The UK anti-money laundering regime: Statutory offences and the role of the FSA

SLAUGHTER AND MAY
March 2009
CONTENTS

1. Part 1: The UK statutory framework 1
   1.1 Introduction 1
   1.2 Statutory offences 2
   1.3 Proceeds of Crime Act 4
      1.3.1 The principal money laundering offences 4
      1.3.2 The failure to disclose offences 11
      1.3.3 The tipping-off offences 18
      1.3.4 Practical issues associated with the consent regime 22
   1.4 The Terrorism Act 2000 26
      1.4.1 The terrorist finance offences 26
      1.4.2 The failure to disclose offences 30
      1.4.3 The tipping-off offence 32
      1.4.4 Practical issues associated with the consent regime 34
   1.5 The Wire Transfer Regulation 34
   1.6 Investigations, confiscation and asset freezing 36
      1.6.1 Investigatory orders 36
      1.6.2 Asset recovery and other remedies 38
      1.6.3 Freezing orders and sanctions legislation 43
   1.7 Conclusion 47

2. Part 2: The role of the FSA in the UK money laundering regime 48
   2.1 Background 48
   2.2 The SYSC rules and guidance on Money Laundering 52
      2.2.1 SYSC 1 – Application and purpose 54
2.2.2 SYSC 6.1.1R/SYSC 3.2.6R – Adequate practices and procedures 55

2.2.3 SYSC 6.3.1R/SYSC 3.2.6AR – Adequacy of systems and controls 56

2.2.4 SYSC 6.3.2G/SYSC 3.2.6BG – Definition of “money laundering risk” 56

2.2.5 SYSC 6.3.3R/SYSC 3.2.6CR – Regular assessment 57

2.2.6 SYSC 6.3.4G/SYSC 3.2.6DG – Other legal obligations 57

2.2.7 SYSC 6.3.5G/SYSC 3.2.6EG – Relationship with the Guidance Notes 57

2.2.8 SYSC 6.3.6G/SYSC 3.2.6FG – Identifying money laundering risk 58

2.2.9 SYSC 6.3.7G/SYSC 3.2.6GG – Nature of systems and controls 58

2.2.10 SYSC 6.3.8R/SYSC 3.2.6HR – Senior management responsibility 60

2.2.11 SYSC 6.3.9R/SYSC 3.2.6I – The Money Laundering Reporting Officer 60

2.2.12 SYSC 6.3.10G/SYSC 3.2.6JG – The role of the Money Laundering Reporting Officer 61

2.3 Conclusion 61
1. PART 1: THE UK STATUTORY FRAMEWORK

1.1 Introduction

In this first decade of the century, we have seen in the UK a concerted effort by the Government to combat organised crime and terrorism with far-reaching and sometimes controversial measures. Attacking the financial aspects of crime and terrorism has been a key priority for law enforcement agencies, the Government and the European Union.

Estimates for the total amount of illicit funds laundered globally each year range from £1 trillion to £3 trillion; it is difficult to know whether these estimates are even remotely accurate, but it is clear that whatever the true size of the problem, the laundering of the proceeds of crime, and the financing of terrorist operations, continue to be areas of significant political and legal concern and unfortunately seems destined to remain so for some time to come.

In recent years there have been ongoing developments in the UK anti-money laundering regime; mostly these developments have been intended to strengthen rather than to liberalise the regime, and they have largely been the product of growing public and governmental concern (both in the UK and in Europe) at the way in which crime, and particularly organised criminal and terrorist enterprises, appears to have been growing. The more significant of these developments include:

- the implementation of the Third EU Money Laundering Directive (the "Third Directive") in the UK in the form of the Money Laundering Regulations 2007 (the "2007 Regulations"), replacing the earlier Money Laundering Regulations 2003 (the "2003 Regulations");
- the replacement of the FSA's Money Laundering Sourcebook with high-level principles in the Senior Management Arrangements, Systems and Controls Sourcebook;
- the consolidation of the functions of, among others, the National Criminal Intelligence Service and the Asset Recovery Agency, into a single money laundering enforcement and recovery agency, SOCA; and
- revisions to the tipping-off offences under the Proceeds of Crime Act 2002 ("POCA") and the Terrorism Act 2000 (the "Terrorism Act").

Balancing the costs and inconveniences for financial sector businesses of compliance requirements with issues of public safety, criminal justice and financial stability is certainly not an easy task; and it is not made any easier during a period in which governments generally as far as possible want to minimise burdens on businesses to stimulate economic growth.

The financial sector is experiencing a period of turmoil which is unprecedented in recent history. In these conditions, it would not be surprising to find that for senior management at some firms, matters of day-to-day compliance, including anti-money laundering requirements, have not been at the top of the list of priorities. Not surprising perhaps, but not acceptable as far as the key anti-money laundering authorities, the Financial Services Authority ("FSA"), HM Revenue & Customs ("HMRC") and the Serious Organised Crime Agency ("SOCA"), are concerned.
The FSA has consistently emphasised its view that anti-money laundering requirements are a key pillar of the UK regulatory regime, and that keeping up-to-date with those requirements should be a high priority for board-level executives as much as the compliance department in relevant firms.

The FSA’s director of financial crime and intelligence, Philip Robinson, in a speech to the FSA’s Annual Financial Crime Conference in 2008 commented that:

“Preventing financial sector firms from being used for a purpose connected with financial crime is one of our four statutory objectives. It is a responsibility that we are given by law. We will certainly reprioritise our efforts when a firm is in crisis, but we cannot and will not simply set this responsibility aside during periods of market turbulence. Nor do we think that we should try to do so.”

The FSA has had to reorganise itself, and to some extent reallocate its resources to address the challenges of the moment. The FSA doubtless recognises that in tighter economic conditions firms can find themselves in a similarly difficult position, so that management priorities may (and perhaps should) change, and resources may need to be reallocated. Indeed, that flexibility to deploy resources where they are most needed is intended to be one of the key benefits of the risk-based approach to compliance which the FSA has championed. Nevertheless, the FSA has sought to deliver a clear warning to the financial services sector that the detection and prevention of financial crime should remain a board-level issue even when the board has other pressing concerns to address.

Part 1 of this paper reviews the current statutory framework for anti-money laundering in the UK, focusing on the primary statutory offences relating to money laundering and terrorist financing but also considering the enforcement and asset tracing processes which are available to the UK’s investigatory and prosecuting authorities. However, readers should appreciate that the implementation of the Third Directive through the Money Laundering Regulations 2007, and the FSA’s Senior Management Arrangements, Systems and Controls Sourcebook, are also key constituents of the statutory framework in the UK.

Though the remainder of Part 1 focuses on the key statutory provisions contained in POCA and the Terrorism Act, references are made to those other sources of law, regulation and guidance which affect or contribute to the UK’s wider anti-money laundering framework. References to regulated sector firms are to those firms which carry on a business in the regulated sector, as set out in Schedule 9 of POCA, which is intended to correspond to those categories of firms which are subject to the 2007 Regulations¹. The role of the FSA in the UK money laundering regime is considered in more detail in Part 2 of this paper.

1.2 Statutory offences

POCA and the Terrorism Act set out a range of criminal offences the effect of which is to require businesses, in particular businesses in the regulated sector, to monitor for and to report potential money launderers and terrorist financing. These statutory measures also provide legal tools, including court-issued disclosure orders, for the investigating and prosecuting authorities to pursue and disrupt organised criminals and terrorist organisations.
The primary statutory offences relating to money laundering are contained in Part 7 of POCA and Sections 15 to 22 and 39 of the Terrorism Act. These offences replaced the predecessor money laundering offences under the Criminal Justice Act 1988, the Prevention of Terrorism (Temporary Powers) Act 1989, the Drug Trafficking Act 1994 and the equivalent statutes applicable in Scotland and Northern Ireland. In July 2005, a number of supplemental amendments were made to POCA by the Serious Organised Crime and Police Act 2005 (“SOCPA”) and, in 2007, POCA and the Terrorism Act were further amended by the Terrorism Act 2000 and the Proceeds of Crime Act 2002 (Amendment) Regulations 2007 (the “Terrorism Act and POCA Amendment Regulations”).

Under POCA and the Terrorism Act there are essentially three “principal” money laundering offences. A person (including a firm or an individual) commits a money laundering offence if he:

(a) conceals, disguises, converts or transfers the proceeds of criminal conduct or of terrorist property;

(b) becomes concerned in an arrangement to facilitate the acquisition, retention or control of, or to otherwise make available, the proceeds of criminal conduct or of terrorist property;

(c) acquires, possesses or uses property while knowing or suspecting it to be the proceeds of criminal conduct or of terrorist property;

and three “secondary” or third party offences:

(d) failure to disclose any of the above offences;

(e) tipping-off of persons engaged in money laundering or terrorist financing as to any investigation; and

(f) prejudicing an investigation in relation to money laundering or terrorist finance offences.

The provisions of POCA and the Terrorism Act apply to all legal persons, individual and corporate, so that fines can be imposed not only on corporate entities, but also on individual directors, managers and officers – who can also be imprisoned. The personal liability aspect of the statutory money laundering offences gives senior officers in regulated sector firms ample reason to be cautious in this area.

Apart from the personal liability for individuals working in the regulated financial services industry, and in particular senior management and compliance staff, the reputational damage which a conviction and fine is likely to cause at a corporate level must also be a serious concern for any regulated sector firm. The 2007 Regulations (and, when applicable to a regulated sector firm, the FSA’s Senior Management Arrangements, Systems and Controls Sourcebook) impose regulatory obligations on firms to train their staff in anti-money laundering procedures but, regulatory obligations aside, it is quite clearly both in the personal and corporate best interests of firms and their management to ensure that staff at all levels of the business are aware of their statutory obligations and liabilities and are adequately equipped to face them.
1.3 Proceeds of Crime Act

Part 7 of POCA, which contains the primary offences relating to money laundering, came into force on 24 February 2003. Transitional provisions apply so that the principal offences under Sections 327-29 and 333 of POCA can only be committed if the conduct constituting the offence was committed after 24 February 2003. Similarly, the Section 330 “failure to disclose” offence under POCA (see 1.3.2 below) may only be committed if the information which gives rise to the requisite knowledge, suspicion or reasonable grounds for knowledge or suspicion, came to a person after 24 February 2003.

1.3.1 The principal money laundering offences

Sections 327, 328 and 329 of POCA constitute the principal money laundering offences – concealment, acquisition and assisting the retention of the proceeds of crime, defined in POCA as "criminal property".

Criminal property means, for the purposes of these offences, property of all forms (including, of course, money) which constitutes or represents, in whole or in part, directly or indirectly, a person's benefit from criminal conduct. Criminal conduct is conduct which constitutes an offence in any part of the UK, or would do so if the conduct occurred in the UK.

