.12A Upon the expiry of the five year period referred to in paragraph 8.12, firms must delete any personal data unless:

- the firm is required to retain records containing personal data by, or under, any enactment, or for the purposes of any court proceedings; or
- the data subject has given express consent to the retention of that data.

Regulation 39(5)

8.12B A firm which is relied on by another firm for the purposes of customer due diligence must keep the records referred to in paragraph 8.7 for five years beginning on the date on which the firm was relied on.

8.13 Where documents verifying the identity of a customer are held in one part of a group, they do not need to be held in duplicate form in another. The records do, however, need to be accessible to the nominated officer and the MLRO and to all areas that have contact with the customer, and be available on request, where these areas seek to rely on this evidence, or where they may be called upon by law enforcement to produce them.

8.14 When an introducing branch or subsidiary undertaking ceases to trade or have a business relationship with a customer, as long as his relationship with other group members continues, particular care needs to be taken to retain, or hand over, the appropriate customer records. Similar arrangements need to be made if a company holding relevant records ceases to be part of the group. This will also be an issue if the record keeping has been delegated to a third party.

Transactions

8.15 All transactions carried out on behalf of or with a customer in the course of relevant business must be recorded within the firm's records. Transaction records in support of entries in the accounts, in whatever form they are used, e.g. credit/debit slips, cheques, should be maintained in a form from which a satisfactory audit trail may be compiled where necessary, and which may establish a financial profile of any suspect account or customer.

Regulation 3~~1~~9(3)

8.16 Records of all transactions relating to a customer must be retained for a period of five years from:~~the date on which the transaction is completed.~~

- where the records relate to an occasional transaction, the date when the transaction is completed; or
- in other cases, the date the business relationship ended, i.e. the closing of the account or accounts.

8.17 In the case of managers of investment funds or issuers of electronic money, where there may be no business relationship as defined in the ML Regulations, but the customer may nevertheless carry out further occasional transactions in the future, it is recommended that all records be kept for five years after the investment has been fully sold or funds disbursed.

Regulation 39(4)

8.18A Upon the expiry of the five year period referred to in paragraph 8.16, firms must delete any personal data unless:

- the firm is required to retain records containing personal data by, or under, any enactment, or for the purposes of any court proceedings; or
- the data subject has given express consent to the retention of that data.

Internal and external reports

8.18 A firm should make and retain:

- records of actions taken under the internal and external reporting requirements; and
- when the nominated officer has considered information or other material concerning possible money laundering, but has not made a report to the NCA, a record of the other material that was considered.

8.19 In addition, copies of any SARs made to the NCA should be retained.

8.20 Records of all internal and external reports should be retained for five years from the date the report was made.

Other

8.21 A firm's records should include:

(a) in relation to training:

- dates AML training was given;
- the nature of the training;
- the names of the staff who received training; and
- the results of the tests undertaken by staff, where appropriate.

(b) in relation to compliance monitoring -

- reports by the MLRO to senior management; and
- records of consideration of those reports and of any action taken as a consequence.

Regulation 20(4)21(8),(9)

8.22 A firm must establish and maintain systems which enable it to respond fully and rapidly to enquiries from financial investigators accredited under s3 of POCA, persons acting on behalf of the Scottish Ministers in their capacity as an enforcement authority under the Act, officers of HMRC or constables, relating to:

- whether it maintains, or has maintained during the previous five years, a business relationship with any person; and
- the nature of that relationship.

Form in which records have to be kept

8.23 Most firms have standard procedures which they keep under review, and will seek to reduce the volume and density of records which have to be stored, whilst still complying with statutory requirements. Retention may therefore be:

- by way of original documents;
- by way of photocopies of original documents;
- on microfiche;
- in scanned form;
- in computerised or electronic form.

8.24 The record retention requirements are the same, regardless of the format in which they are kept, or whether the transaction was undertaken by paper or electronic means.

8.25 Firms involved in mergers, take-overs or internal reorganisations need to ensure that records of identity verification and transactions are readily retrievable for the required periods when rationalising computer systems and physical storage arrangements.

Location

8.26 The ML Regulations do not state where relevant records should be kept, but the overriding objective is for firms to be able to retrieve relevant information without undue delay.

8.27 Where identification records are held outside the UK, it is the responsibility of the UK firm to ensure that the records available do in fact meet UK requirements. No secrecy or data protection legislation should restrict access to the records either by the UK firm freely on request, or by UK law enforcement agencies under court order or relevant mutual assistance procedures. If it is found that such restrictions exist, copies of the underlying records of identity should, wherever possible, be sought and retained within the UK.

8.28 Firms should take account of the scope of AML/CTF legislation in

other countries, and should ensure that group records kept in other countries that are needed to comply with UK legislation are retained for the required period.

~~8.29~~ ~~Records relating to ongoing investigations should, where possible, be retained until the relevant law enforcement agency has confirmed that the case has been closed. However, if a firm has not been advised of an ongoing investigation within five years of the disclosure being made, the records may be destroyed in the normal course of the firm's records management policy.~~

8.30 There is tension between the provisions of the ML Regulations and data protection legislation; the nominated officer and the MLRO must have due regard to both sets of obligations.

8.31 When setting document retention policy, financial sector businesses must weigh the statutory requirements and the needs of the investigating authorities against normal commercial considerations. When original vouchers are used for account entry, and are not returned to the customer or his agent, it is of assistance to the law enforcement agencies if these original documents are kept ~~for at least one year~~ to assist in forensic analysis. This can also provide evidence for firms when conducting their own internal investigations. However, this is not a requirement of the AML legislation ~~and there is no other statutory requirement in the UK that would require the retention of these original documents.~~ , and retaining electronic/digital copies may be a more realistic storage method.

Sanctions and penalties

Regulation ~~45(1)~~83(1) 8.32 Where the record keeping obligations under the ML Regulations are not observed, a firm or person is open to prosecution, including imprisonment for up to two years and/or a fine, or regulatory censure.