If a person obtains what is referred to, rather arcaneously, as a “pecuniary advantage” as a result of or in connection with criminal conduct, he is treated as having obtained a benefit as a result of or in connection with that criminal conduct. In other words, it is not necessary for a person actively to receive “proceeds” from an offence in order for his assets to constitute or represent the benefit of criminal conduct. The savings that a person makes as a result of tax evasion are, therefore, treated as criminal property albeit perhaps without there being any specifically identifiable “proceeds” from that criminal conduct.

Significantly, an alleged offender must know or suspect that property constitutes or represents a benefit from criminal conduct, so property will not be treated as criminal property in determining whether an offence has been committed under Sections 327, 328 or 329 if the alleged offender is unaware that the property involved is the proceeds of criminal conduct.

Unless, therefore, a firm’s employees knowingly engage in business with a suspected money launderer or otherwise intentionally assist a money launderer, both the firm and the employees are unlikely to be at significant risk of committing these offences as principal offenders – all three offences require a degree of intent.

All firms should, however, be familiar with the nature and extent of these principal money laundering offences; a regulated sector firm must additionally ensure that its employees receive appropriate training in relation to money laundering, including as to the scope of these principal offences.

In particular, relevant employees of a regulated sector firm must be trained to identify potentially disclosable offences for the purposes of the failure to disclose offences under POCA: if employees...
in the regulated sector, and hence the firms which employ them, know or suspect or have reasonable grounds to know or suspect that a customer, counterparty or other person is engaged in money laundering activities (collectively herein “suspicious persons”) they may commit a criminal offence if they fail to disclose that information (see 1.3.2 below for a more detailed explanation of the failure to disclose offences).

If a regulated sector firm or any of its employees knows or suspects that a person is engaged in money laundering activities, but nevertheless enters into a particular course of conduct with that suspicious person, that firm and its employees may commit one of the principal money laundering offences under POCA unless they can make use of the limited defence of making an after-the-event disclosure of the course of conduct to SOCA, and have a “reasonable excuse” for not having made the disclosure before the event.

In general, firms should not engage in any activity with a suspicious person unless they have submitted a request for consent to SOCA and received confirmation that SOCA consents to the particular course of conduct (see 1.3.4 below on the “consent regime”).

The three principal money laundering offences set out in POCA are:

1.3.1.1 Concealing the proceeds of crime

Section 327 of POCA provides that:

“(1) A person commits an offence if he -

(a) conceals criminal property;

(b) disguises criminal property;

(c) converts criminal property;

(d) transfers criminal property;

(e) removes criminal property from England and Wales or from Scotland or from Northern Ireland.

…

(3) Concealing or disguising criminal property includes concealing or disguising its nature, source, location, disposition, movement or ownership or any rights with respect to it.”

This is the basic “money laundering” offence, criminalising conduct which enables criminals to conceal, disguise or move the proceeds of their crimes. The offence can be committed by the predicate offender, though it is presumably more likely to be used against a money laundering intermediary.
An offence under Section 327 is punishable by a fine and up to 14 years’ imprisonment.

1.3.1.2 Assisting money laundering

Section 328 of POCA provides that:

“(1) A person commits an offence if he enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.”

There is perhaps greater potential for a regulated sector firm to commit an assistance offence under Section 328 than the basic concealment or acquisition offences under Sections 327 and 329, but as previously mentioned, for the offence to be committed, any alleged offender under Section 328 must know or suspect that the relevant property is criminal property as well as knowing or suspecting that the arrangement into which he enters, or becomes concerned in, facilitates the retention or control of that criminal property.

In practice, therefore, the assistance offence cannot be committed without a degree of knowledge or suspicion on the part of the persons involved. The offence is, of course, a disclosable offence for the purposes of the Section 330 “failure to disclose” offence and as such it remains important for regulated sector firms and their employees to be aware of and understand the crime.

An offence under Section 328 is punishable by a fine and up to 14 years’ imprisonment.

1.3.1.3 Acquiring criminal property

Section 329 of POCA provides that:

“(1) A person commits an offence if he -

(a) acquires criminal property;

(b) uses criminal property;

(c) has possession of criminal property.”

In effect, this is a form of “handling stolen goods” offence in a money laundering context. A person may be convicted under Section 329 if it is established that he knew or suspected that property which he had acquired, used or taken possession of constituted or represented the benefit of criminal conduct. This crime is presumably intended to apply to persons who are not necessarily involved in the underlying criminal conduct or subsequent laundering activities, but nonetheless knowingly enjoy the benefits of criminal activity. Unknowing possession of the proceeds of criminal conduct, however, is not within the offence.
It is a defence for a person who acquires, uses or has possession of criminal property to show that he acquired, used or had possession for adequate consideration. Adequate is, perhaps unsurprisingly, not a defined term, but most probably should be interpreted in terms of “market-rate” consideration rather than “peppercorn” consideration, which in some other legal contexts may be construed as adequate.

An offence under Section 329 is punishable by a fine and up to 14 years’ imprisonment.

1.3.1.4 The scope of the primary offences

The nature of the underlying offences of which a person’s knowledge or suspicion can give rise to a primary offence (and consequently also the secondary offences discussed below) under POCA is widely drafted. Criminal property is defined in POCA as any property which constitutes or represents the benefit of criminal conduct. Criminal conduct is conduct which constitutes any offence in the UK or, subject to the limited territorial carve-out discussed below, would do so if it occurred in the UK. There is no time limit to the test, so the proceeds of criminal conduct which occurred prior to POCA coming into force are nevertheless criminal proceeds for the purposes of POCA even though, as noted above, conduct in relation to those proceeds can only constitute an offence under POCA if it occurred after POCA came into force.

Under the predecessor legislation, the money laundering offences were concerned only with the proceeds of serious crime, which in essence meant offences punishable in the Crown Court by at least one year of imprisonment. Indeed, the Second and Third EU Money Laundering Directives, which each sought to harmonise the approach to anti-money laundering law and regulation across the EU, required Member States to criminalise money laundering only to the extent that it relates to the proceeds of serious crimes. While the definition of “serious” differs between those directives, in both cases the fundamental point was that the crimes would be punishable by a maximum of at least one year in jail.

As noted above, however, under POCA the proceeds of any conduct which constitutes (or would constitute) a criminal offence in the UK can be the subject of laundering for the purposes of the statutory money laundering offences. In other words, the UK’s legislation is super-equivalent to that required by European law.

The wide scope of the definition of criminal conduct in POCA has, however, raised some difficult practical issues for firms, and particularly those in the regulated sector: will a firm risk committing a serious primary money laundering offence under POCA if it deals with another person when it knows or suspects that person has obtained a “pecuniary advantage” from criminal conduct even if the underlying “criminal conduct” concerned is merely a minor breach of health and safety or employment regulations?

The original letter of the law in POCA apparently required that a firm in that circumstance must seek the prior consent of SOCA (or its predecessor agencies) before becoming involved with a suspicious person; regulated sector firms might additionally be required to file a suspicious activity report (“SAR”). In practice, however, firms have found that seeking consent, and/or filing SARs, in
every such (comparatively) minor circumstance could cause quite serious disruption to business dealings and risk damaging business relationships.

It also became apparent that SOCA and other regulatory authorities were relatively uninterested in receiving frequent and voluminous disclosures relating to suspected minor offences, particularly if the suspected “criminal conduct” occurred somewhere other than the UK. The Government was, however, reluctant to cut back the scope of the POCA offences, and SOCA (and its predecessors) concluded, rightly, that they could not unilaterally determine that the strict requirements of law should be disregarded.

Under the original wording of POCA, conduct which constituted an offence in any part of the UK or would constitute an offence in any part of the UK if it occurred there was treated as giving rise to criminal property which could then be laundered for the purposes of POCA. This test is known as the single-criminality test because it characterises conduct occurring outside the UK as criminal conduct without taking into account whether the conduct is an offence in the jurisdiction in which it is carried on. The peculiar result of the single-criminality test as originally drafted was that it meant conduct which is entirely lawful in the country in which it actually occurs, but which would be criminal if carried on in the UK, may amount to criminal conduct for POCA purposes.

In recognition of the fact that this could cause a number of problems – the most widely quoted example was of the Spanish matador whose earnings were, under the single-criminality test, proceeds of criminal conduct in the UK – and following lobbying by, among others, financial institutions and their trade associations, the Government introduced under SOCPA two key amendments to POCA in relation to the primary money laundering offences which took effect in 2006.

The first set of amendments specifically addressed the single-criminality issue. Defences were introduced so that, subject to certain qualifications, a person charged with a primary money laundering offence who knows or believes on reasonable grounds that the relevant criminal conduct (in relation to which relevant knowledge or suspicion of money laundering has arisen) occurred outside the UK will not commit a primary money laundering offence in the UK if the relevant conduct was not at the time it occurred unlawful in the jurisdiction in which it occurred and was not otherwise conduct of a description prescribed for this purpose by the Government; a double-criminality override defence to the single-criminality test.

The Government then made an order, which came into force in May 2006, which prescribed for the purposes of the double-criminality override defence to the primary money laundering offences conduct which would be punishable in the UK by more than one year of imprisonment had the conduct occurred; but that order specifically excluded:

> conduct which would constitute an offence under certain gaming legislation; and

> conduct which would constitute an offence under Section 23 or 25 of the Financial Services and Markets Act 2000 (“FSMA”) (i.e. carrying on regulated activities by way of business without authorisation in breach of the general prohibition, or communicating an unlawful financial promotion).
The result is that a person will not now commit a primary money laundering offence if the criminal conduct potentially giving rise to such an offence is conduct which a person knows or believes on reasonable grounds occurred overseas and which, had it occurred in the UK, would be punishable by one year or less of imprisonment or would have constituted an offence under the relevant gaming legislation or Section 23 or 25 of FSMA.

An equivalent defence was introduced in relation to the secondary failure to disclose offence discussed in 1.3.2 below but the order described above does not apply to that defence; as a consequence, a person does not commit an offence under Section 330 if he fails to make a report in relation to conduct which he knows or believes on reasonable grounds to be money laundering occurring in a jurisdiction outside the UK in which that conduct is not unlawful, regardless of the fact that the money laundering offences in the UK are punishable by substantially more than one year of imprisonment.

The second set of amendments addressed limited categories of de minimis transaction which would otherwise have been caught by the primary offences. The Government introduced a de minimis carve out from the primary money laundering offences, available only to deposit taking institutions, with the effect that a money laundering offence will not be committed by those institutions if the acts which would have given rise to the offence occur in the course of operating a customer account, and the value of the funds concerned is less than £250 (or such higher limit as may from time to time be agreed by SOCA). This exclusion enables banks to permit de minimis standing orders and direct debits to continue to be drawn out of a bank account, e.g. utility and other lifestyle-essential payments, without specific consent from SOCA even after the bank has become suspicious of its customer and filed a SAR.

1.3.1.5 Prior consent of SOCA as a defence

If a regulated sector firm or any of its officers or employees knows or suspects that a suspicious person is engaged in money laundering activities and that a particular course of conduct with which they (or their firm) are asked to become involved would or could therefore involve the commission of an offence under Sections 327, 328 or 329 of POCA, that individual or firm may avail itself of a statutory defence by seeking the prior consent of SOCA in respect of the relevant proposed conduct. Unless there is a reasonable excuse for not doing so, to make use of this defence the request for consent must be submitted before the relevant conduct being undertaken by the firm.

It is worth differentiating at this stage between:

(a) a request for consent, known in POCA as an “authorised disclosure”, made by a regulated sector firm or any of its employees in order to trigger the defence to the offences set out in Sections 327, 328 and 329 of POCA; and

(b) a suspicious activity report or “SAR” which may be filed by a firm, or any of its employees, as required by Sections 330 or 331 of POCA.
Although the term SAR is commonly used interchangeably to refer to either case, strictly speaking a request for consent is made by or on behalf of a firm which is seeking consent from SOCA to enable it to carry out a proposed course of action without committing a primary money laundering offence. A regulated sector firm may in addition be required to submit a SAR to SOCA if the firm, including any of its officers and employees, has knowledge or a suspicion that another person is engaged in money laundering whether or not the firm has been asked to or intends to become involved in a transaction with that person. To avoid confusion, in this chapter we differentiate between the terms “authorised disclosure” and “SAR” in accordance with these interpretations.

An authorised disclosure should normally be made to SOCA by a firm’s Money Laundering Reporting Officer (“MLRO”). POCA stipulates that SOCA must respond to an authorised disclosure at the latest seven working days after the disclosure is made; the response will be to either grant or refuse consent for the firm to proceed any further with the proposed course of conduct. If a firm makes an authorised disclosure and does not receive a response from SOCA within that seven working day period, consent is deemed to have been given.

When SOCA receives an authorised disclosure it will either refer the case to another law enforcement agency for a decision to be made, or make a decision itself, as to whether the proposed conduct or the suspicious person involved should be investigated further and will grant or refuse consent accordingly.

If SOCA refuses consent to proceed with a particular course of conduct, the authorities have 31 days (calendar rather than working days) from the date of the refusal to investigate the proposed conduct or the suspicious person and, if appropriate, take action against the suspicious person. Upon the expiry of that 31-day period, and in the absence of an interim restraining action, the firm which made the authorised disclosure is deemed to have received consent to proceed with the particular course of action.

By way of a practical example, if an MLRO reports a suspicion of money laundering to SOCA on Tuesday 1 March, SOCA has seven working days from Wednesday 2 March to respond. If, therefore, the firm has not received a response by the end of the following Friday 10 March, consent to proceed with a particular transaction is deemed to have been given. If consent is refused by SOCA on Thursday 3 March, for instance, law enforcement authorities have 31 calendar days from and including 3 March (that is, until 2 April) in which to investigate the proposed conduct and the suspicious person.

SOCA’s “Suspicious Activity Reports Regime, Annual Report 2008” shows that in the year to end-September 2008, on average 37% of all authorised disclosures (both those dealt with only by SOCA and those referred to another law enforcement agency) were responded to either on the day of receipt or on the following day (day 0 or day 1). Over half of the authorised disclosures (58%) were responded to on days 0, 1 or 2 and 100% of the authorised disclosures were responded to within the 7-day period. SOCA have indicated that factors such as the complexity of the case, the need to clarify information with the reporter, and the likelihood of it, or another agency, refusing consent, all contribute to the time taken to respond to a authorised disclosure.
If an MLRO makes an authorised disclosure to SOCA as a result of having received an internal disclosure from another employee, but gives consent for the activity to proceed before receiving formal consent from SOCA, the MLRO may be guilty of a criminal offence under Section 336 of POCA and be liable to a fine and up to five years’ imprisonment. An employee who innocently carries out the (prohibited) course of conduct having relied on that MLRO’s consent, however, will maintain a defence by virtue of having made an internal disclosure to the MLRO (presumably provided that he does not have knowledge of the MLRO’s offence).

1.3.2 The failure to disclose offences

Section 330 of POCA provides that:

“(1) A person commits an offence if each of the following three conditions is satisfied.

(2) The first condition is that he -

   (a) knows or suspects, or

   (b) has reasonable grounds for knowing or suspecting,

   that another person is engaged in money laundering.

(3) The second condition is that the information or other matter -

   (a) on which his knowledge or suspicion is based, or

   (b) which gives reasonable grounds for such knowledge or suspicion,

   came to him in the course of a business in the regulated sector.

(3A) The third condition is -

   (a) that he can identify the other person mentioned in subsection (2) or the whereabouts of any of the laundered property,

   (b) that he believes, or it is reasonable to expect him to believe, that the information or other matter mentioned in subsection (3) will or may assist in identifying that other person or the whereabouts of any of the laundered property, or

(4) The fourth condition is that he does not make the required disclosure to -

   (a) a nominated officer, or

   (b) a person authorised for the purposes of this Part by the Director General of SOCA\textsuperscript{a}.”
Money laundering means, for these purposes, the offences under Sections 327, 328 or 329 of POCA. The “laundered property” is the property forming the subject matter of the money laundering known, suspected, or in respect of which there are reasonable grounds for knowing or suspecting that another person has engaged. Practitioners will be aware that the obligation to file SARs with SOCA to avoid committing an offence applies not only in relation to knowledge or suspicions concerning a regulated sector firm’s own customers, but any person with whom it has dealings in the course of its business in the regulated sector (e.g. including counterparties to transactions, lenders, agents, advisers to those parties and prospective customers).

The failure to disclose offence is something which the financial services industry in the UK became accustomed to dealing with over a period of many years in relation to terrorist financing and drug trafficking-related offences. One of the key features of the Section 330 failure to disclose offence, however, is that it applies not only in relation to dealings with the proceeds of serious offences, but to dealings with the proceeds of all crimes. The formal reporting obligation is, therefore, rather broader than the predecessor regimes.

The other key feature of the failure to disclose offence under POCA is that it utilises an objective test and thereby effectively criminalises negligence in the regulated sector.

If an individual employed in the regulated sector fails to detect or suspect that a suspicious person is engaged in money laundering activities, but a court determines that objectively, in the given circumstances, he should have done so, that individual (and consequently the firm) may be guilty of a criminal offence punishable by a fine and up to five years’ imprisonment. The fact that the individual was genuinely not suspicious will not be a defence if a court determines, with the benefit of hindsight, that there were circumstances which should have led him, or the firm, to be suspicious.

By virtue of Section 340(11)(d), money laundering includes, for these purposes, not only conduct which constitutes a primary money laundering offence in the UK, but also conduct which would constitute such an offence if done in the UK.

As noted above, a double-criminality override defence was introduced in relation to the failure to disclose offence in May 2006 in the following terms:

“(7A) Nor does a person commit an offence under this section if -

(a) he knows, or believes on reasonable grounds, that the money laundering is occurring in a particular country or territory outside the United Kingdom, and

(b) the money laundering -

(i) is not unlawful under the criminal law applying in that country or territory, and

(ii) is not of a description prescribed in an order made by the Secretary of State.”
The Government has not yet prescribed any description of money laundering for the purposes of Section 330(7A)(b)(ii). Consequently, a person will not commit a Section 330 offence if he fails to disclose money laundering which he knows or believes on reasonable grounds to be occurring in a jurisdiction outside the UK in which that activity is not unlawful, regardless of the fact that the money laundering offences in the UK are serious offences carrying substantial penalties.

1.3.2.1 Required disclosures for employees in the regulated sector

Individuals working for regulated sector firms can discharge their disclosure obligations and thereby avoid committing an offence under Section 330 by making a “required disclosure”. The required disclosure will most often be an internal report to the firm’s MLRO in accordance with that firm’s established reporting procedures rather than a direct report (a SAR) to SOCA.

If an individual working in the regulated sector does not make a required disclosure concerning a suspicious transaction or other activity and a court determines that the individual concerned knew or suspected, or had reasonable grounds for knowing or suspecting, that the transaction or other activity involved money laundering, only two general defences are available:

(a) the individual has a “reasonable excuse” for not making a required disclosure – the legal meaning of reasonable excuse is not clear and has not yet been tested in the courts; the prudent view must be that the term will be construed narrowly and should not be relied upon in practice, except in very special circumstances, to determine whether a disclosure should be made; or

(b) the individual has not been provided with suitable training by his employer and did not have actual knowledge or suspicion of money laundering. (Under the 2007 Regulations, employers are required to provide their employees with adequate training on how to identify potential money laundering and on their legal duties and liabilities under, inter alia, POCA).

The latter defence emphasises the obligation for senior management under the 2007 Regulations to ensure that staff are properly trained.

If an individual is thought to have committed a Section 330 offence but can successfully demonstrate that the firm had failed to provide adequate training, the inevitable conclusion to be drawn is that senior management, either individually or collectively, are responsible for that regulatory failure (although not necessarily for the commission of a primary statutory offence). Under the 2007 Regulations, any director or other senior officer who has contributed to the firm’s failure to comply with training requirements may be liable to prosecution and, on conviction, to up to two years’ imprisonment.

Lawyers and certain other “relevant professional advisers” are not required to make a disclosure to SOCA if the information or other matter on which their knowledge or suspicion of money laundering was based, or which gave reasonable grounds for knowledge or suspicion, came to them in privileged circumstances. Originally, this defence was available only to lawyers, but
following representations made to the Treasury by the accountants (through the Institute of Chartered Accountants in England and Wales ("ICAEW") and other professional bodies, the defence was extended to accountants, auditors and tax advisers who are members of certain professional bodies.

1.3.2.2 The MLRO offence

In addition to the general failure to disclose offence under Section 330, if an employee makes an internal report in accordance with that firm's reporting procedures, the firm's MLRO may commit a separate failure to disclose offence if he then fails to deliver a SAR to SOCA.

Section 331 provides that:

“(1) A person nominated to receive disclosures under Section 330 commits an offence if the conditions in subsections (2) to (4) are satisfied.

(2) The first condition is that he -

(a) knows or suspects, or

(b) has reasonable grounds for knowing or suspecting,

that another person is engaged in money laundering.

(3) The second condition is that the information or other matter -

(a) on which his knowledge or suspicion is based, or

(b) which gives reasonable grounds for such knowledge or suspicion,

came to him in consequence of a disclosure made under Section 330.

(3A) The third condition is -

(a) that he knows the identity of the other person mentioned in subsection (2), or the whereabouts of any of the laundered property, in consequence of a disclosure made under Section 330,

(b) that that other person, or the whereabouts of any laundered property, can be identified from the information or other matter mentioned in subsection (3), or

(c) that he believes, or it is reasonable to expect him to believe, that the information or other matter will or may assist in identifying that other person or the whereabouts of the laundered property.
(4) The fourth condition is that he does not make the required disclosure to a person authorised for the purposes of this Part by the Director General of SOCA as soon as is practicable after the information or other matter mentioned in subsection (3) comes to him.”

If an employee makes a required disclosure report to the MLRO in accordance with the firm's reporting procedures and the MLRO then fails to disclose that information to SOCA after having determined (or negligently failed to determine) that it was a justified report, he may commit an offence unless he had a "reasonable excuse".

The MLRO failure to disclose offence is punishable by a fine and up to five years’ imprisonment.

1.3.2.3 Limited value SARs

In July 2005 the Government amended Section 330 with the specific aim of "easing the money laundering reporting requirements on the regulated sector”22.

The introduction of subsection 330(3A) has narrowed the scope of the failure to disclose offence by requiring a person working in the regulated sector to make a required disclosure or file a SAR with SOCA only if either the identity of the person committing the money laundering, or the whereabouts of the laundered property, can be identified, or it is reasonable to believe that the information which the person possesses would enable such matters to be established.

The practical effect of this amendment should be that if a person working in the regulated sector becomes aware that another person has committed an offence but is not in a position either to identify the offender or to know where the proceeds of the criminal conduct could be found, it may not be necessary to make a required disclosure or file a SAR.

A similar qualification applies in relation to the MLRO failure to disclosure offence under Section 331.

This qualification should be particularly relevant if the underlying offence is a remote or anonymous offence, such as credit card fraud, where the financial institutions involved in detecting the offence have a limited (if any) ability to interact with or identify the offender.

The amendment provided some relief for firms which might otherwise have needed to file “limited intelligence value” SARs with SOCA, but it is critical to note that the (objective) second limb to subsection 3A somewhat diluted the effect of the new subsection. The possibility that a court could determine after the fact that a subjective assessment of the relevance of particular information was wrong means that individual employees may not wish to make (and perhaps should not be encouraged to make) an assessment of whether a required disclosure is in fact required; it is probably best reserved for the MLRO to make that assessment in light of any other information of which the firm is aware which might have a bearing on a decision to file a SAR.

It is one thing for an MLRO to conclude that, on the basis of all of the information available to the MLRO (and therefore the firm), it is not reasonable to believe that information will or may
assist in identifying a person or laundered property; there would be a risk to the firm involved, however, if the internal reporting policy permitted individual employees to make that assessment. Firms may not therefore wish to emphasise this element of the offence in the context of internal training sessions and reporting procedures.

Ultimately the consequences of being second-guessed by an investigatory authority or a court in relation to the relative value of the information possessed by a firm may outweigh the relatively minor administrative inconvenience for an MLRO in filing a SAR.

SOCA continues to provide the means for regulated sector firms to submit SARs in circumstances where the information concerned is of limited value. In the notes to accompany its “limited intelligence value” reporting form, SOCA acknowledges “that the reporting requirements under Part 7 POCA sometimes result in reports being required in circumstances where there is likely to be limited intelligence value to law enforcement, although wider analysis of such reports may provide useful data”23.

The notes give examples of the circumstances in which SOCA considers that a limited intelligence value report may be appropriate including cases where the conduct has occurred overseas, was not unlawful in the jurisdiction in which it occurred, and did not relate to “serious” crime such as terrorism, drug offences or sex offences; cases where the underlying criminal conduct is the consequence of minor irregularity not involving dishonesty; cases where another regulatory or investigatory authority is already aware of the underlying conduct; and cases involving strict liability offences under VAT legislation or breaches of an administrative nature in areas such as employment and software licensing. SOCA also has in place arrangements to enable major retail business, including the banks, to make bulk reports of low value intelligence, e.g. in relation to credit card frauds where the alleged offender and the proceeds of the fraud cannot be traced.

The combination of the Government’s attempt to ease the reporting burden on firms by amending the offences under POCA and SOCA’s practical approach to the reporting requirement means that regulated sector firms are now better able to meet the requirements imposed upon them by Section 330.

1.3.2.4 Relevance of guidance

Subsection 330(8) of POCA provides that:

“(8) In deciding whether a person committed [a failure to disclose offence] the court must consider whether he followed any relevant guidance which was at the time concerned -

(a) issued by a supervisory authority or any other appropriate body,

(b) approved by the Treasury, and

(c) published in a manner it approved as appropriate in its opinion to bring the guidance to the attention of persons likely to be affected by it.”
The effect of this provision is that certain pieces of industry guidance may be given statutory recognition by the Treasury so that firms which are subject to the UK anti-money laundering regime, and regulated sector firms in particular, are provided a degree of comfort that compliance with widely recognised industry standards should, in general, be viewed positively by the courts (and consequently also by relevant supervisory authorities). Subsection 330(8) does not, however, go as far as to establish a safe harbour for firms complying with approved guidance.

The Guidance Notes for the Financial Sector (the “Guidance Notes”) produced by the Joint Money Laundering Steering Group (“JMLSG”) were for a number of years the only set of guidance which had been approved by the Treasury for these purposes. However, in July 2008 it was announced that the Treasury had approved for these purposes HMRC’s guidance for those firms which are subject to its supervision under the 2007 Regulations, such as trust and company service providers (including non-executive directors) and money service businesses24, as indeed may other industry bodies in due course. Guidance contained in the FSA’s Senior Management Arrangements, Systems and Controls Sourcebook which applies to FSA-authorised firms (addressed in more detail in Part 2) does not constitute relevant guidance for the purpose of Section 330(8), although it is, of course, relevant to those authorised firms in a more general sense.

The Guidance Notes underwent a wholesale revision during 2006 and 2007, and an entirely new set of notes was then published in November 2007. This new set of notes received approval by the Treasury with effect from 15 December 2007 to coincide with the coming into force of the 2007 Regulations on that date.

The Guidance Notes probably have greater relevance in the context of compliance with the 2007 Regulations (which deal more with procedural anti-money laundering requirements) than with POCA; they contain a great deal of helpful information, both generic and sectoral-specific, in relation to the customer identification and verification processes requirement by the 2007 Regulations.

Nevertheless, the Guidance Notes also set out practical tips for firms on the circumstances in which transactions may (or ought to) attract suspicion for the purposes of POCA, to assist regulated sector firms in particular in their assessment of the more onerous objective test for the Section 330 offence. The Guidance Notes continue to be updated to reflect amendments to POCA and developments more generally in the approach to anti-money laundering at both a national and international level.

Whilst the Guidance Notes have no legal force per se evidentially they have become important as a result of Section 330(8) POCA and equivalent provisions in the Terrorism Act and the 2007 Regulations25. Regulated sector firms should therefore be aware of the best practice standards which are set out in the Guidance Notes and, where appropriate, use them as a benchmark against which to measure the firm’s compliance.

If a firm finds itself in the position of having failed to detect or disclose potential money laundering activities it will doubtless find itself in a more comfortable position if it can
demonstrate that it has in place systems and controls to detect and prevent money laundering which meet or exceed the standards suggested by the Guidance Notes, notwithstanding that potential money laundering may nevertheless have passed undetected or undisclosed.

1.3.3 The tipping-off offences

The tipping-off offences in POCA were substantially revised in December 2007 (along with certain aspects of the Terrorism Act which are addressed in the following sections) to give effect to certain of the requirements of the Third Directive.26 The former tipping-off offence under Section 333 of POCA, which applied to all persons, has been repealed and in its place a new offence under Section 333A now applies only to the regulated sector.

Section 333A provides that:

“(1) A person commits an offence if -

(a) the person discloses any matter within subsection (2),

(b) the disclosure is likely to prejudice any investigation that might be conducted following the disclosure referred to in that subsection, and

(c) the information on which the disclosure is based came to the person in the course of a business in the regulated sector.

(2) The matters are that the person or another person has made a disclosure under this Part -

(a) to a constable,

(b) to an officer of Revenue and Customs,

(c) to a nominated officer,

(d) to a member of staff of the Serious Organised Crime Agency authorised for the purposes of this Part by the Director General of that Agency,

of information that came to that person in the course of a business in the regulated sector.

(3) A person commits an offence if -

(a) the person discloses that an investigation into allegations that an offence has been committed is being contemplated or is being carried out,

(b) the disclosure is likely to prejudice that investigation, and
(c) the information on which the disclosure is based came to the person in the course of a business in the regulated sector."

Each of the two offences described above carry a penalty of a fine and up to two years of imprisonment\(^27\) (reduced from five years for the predecessor offence under Section 333 of POCA).

Effectively, therefore, POCA contains two separate tipping-off offences for persons carrying on business in the regulated sector: tipping-off in relation to reports of suspicion, and prejudicing an investigation. The first offence involves disclosing that a report has been made either internally (to an MLRO) or externally to SOCA or another relevant authority. The second offence involves disclosing that an investigation is being contemplated or is being carried out.

While there may be some scope for overlap between these two offences, there are also some significant differences between them and, accordingly, it is necessary for all those working in the regulated sector to be aware of the conditions precedent to each. The first offence requires that an internal report of suspicion to an MLRO, or an external SAR or request for consent has been filed; the second offence requires that an investigation into an alleged money laundering offence under POCA is being carried out or is contemplated (note that the investigation must relate to an offence under POCA and not to the underlying criminal conduct, although in practice it may not be easy to make a clear distinction).

In either case, however, an offence will only be committed if the disclosure of information by the firm or individual in the regulated sector is likely to prejudice any investigation which may ensue, is being contemplated, or is being carried out.

In circumstances where an individual employed by a regulated sector firm has suspicions about a particular person or activity, it can be difficult to determine how best to deal with that suspicion in practice. To avoid committing a criminal offence under Section 330, the individual must make an internal report to his firm’s MLRO. The MLRO must then determine whether a SAR needs to be filed with SOCA or, if the firm is asked to engage in activities which would involve it dealing with the suspicious person, whether an authorised disclosure needs to be submitted to SOCA and consent obtained before proceeding.

If the MLRO seeks a consent from SOCA, the firm and individuals involved may commit an offence under any of Sections 327, 328 or 329 of POCA if the firm engages in any further activity with the suspicious person. At the same time, however, the firm will be concerned to ensure that a tipping-off offence is not committed by either expressly or impliedly confirming to the customer that the firm cannot proceed with a requested transaction, or must wait before engaging in certain activities, because a request for consent has been submitted.

Failing to follow a customer’s instructions in relation to a transaction while a report is processed may alert that customer to the fact that the firm has become suspicious of the customer’s activities; could the fact that the customer could draw his own conclusion that the firm had submitted an authorised disclosure and was waiting for consent to proceed as a result of the firm refusing to complete a requested transaction (or seeking to delay completion without giving the
customer a clear explanation) amount to tipping-off? This seems unlikely; the offence requires that a person discloses relevant information, indicating that an active disclosure is contemplated.

In any event subsections 333D(3) and (4) go further by confirming that a person will not commit an offence under Section 333A if he did not know or suspect that the disclosure would be likely to prejudice an investigation. In other words it is not sufficient that a firm or individual simply disclosed relevant information to another person; a prosecuting authority would need also to demonstrate that the firm or individual knew or suspected that making that disclosure would be likely to prejudice any subsequent (or ongoing) investigation. The offence seemingly therefore requires the person or firm concerned to know or suspect that there is an investigation, or the possibility of an investigation, and to have an intention to prejudice, or at least a reckless disregard whether prejudice would follow.

In the absence of evidence that a firm or individual officer or employee sought tacitly to confirm the understanding of a suspicious person that a relevant disclosure had been made, or an investigation commenced, it seems unlikely that either offence would be committed if there is no active communication of those matters. Perhaps more importantly, however, unless it can be shown that the firm or individual knew or suspected that the disclosure would be likely to prejudice an investigation, the offence should not arise. Section 333A does not therefore prohibit any communication between a firm and its customer once an authorised disclosure has been submitted to SOCA. When considered in this light, the tipping-off offences are, perhaps, not quite as substantial a bear-trap as some firms have in the past feared.

It is possible, though, that more difficult situations may arise from time to time and so one must continue to tread carefully. If a firm of auditors forms a suspicion in the course of an audit that its client may have been involved in money laundering, that firm may be required to cease acting for its client and to provide a full and clear explanation to its client; auditors are required to explain their reasons if they cease to act for a client[28]. Would any such explanation amount to tipping-off? It seems at least possible that it could.

It is likely that in some situations refraining from dealing with a suspicious person will prompt questions which could put the firm at risk of being forced into making a statement of some nature, thereby risking an active tipping-off “disclosure”; this will be more likely if the suspicious person concerned is a customer or client of the firm. Banks in particular have found it difficult to reconcile the tensions inherent in POCA between the failure to disclose offence and the tipping-off offences.

SOCA has been sympathetic. While it is not in a position to provide binding guidance on the matter, SOCA has encouraged firms to raise any tipping-off concerns when submitting an authorised disclosure so that it can provide practical guidance wherever possible. The courts have also been required to consider the difficulties faced by firms in the regulated sector in this context and have sought to provide some comfort (in relation to which see the following section).

In practice, it seems unlikely that a prosecuting authority would pursue a firm for tipping-off if it had complied in all respects with its disclosure obligations under POCA, had taken no active steps
to tip off the suspicious person in question and had followed any instructions from SOCA after making its disclosure.

The regulations which implemented the changes to the tipping-off offences under POCA also introduced limited safe-harbours from the offence in the form of "permitted disclosures", the scope of which is set out in Sections 333B to 333E. The new permitted disclosures regime carves out from the Section 333A offence, *inter alia*, the following disclosures:

> a disclosure of relevant information between employees or offices within the same undertaking;

> a disclosure by a credit or financial institution to another credit or financial institution in the same consolidated group which is subject to the Third Directive or equivalent requirements;

> a disclosure between two credit institutions, between two financial institutions, between two professional legal advisers or between two firms of accountants of relevant information relating to a client or former client of both firms, a transaction involving both firms or the provision of a service by both firms, in each case to prevent a money laundering offence being committed under POCA and provided that the recipient of the disclosure is subject to the Third Directive or equivalent requirements and that both firms are subject to the Data Protection Act or equivalent duties of professional confidentiality and protection of personal data; and

> a disclosure of relevant information by a professional legal adviser or other professional adviser (including accountants) to a client to dissuade the client from engaging in conduct which would amount to an offence.

In addition to the tipping-off offences for the regulated sector, a general offence of prejudicing an investigation remains relevant for non-regulated sector firms. Section 342 provides that:

“(1) This section applies if a person knows or suspects that an appropriate officer or (in Scotland) a proper person is acting (or proposing to act) in connection with a confiscation investigation, a civil recovery investigation, a detained cash investigation or a money laundering investigation which is being or is about to be conducted.

(2) The person commits an offence if -

(a) he makes a disclosure which is likely to prejudice the investigation,

(b) he falsifies, conceals, destroys or otherwise disposes of, or causes or permits the falsification, concealment, destruction or disposal of, documents which are relevant to the investigation.”

The Section 342 offence may only be committed by non-regulated sector firms, and applies in slightly narrower, although nevertheless egregious, circumstances than the Section 333A offences.
(namely making a disclosure which prejudices an investigation which is known or suspected to be underway or about to be commenced, or falsifying or destroying documents which are relevant to an investigation), but remains a serious money laundering offence punishable by a fine and up to five years’ imprisonment.

Subsection 342(3)(a) provides that a person does not commit the offence if he does not know or suspect that a relevant disclosure is likely to prejudice an investigation. The Section 342 offence therefore again requires an intention to prejudice, or at least reckless disregard as to whether prejudice will follow from a relevant disclosure.

1.3.4 Practical issues associated with the consent regime

As previously discussed, where a regulated sector firm or any of its employees knows or suspects that a suspicious person is engaged in money laundering activities and that a particular course of conduct with which they are asked to become involved would or could involve the commission of an offence under any of Sections 327, 328 or 329 of POCA, that firm should make an authorised disclosure to SOCA to avoid committing that offence.

The firm is then required to allow up to seven working days for SOCA to respond to the request for consent, refusing consent or declaring that a 31-day moratorium period (during which the firm may not engage in any activity with the suspicious person) has commenced. This process, known as the consent regime, has come under wide scrutiny since POCA was enacted due to the difficulties that it causes for firms, particularly in relation to the tipping-off offences.

The key issue that has been raised by firms in respect of the consent regime is the difficulty in suspending all activity in relation to a particular customer for the period between the making of an authorised disclosure and the time at which consent to proceed is granted by SOCA. During such periods of suspension it is not uncommon for the firm to have to deal with difficult questions about why a transaction has not proceeded in accordance with instructions; in some cases customers of firms which have sought consent and in effect frozen customer accounts in the meantime have begun legal proceedings to force the firm to process the transactions.

In these circumstances, firms find themselves in a difficult position. Explaining to a customer that a transaction cannot be processed due to the firm’s suspicion of money laundering and consequent disclosure to SOCA could in some circumstances amount to a “tipping-off” offence (if the firm considers that any subsequent investigation is likely to be prejudiced as a result). On the other hand, offering no explanation why a transaction or payment instruction is being delayed could damage relationships and reputations and, potentially, give rise to contractual or tortious liabilities for the firm.

1.3.4.1 Judicial guidance

The courts have been asked to consider such circumstances and, accordingly, we now have some useful judicial commentary on the appropriate way to address that particular difficulty.
In Squirrell Ltd v. National Westminster Bank plc the customer, Squirrell, had brought legal proceedings against NatWest to force it to process a transaction. NatWest, suspecting that monies received by Squirrell could be criminal property, had made an authorised disclosure in respect of the customer and had therefore concluded that it was unable to process the transaction. NatWest had blocked Squirrell’s account without providing an explanation to Squirrell. Squirrell made an application to the court requesting that its account be unblocked and for the bank to give reasons why it had been blocked.

The High Court dismissed Squirrell’s application on the grounds that the test under POCA required NatWest to cease processing transactions and make a disclosure as soon as it had a suspicion of money laundering. There did not need to be any actual evidence of money laundering for that suspicion to arise. Accordingly, the course of action taken by NatWest was “unimpeachable” as it had done what was required of it by legislation.

The court had sympathy for customers in Squirrell’s position in respect of whom no evidence of criminal conduct had been provided, whose business had possibly suffered serious detriment as a result of the account having been frozen, but who could not expect to receive damages from the bank or the authorities. Despite its sympathy, however, on the basis that Parliament had clearly laid out in POCA the mechanism to deal with the issue of consent, the court held that it was powerless to intervene for Squirrell.

The Squirrell case also highlighted the importance of liaising at an early stage with SOCA. Once the application to the court had been made by Squirrell, NatWest found itself in the difficult position of not being able to offer a defence to the court for fear of committing the offence of tipping-off. This dilemma was resolved by the intervention of HM Customs and Excise (now part of HMRC) which enabled the court to be informed of the reasons for NatWest’s refusal to operate Squirrell’s account.

Similar circumstances were then considered by the Court of Appeal in K Ltd v. National Westminster Bank plc. In this case the customer, K, wished to process two large business transactions through its account with NatWest and a director of K gave pre-warning of these transactions to the account manager at NatWest. At the time of the second transaction, however, NatWest suspected that the monies could amount to criminal proceeds and, accordingly, refused to process the transaction and filed a SAR in relation to K. NatWest then wrote to K informing it that it could not process the transaction, but without offering any reason.

K made an application to the court for a mandatory injunction to force NatWest to comply with its instructions. At first instance K’s application was rejected and K appealed to the Court of Appeal arguing, inter alia, that by refusing to process its instructions, NatWest was in breach of its mandate and, accordingly, that the judge should have restrained the bank from continuing to act in breach of contract.

The Court of Appeal agreed with the decision in Squirrell that Parliament had struck a “precise and workable balance of conflicting interests” in POCA by considering that a limited amount of interference is to be tolerated in preference to allowing money laundering to be carried on in
commercial community. The court ruled that NatWest had followed the correct procedure laid out in POCA by refusing to carry out the transaction and that as the bank held a suspicion it was prohibited as a matter of criminal law from carrying out the customer’s mandate. Accordingly, the mandate with K had been temporarily suspended until the illegality was removed and so NatWest could not be held by the court to be in breach of contract.

Clearly the courts recognise that a firm will commit a criminal offence if, having identified a suspicion of money laundering, it does not freeze relevant accounts or transactions and file a SAR. The practical consequence is that any adversely affected person may then apply to court for assistance, or to enforce contractual rights, but the court seems to be indicating that it will not assist or otherwise require the firm concerned to perform specific actions if to do so would be to require the firm to commit the criminal offence which it seeks to avoid. The practical conclusion must be, therefore, that firms should prioritise their obligations under POCA (and the Terrorism Act) over contractual obligations and other duties owed to customers and counterparties.

1.3.4.2 Reform of the consent regime

Following a review of SARs processes published in March 2006 by Sir Stephen Lander, the non-executive Chairman of SOCA, which included some wider consideration of the consent regime, the Home Office consulted in December 2007 on the possibility of making certain changes to improve the way in which the consent regime operates, including changes which might help to address the tension for firms operating in the regulated sector between the statutory reporting obligations and the tipping-off offences.

The Home Office consultation also sought to address other practical difficulties with the consent regime which had been brought to their attention. For example, some members of the regulated sector had notified the Home Office of their concern about the risk of conflict between their duty of notification under POCA and their contractual duties to their clients. It was argued that by seeking consent under POCA, they opened themselves up to legal action for breach of contract. As noted in the Home Office consultation, this issue had been addressed by the court in the Squirrell and K Ltd cases (see 1.3.4.1 above).

More significantly, however, was a concern about the interaction between the requirements of the consent regime and the principle of “fungibility”. Consent requests are necessarily before-the-act notifications – an institution suspecting that a proposed transaction is a prohibited act under POCA will request consent from SOCA before carrying out the transaction. The transaction can then only be carried out if consent is granted, or the moratorium period has expired. The banking sector have argued that this can cause difficulties as banks may be unable to stop, or obtain consent for, all individual transactions carried out for a customer after the moment at which knowledge or suspicion of money laundering has arisen, as many are automated. This raises difficult questions of interpretation as to whether all payments out of an account into which a single suspicious payment has been made are themselves then suspicious payments in relation to which a notification and request for consent is required.

The British Bankers’ Association Money Laundering Advisory Panel (the “BBA Panel”) raised with the Home Office their view that the requirements of the consent regime in this context
cannot easily be reconciled with POCA’s wide definition of criminal property and the principle of fungibility. The BBA Panel explained their view that money in a bank account is fungible and that as a matter of property law a bank account is a single “indistinguishable mixed fund”. Consequently, once a payment has been made into a mixed bank account, that payment cannot be distinguished from the other funds in the account and, accordingly, if the payment was a suspicious transaction the payment funds could have effectively tainted the rest of the account and, possibly, any other account held by the same individual. This would result in all subsequent transactions on the suspect accounts becoming acts of money laundering under POCA.

The Home Office indicated that it had not intended for POCA to have this unintended effect, but acknowledges the difficulties which arise out of the legal fungibility of funds held in a bank account. An alternative analysis is set out by the Home Office, namely that a single suspicious payment into a bank account is converted into a chose in action for the depositor concerned (i.e. relying on the “valuable consideration” defence in Section 329), so that the chose in action then represents the criminal property rather than the payment tainting all of the funds in the account. If this analysis were correct, the Home Office considers that the bank concerned would then only commit an offence if it knew or suspected the criminal origin of the funds and failed to file a SAR. There remains considerable doubt, however, as to the effect of fungibility on funds held in a bank account which the Home Office consultation appears to have been unable to resolve.

The consultation proposed three options for developing the POCA consent regime, namely:

> **Build on the current regime** – i.e. keeping the regime much as it currently stands, but looking to SOCA and the courts to provide more guidance on acceptable behaviour in relation to the tipping-off risk, fungibility etc;

> **Twin track approach** – this would give firms the option of either freezing a transaction and asking for consent as in the current regime or, alternatively, avoiding liability by making a pre-event notification to SOCA of their suspicion that an offence may be committed in the future (e.g. where a transaction is contemplated but not yet completed) and then proceeding with the transaction unless restrained; and

> **Addressing the fungibility issue through specific statutory amendments** – this option was intended as a supplement to either of the first two options; it would have been a means of addressing the issue highlighted by the BBA Panel which would clarify that obtaining consent in relation to an initial suspicious transaction would cover any subsequent so-called “technical” offences (i.e. those involving funds thought to have been tainted by the original suspicious transaction) so that there would be no need to separately report each such suspicion.

The consultation closed in March 2008. The SOCA Suspicious Activity Reports Regime Annual Report 2008, published on 20 November 2008, subsequently confirmed that following a consideration of responses to the consultation the Home Office and SOCA had reached the conclusion that the responses demonstrated that there was “no clear way forward on this issue as regards to further amendments to the current legislation”. Despite this fairly inconclusive
close to the consultation, SOCA reported that over recent years a valuable pragmatic approach
to the regime’s operation had developed and that work is taking place to build on this pragmatic
approach.

It therefore appears that the current consent regime will not be substantially revisited in the short
term, but SOCA will instead simply continue to do what it can (with the assistance of the courts
where necessary) to operate the regime in a way which better enables firms in the regulated
sector to manage their legal risks under POCA with wider legal, reputational and relationship risks.
Overall, this is far from satisfactory for those firms which on a daily basis are required to manage
money laundering risks against contractual, reputational and relationship risks.

1.4 The Terrorism Act 2000

With effect from 19 February 2001, the majority of the UK’s anti-terrorism legislation was
repealed and replaced by the Terrorism Act. The Terrorism Act, among other things, criminalises
the financing and supporting of terrorists and terrorism through a number of offences, which for
convenience are collectively described here as the terrorist finance offences. The offences under
the Terrorism Act mirror to a large extent the money laundering offences under POCA.

The terrorist finance offences, each punishable by a maximum of 14 years’ imprisonment and/or a
fine, are:

(a) fund-raising, receiving or providing money or other property knowing or having reasonable
cause to suspect that it will or may be used for the purposes of terrorism;

(b) using or possessing money or other property knowing or having reasonable cause to suspect
that it will or may be used for the purposes of terrorism;

(c) entering into or becoming concerned in an arrangement as a result of which money or other
property is made available to another while having reasonable cause to suspect that it will
or may be used for the purposes of terrorism.

A separate terrorist money laundering offence is committed by a person who enters into or
becomes concerned in an arrangement which facilitates the retention or control of terrorist
property by concealment, removal from the jurisdiction, transfer to nominees or in any other way.

In addition to these offences, the Terrorism Act also contains failure to disclose and tipping-off
offences on equivalent terms to the offences under Sections 330, 333A and 342 of POCA.

1.4.1 The terrorist finance offences

As with the principal POCA offences, if a firm knowingly engages in business with, or otherwise
intentionally assists, a suspected terrorist or terrorist fundraising organisation, it is likely to
commit one of the three principal terrorist finance offences – fundraising, terrorist treasury or
assistance to terrorists – as a principal offender.
Additionally, in contrast to the primary POCA offences which, as discussed above, require an element of subjective intent (i.e. conducting business with knowledge or suspicion of money laundering), the Terrorism Act applies a second limb objective test to the terrorist finance offences, so that a firm may also commit one of the three principal terrorist finance offences by negligently engaging in business with or assisting a suspected terrorist money launderer.

Specifically, Section 15 of the Terrorism Act – the fundraising offence – provides that:

“(1) A person commits an offence if he -
(a) invites another to provide money or other property, and
(b) intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism.

(2) A person commits an offence if he -
(a) receives money or other property, and
(b) intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism.

(3) A person commits an offence if he -
(a) provides money or other property, and
(b) knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism.”

Section 16 of the Terrorism Act – the terrorist treasurer’s offence – provides that:

“(1) A person commits an offence if he uses money or other property for the purposes of terrorism.

(2) A person commits an offence if he -
(a) possesses money or other property, and
(b) intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism.”

Section 17 of the Terrorism Act – the assistance offence – provides that

“A person commits an offence if -
(a) he enters into or becomes concerned in an arrangement as a result of which money or other property is made available or is to be made available to another, and
(b) he knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism.”

In each case, the alleged offender must at least know (intent) or have reasonable cause (negligence) to suspect that money or other property will be used for the purposes of terrorism.

Terrorism means, for these purposes, the use or threat of serious violence or other specified action to persons or property which is designed to influence a government or an international governmental organisation or to intimidate a section of the public for the purpose of advancing a political, religious or ideological cause. The Counter-Terrorism Act 2008 contains provision to extend this to include the advancing of a racial cause, however, at the time of writing the relevant section is yet to brought into force. There is no jurisdictional limit to “terrorism” so that the terrorist finance offences may be committed in relation to entirely non-UK terrorist activities.

In addition, pursuant to Section 63, if a person does anything outside the UK which would have constituted the commission of an offence under any of Sections 15 to 17 if it had been done in the UK, he will be treated as having committed that offence (in the UK). There is no double-criminality override in relation to the Terrorism Act as there is in relation to the POCA offences.

An offence under Sections 15, 16 or 17 is punishable by a fine and up to 14 years’ imprisonment.

1.4.1.1 The terrorist money laundering offence

The terrorist money laundering offence is essentially the fourth terrorist finance offence, although in one sense it sits apart from Sections 15 to 17 because it is a strict liability offence. Section 18 provides that:

“(1) A person commits an offence if he enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property -

(a) by concealment,

(b) by removal from the jurisdiction,

(c) by transfer to nominees, or

(d) in any other way.

(2) It is a defence for a person charged with an offence under subsection (1) to prove that he did not know and had no reasonable cause to suspect that the arrangement related to terrorist property.”

An offence under Section 18 is punishable by a fine and up to 14 years’ imprisonment.
Terrorist property means money or other property which is likely to be used for the purposes of terrorism, the proceeds of acts of terrorism and the proceeds of acts carried out for the purposes of terrorism⁴¹.

Again, pursuant to Section 63, if a person does anything outside the UK which would have constituted the commission of an offence under Section 18 if it had been done in the UK, he will be treated as having committed that offence (in the UK).

The terrorist money laundering offence can be described as a strict liability offence because it can be committed without establishing intention or suspicion of a terrorist purpose on the part of the alleged offender. The reason it is not a strict liability offence in practice, however, is the existence of the specific defence in subsection (2) that a person may show that he did not know and had no reasonable cause to suspect that the arrangement in question related to terrorist property. The end result may appear to be the same for this offence as for the Sections 15 to 17 offences – if there is no intention or suspicion, there is no offence – but in practice the burden of proof is reversed. A firm or individual MLRO charged with a Section 18 offence must establish the defence to defend the charge, whereas the prosecuting authorities must establish intention or reasonable cause suspicion before they can charge for a Section 15, 16 or 17 offence.

As with the principal POCA offences, most firms may rightly consider the possibility of being charged with a principal terrorist finance offence to be remote in the absence of some degree of intention or recklessness on the part of their employees. However, firms and their employees clearly need to be familiar with the nature and extent of all the terrorist finance and money laundering offences so that they are in a position to avoid being reckless as regards those offences and to identify potentially disclosable offences for the purposes of the regulated sector failure to disclose offence under the Terrorism Act, discussed at 1.4.2 below.

Curiously, under the 2003 Regulations the training provisions specifically required regulated sector firms to train their staff in relation to the terrorist money laundering offence but made no such specific requirement in relation to the other principal terrorist finance offences. This slight oddity was corrected by the 2007 Regulations which impose a general requirement on firms to take appropriate measures to ensure that all relevant staff are "made aware of the law relating to... terrorist financing", which is defined to include all of the offences under Sections 15 to 18⁴⁴.

1.4.1.2 Cooperation with the police and SOCA (the Terrorism Act consent regime)

If a firm or an individual officer or employee of the firm knows or suspects that a suspicious person is engaged in terrorist activities, but nevertheless engages in activity with that suspicious person, that firm and the individuals involved may commit one of the terrorist finance offences if there is knowledge or reasonable cause to suspect that money or other property will as a result be used or made available for the purposes of terrorism.

The “authorised disclosure” regime discussed at 1.3.1 above in relation to the principal POCA offences is broadly reflected in the Terrorism Act at Sections 21, 21ZA and 21ZB.
Pursuant to subsection 21(1), a person does not commit a terrorist finance offence, or the terrorist money laundering offence, if he acted with the express consent of a constable (which in this case means the police rather than SOCA, although the constable is then required to notify the disclosure under this section to SOCA).

Pursuant to subsection 21(2) and Section 21ZB (introduced into the Terrorism Act in December 2007), a person does not commit a terrorist finance offence, or the terrorist money laundering offence, if he disclosed to a constable or SOCA, on his own initiative and as soon as reasonably practicable after having become involved in a transaction or arrangement (and in relation to a disclosure to SOCA under Section 21ZB, that there is a reasonable excuse for having failed to make a disclosure before becoming involved), his suspicion or belief that money or other property involved in that transaction or arrangement is terrorist property, and he did not subsequently act contrary to the instructions of the constable or SOCA.

It is also a defence to any those offences for a person to prove that he intended to make such a disclosure and there is a reasonable excuse for his failure to do so.

Under Section 21ZA, also introduced into the Terrorism Act in December 2007, a person does not commit a terrorist finance offence, or the terrorist money laundering offence, if before becoming involved in any transaction or arrangement he discloses to SOCA his suspicion or belief that money or other property involved in that transaction is terrorist property and the information on which that suspicion or belief is based, and he obtains consent to becoming involved in the transaction or arrangement concerned.

There are no prescribed time limits within which a constable may be required to give “express consent” for the purposes of subsection 21(1), but SOCA has seven working days after the day on which a disclosure is made to it under Section 21ZA in which to deny that consent, after which the person making the disclosure is entitled to construe consent as having been given.

These disclosures and consent requests are equivalent to “authorised disclosures” under POCA, and can be distinguished from the SARs regime which arises by virtue of the failure to disclose offences.

1.4.2 The failure to disclose offences

The Terrorism Act contains two failure to disclose offences. The first, set out in Section 19, applies to businesses other than regulated sector firms and uses a basic subjective test, i.e. does the person concerned believe or suspect that another person has committed a terrorist finance or money laundering offence. An offence under this section is punishable by a fine and up to five years’ imprisonment.

The second, at Section 21A, introduced to the Terrorism Act on 20 December 2001 by the Anti-terrorism, Crime and Security Act 2001 (the “ATCSA”), applies only to regulated sector firms and uses the objective negligence test which POCA has also subsequently applied to the regulated sector.
The history of the Section 21A failure to disclose offence is interesting, not least because of the speed at which it passed through Parliament (a matter of a few days), receiving Royal Assent in the early hours of 13 December 2001 and coming into force a week later; all part of the UK’s legislative response to the terrorist activities in New York and Washington DC in September of that year.

In fact, the objective negligence test for failing to disclose knowledge or suspicion of money laundering was a concept first proposed in the Proceeds of Crime Bill (as it then was). After September 2001, the objective test element of that Bill was essentially cut-and-pasted into the ATCSA in respect of terrorist finance offences and accelerated into the statute book.

Section 21A provides that:

“(1) A person commits an offence if each of the following three conditions is satisfied.

(2) The first condition is that he -

(a) knows or suspects, or

(b) has reasonable grounds for knowing or suspecting, that another person has committed or attempted to commit [a terrorist finance or money laundering offence].

(3) The second condition is that the information or other matter -

(a) on which his knowledge or suspicion is based, or

(b) which gives reasonable grounds for such knowledge or suspicion,

came to him in the course of a business in the regulated sector.

(4) The third condition is that he does not disclose the information or other matter to [a constable, SOCA] or [his firm’s MLRO] as soon as is practicable after it comes to him.”

The Section 21A failure to disclose offence is punishable by a fine and up to five years’ imprisonment.

The introduction of the objective test for regulated sector firms by the ATCSA was, like subsection 330(2)(b) of POCA, one of the most significant changes in anti-money laundering law in recent years because it effectively criminalises negligence. As with Section 330 POCA, if an individual employed in the regulated sector knows or suspects that a person is engaged in terrorist finance activities, or if a court determines that objectively he should have done, and he fails to notify SOCA or his MLRO, that individual may commit a serious criminal offence.

The obligation to disclose is in respect of knowledge or suspicion of conduct which constitutes a terrorist finance or money laundering offence or would do so if relevant conduct occurred in the...
UK\textsuperscript{51}. As noted above, the double-criminality override test under POCA, which carves out from the definition of criminal conduct certain conduct which is lawful in the jurisdiction in which it occurs even if unlawful in the UK, does not apply under the Terrorism Act.

As under POCA, an individual officer or employee of a firm can discharge his Terrorism Act disclosure obligations, and thereby avoid committing a criminal offence, by making a disclosure to his firm’s MLRO in accordance with the firm’s internal reporting procedures.

Again, the Guidance Notes have statutory recognition under the Terrorism Act as they do under POCA (see 1.3.2.4 above) so that a court “must” take into account a person’s compliance with the Guidance Notes in considering whether a terrorist finance offence has been committed. The Guidance Notes contain specific advice on how regulated sector firms can assess the objective test in the context of terrorist financing activity disclosures\textsuperscript{52}.

As under POCA, legal advisers and certain other professional advisers may in limited circumstances rely on a defence of privilege to avoid committing a failure to disclose offence under the Terrorism Act. It is also a defence for an individual charged with a failure to disclose offence under Section 21A to show that he had a “reasonable excuse” for not having made a disclosure\textsuperscript{53}. Again, the legal meaning of reasonable excuse in this context has not yet been tested in the courts and the prudent view is that the term will be construed narrowly. Legal professional privilege may be raised as a defence by lawyers charged with failing to disclose knowledge or suspicion of terrorist finance offences.

1.4.3 The tipping-off offence

As a result of legislative amendments made in December 2007\textsuperscript{54}, the tipping-off regime under the Terrorism Act is now on an equal footing with the tipping-off regime under POCA (see 1.3.3 above).

The main tipping-off offence under the Terrorism Act, at Section 21D, therefore now applies only to the regulated sector; it is largely the same as the POCA Section 333A offence, save that it applies in respect of persons who tip off others about the fact that a disclosure has been made to the police or SOCA or that an investigation is being contemplated or carried out in relation to Terrorism Act offences.

Section 21D of the Terrorism Act provides that:

“(1) A person commits an offence if -

(a) the person discloses any matter within subsection (2);

(b) the disclosure is likely to prejudice any investigation that might be conducted following the disclosure referred to in that subsection; and

(c) the information on which the disclosure is based came to the person in the course of a business in the regulated sector.
(2) The matters are that the person or another person has made a disclosure under a provision of this Part -

(a) to a constable,

(b) in accordance with a procedure established by that person’s employer for the making of disclosures under that provision;

(c) to a nominated officer, or

(d) to a member of staff of [SOCA] authorised for the purposes of that provision by the Director General of [SOCA],

of information that came to that person in the course of a business in the regulated sector.

(3) A person commits an offence if -

(a) the person discloses that an investigation into allegations that an offence under this Part has been committed is being contemplated or is being carried out;

(b) the disclosure is likely to prejudice that investigation; and

(c) the information on which the disclosure is based came to the person in the course of a business in the regulated sector.”

Like its equivalent in Section 333A of POCA, the Section 21D tipping-off offence is punishable by a fine and up to two years’ imprisonment.

The commentary in paragraph 1.3.3 on the POCA tipping-off offences for the regulated sector applies in essentially the same terms to the Terrorism Act tipping-off offences, with appropriate substituted references to the underlying terrorist offences. The Terrorism Act also provides limited safe-harbours from the tipping-off offence in the form of permitted disclosures which mirror those permitted disclosures set out in Sections 333B to 333E of POCA.55

In addition to this new tipping-off offence, the original tipping-off offence in Section 39 of the Terrorism Act, which is equivalent to the offence under Section 342 of POCA, remains and continues to apply to non-regulated sector firms.

Section 39 provides that where a person knows or has reasonable cause to suspect that law enforcement authorities are conducting or propose to conduct an investigation in connection with the commission of terrorist offences, that person commits an offence if he:

“(2) …

(a) discloses to another anything which is likely to prejudice the investigation, or
and further that if a person knows or has reasonable cause to suspect that disclosure of a suspected terrorist finance offence has been made to SOCA, that person commits an offence if he:

“(4) …

(a) discloses to another anything which is likely to prejudice an investigation resulting from the disclosure […], or

(b) interferes with material which is likely to be relevant to an investigation resulting from the disclosure […].”

The Section 39 offence is punishable by a fine and up to five years’ imprisonment.

It is a defence to the Section 39 tipping-off offence for an alleged offender to show that he “did not know and had no reasonable cause to suspect that the disclosure or interference was likely to affect a terrorist investigation” or that he had a “reasonable excuse”\(^56\) for the disclosure or interference\(^57\).

1.4.4 Practical issues associated with the consent regime

The same issues associated with the tension between seeking appropriate consents and avoiding tipping-off offences arise under the Terrorism Act as under POCA. If a regulated sector firm has suspicions about a particular customer or counterparty it must disclose those suspicions and seek consent from SOCA to avoid committing a terrorist finance or money laundering offence (and a Section 21A failure to disclose offence). At the same time, the firm must seek to avoid committing a tipping-off offence under Section 21D.

At the time of writing no specific guidance on the difficulties firms may face in respect of the Terrorism Act consent regime has been produced, however, it is assumed that the principles applicable in respect of the POCA consent regime as set out in the cases of Squirrell Ltd v National Westminster Bank plc and K Ltd v National Westminster Bank plc (see 1.3.4.1 above) will apply equally in respect of the Terrorism Act.

1.5 The Wire Transfer Regulation

On 1 January 2007 the EU Wire Transfer Regulation\(^58\) came into force. The Wire Transfer Regulation had been adopted by the EU Parliament and Council in November 2006 to implement Financial Action Task Force (“FATF”) Special Recommendation VII on the information that should be included in electronic funds transfers.

The purpose of the FATF recommendation was to close loopholes by which money launderers and terrorist financiers could use electronic means to transfer funds without having to disclose
their identity. The Wire Transfer Regulation has direct effect in the UK and all other EEA member states and applies to all legal or natural persons whose business includes the provision of transfer of funds services.

The FATF special recommendation, and accordingly the Wire Transfer Regulation, requires that Payment Service Providers ("PSPs") must include certain, specified information in all electronic funds transfers and must have in place measures to verify that information. The key information that is required to be included in a wire transfer instruction is the payer’s name, address and account number, although there are exceptions in certain circumstances.

To comply with the Wire Transfer Regulation, financial sector businesses need to consider which role they are fulfilling during their involvement in a payment chain. In that regard the Wire Transfer Regulation includes the following definitions:

> “Payer” means either a natural or a legal person who holds an account and allows a transfer of funds from that account, or, where there is no account, a natural or legal person who places an order for a transfer of funds,

> “Payment Service Provider” means a natural or legal person whose business includes the provision of transfer of funds services,

> “Intermediary Payment Service Provider” means a payment service provider, neither of the payer nor of the payee, that participates in the execution of transfers of funds.

To aid the interpretation of these definitions the JMLSG Guidance Notes cite the example of a bank or building society which effects an electronic funds transfer on a customer’s direct instructions to the debit of that customer’s account. In such a case, the bank or building society will be a PSP whether it undertakes the payment itself (in which case it must provide its customer’s details as the payer), or via an intermediary PSP. If the transfer is carried out through an intermediary PSP, the bank or building society must provide the required information on its customer to that intermediary PSP. This would include circumstances in which the bank or building society processes the payment through an electronic banking product supplied by the intermediary PSP.

Where, however, a financial sector business processes a transaction through an account in its own name, it would be reasonable for it to consider itself as the payer, rather than the PSP, even where the transaction ultimately relates to a customer, for example in respect of mortgages, insurance claims or financial markets trades.

To allow for enforcement of the Wire Transfer Regulation in the UK, in November 2007 the Treasury made the Transfer of Funds (Information on the Payer) Regulations 2007 (the “Transfer Regulations”). The purpose of these regulations was to make provision for (i) the enforcement of the obligations placed on UK financial sector businesses under the Wire Transfer Regulation, (ii) the supervision of PSPs, and (iii) enforcement powers for the supervisors.
Ultimately, the effect of the Transfer Regulations is that PSPs in the UK which are authorised by the FSA will be supervised by the FSA for the purposes of the Wire Transfer Regulation. Other PSPs in the UK will be supervised by HMRC which has included guidance on the Wire Transfer Regulation in its MLR 8 Guidance (see 1.3.2.4 above). This HMRC guidance is approved by the Treasury for the purpose of the Wire Transfer Regulation.

Failure to comply with the Wire Transfer Regulation can be a criminal offence punishable by a fine and up to two years’ imprisonment.

1.6 Investigations, confiscation and asset freezing

To assist the investigatory and enforcement processes involved in tackling money laundering and terrorist financing, law enforcement authorities and the Treasury have a range of powers to enable wide-ranging and effective investigations of money laundering and to undermine criminal and terrorist enterprises through asset freezing, seizure and confiscation. The most significant of these are contained in POCA, the Terrorism Act and the ATCSA. Since the first edition of this publication, however, further freezing and confiscation powers have been made available under the Serious Crime Act 2007 ("SCA") and the Counter-Terrorism Act 2008 ("CTA").

This paper does not cover the specific application of the investigatory powers, legislative and court processes involved in obtaining and serving the variety of orders available to law enforcement authorities and HM Treasury. It is sufficient that firms are aware that they must comply with a valid court order or Treasury order, subject to serious criminal sanctions either for direct breach of the order or under contempt of court proceedings.

It is useful, however, for firms to recognise some of the key orders which may be obtained by law enforcement authorities in connection with the investigation and enforcement of money laundering and terrorist financing offences and subsequent asset confiscation proceedings.

1.6.1 Investigatory orders

Investigations into money laundering and terrorist finance offences can often involve the analysis of otherwise confidential customer records held by financial institutions. Some law supervisory and enforcement authorities have for some time had the benefit of specific enhanced powers to order or procure disclosure of confidential information, but it is only since the ATCSA and POCA that these powers have become part of the basic toolkit of investigatory measures available to all law supervisory and enforcement authorities.

The key investigatory orders provided for by the ATCSA and POCA are account monitoring orders and customer information orders. Account monitoring orders require ongoing disclosure of information in relation to specific accounts whereas customer information orders require one-off disclosures of information in relation to specific persons.
1.6.1.1 Account monitoring orders

Account monitoring orders enable law enforcement authorities to monitor individual bank accounts for investigatory purposes. Investigators can apply to the court for an account monitoring order under the Terrorism Act in pursuance of an investigation into terrorist finance activities or terrorist organisations. The applicant must show that “the tracing of terrorist property is desirable for the purposes of the investigation” and that granting the order “will enhance the effectiveness of the investigation”\(^65\).

POCA makes provision for an equivalent order in relation to non-terrorist-related money laundering investigations\(^66\). There are three circumstances in which an account monitoring order may be obtained under POCA, namely in pursuance of: (1) a money laundering investigation (i.e. investigating whether a money laundering offence has been committed); (2) a confiscation investigation (i.e. investigating whether a person has benefited from his criminal conduct and identifying property which might be confiscated); or (3) a civil recovery investigation (i.e. investigating whether property is recoverable under the civil recovery process discussed at 1.6.2 below). Orders in relation to civil recovery investigations may only be granted by the High Court.

In each of those three circumstances, the applicant authority must show that there are reasonable grounds for making the order, that the information required to be disclosed by the order “is likely to be of substantial value (whether or not by itself) to the investigation for the purposes of which the order is sought”, and that it is in the public interest for that information to be disclosed\(^67\).

An account monitoring order under either Act requires a specific institution to provide specified information relating to all or any accounts held by a specified person for a continuous period of up to 90 days.

An institution (including its controlling officers) which is served with an account monitoring order but fails to comply is likely to be held in contempt of court.

1.6.1.2 Customer information orders

Unlike account monitoring orders which require financial institutions to give investigators access to customer information for a period of time, customer information orders obtained under the Terrorism Act\(^68\) or POCA\(^69\) require institutions simply to deliver up a snap-shot of the information which they hold in relation to specified customers.

An order may be sought in respect of all financial institutions, a group of institutions or a specific institution.

Customer information orders will only be granted in pursuance of a terrorist investigation, a money laundering investigation, a confiscation investigation or a civil recovery investigation and orders in relation to civil recovery investigations may only be granted by the High Court. The judge must be persuaded either that “the tracing of terrorist property is desirable” and that
granting the order “will enhance the effectiveness of the investigation” or, in the case of a POCA order, that there are reasonable grounds for making the order, that the information required to be disclosed by the order “is likely to be of substantial value (whether or not by itself) to the investigation for the purposes of which the order is sought”, and that it is in the public interest for that information to be disclosed.

If given, an order will require the financial institutions specified in the order to provide “any customer information” held in relation to the specified person or persons. Customer information, for these purposes, includes confirmation that a specified person holds or has held an account with the institution and the details of any such account (names, addresses, date of birth or incorporation details, evidence of identity obtained by the institution, signatories to the customers’ accounts and any other accounts for which the customer is a signatory).

An institution will commit a specific offence, punishable by fine, if it fails to comply with a customer information order or, in the case of a POCA order (but not a Terrorism Act order) provides false or misleading information in response to an order. The Terrorism Act makes specific provision for officers of institutions who consent to or connive in an institution’s failure to comply with a customer information order – an offence punishable by a fine and up to six months’ imprisonment.

1.6.2 Asset recovery and other remedies

The Terrorism Act has, since February 2001, enabled a court to seize property following the commencement of proceedings in respect of a terrorist finance offence, and then to confiscate that property following a conviction, if the property is intended to be used for the purposes of terrorism. The ATCSA enhanced those powers by enabling law enforcement authorities to apply to the court for property to be seized at the commencement of an investigation, even before proceedings were begun.

POCA introduced even wider powers in the context of other criminal investigations and proceedings – enabling courts to confiscate the proceeds of general as well as specific criminal conduct – and perhaps just as importantly established the Assets Recovery Agency (the “ARA”) whose task and objective it was to identify and confiscate criminal property and otherwise to ensure that criminals are deprived of the benefits of their crimes. While the ARA marked significant progress in preventing the distribution of criminal property in the UK, its existence became difficult to justify following a National Audit Office examination carried out in late 2006 which revealed that the ARA had spent £65m recovering £23m of proceeds of crime. While, arguably, the ARA had also disrupted the distribution of many more millions of proceeds of crime, the decision was taken that the ARA’s functions could be better performed if it merged with SOCA. Accordingly, with effect from 1 April 2008 SOCA took on the former responsibilities of the ARA and, in doing so, became the UK’s central agency for dealing with all law enforcement matters relating to serious organised crime.

The key orders which SOCA and certain other authorities may now seek in pursuance of their asset seizure and confiscation objectives are disclosure orders, restraint orders, forfeiture orders and serious crime prevention orders.
1.6.2.1 Disclosure orders

A disclosure order granted under Section 357 POCA enables an appropriate Director or member of staff of SOCA to require “any person whom [that Director or member of staff] considers has relevant information” to answer questions and/or provide information and/or produce documents in connection with an investigation to establish whether particular property may be confiscated or made the subject of a civil recovery action.

The judge must be persuaded that there are reasonable grounds for making the order, that the information required to be disclosed by the order “is likely to be of substantial value (whether or not by itself) to the investigation for the purposes of which the order is sought”, and that it is in the public interest for that information to be disclosed.

Failure to comply with a disclosure order can be punished with a fine and up to six months’ imprisonment. Supplying false or misleading information in response to a disclosure order is punishable by a fine and up to two years’ imprisonment.

A disclosure order cannot require a lawyer to disclose information which is subject to legal professional privilege, except to confirm the name and address of a particular client.

1.6.2.2 Restraint orders

A restraint order prohibits specified persons from dealing with specified property – essentially it is a form of freezing order. The court can make a restraint order under the Terrorism Act or under POCA on its own account, or on the application of law enforcement authorities (in general SOCA), at any time after an investigation has been commenced (in respect of a terrorist finance offence or other criminal offences, respectively). The court will grant the order if it appears that a forfeiture or confiscation order may be made in any proceedings for the offence.

Once a restraint order is made, property subject to the order can be temporarily seized to prevent it being dealt with or removed from the jurisdiction of the court.

1.6.2.3 Forfeiture and confiscation orders

The CTA contains provisions which will extend the current powers of forfeiture under the Terrorism Act. At the time of writing, these provisions of the CTA have not been brought into force, however, if they are given effect without revision the forfeiture provisions under the Terrorism Act will provide that upon conviction for a terrorist finance offence or terrorist money laundering offence, a court may order the forfeiture (i.e. confiscation) of any money or other property which was, at the time of the offence, in the offender’s possession or control and which had been used, which they intended should be used, or (in certain cases) which they had reasonable cause to suspect might be used, for the purposes of terrorism. The court may also order the forfeiture of any money or other property which either wholly or partly, directly or indirectly, is received by the offender as a payment or other reward.
Under POCA, the court has a much wider power to order the confiscation of criminal property when a person is convicted of any offence in, or committed for sentencing to, the Crown Court. The order is discretionary, but if a court is satisfied on the balance of probabilities that the person concerned has either benefited from the commission of that particular offence or benefited from “general criminal conduct”, it must generally order the proceeds of that criminal conduct to be seized (if it has not already been seized pursuant to a restraint order) and confiscated.\(^{81}\)

The ability to confiscate criminal property, even though it cannot be proven to be the proceeds of particular criminal conduct, was a significant development for law enforcement. In essence, it lowered the standard of proof required to confiscate assets. Under POCA, assets of a person convicted of an offence may now be seized on a burden of the balance of probabilities whereas previously it had been necessary to demonstrate that assets represented the benefit of specific criminal conduct for which a conviction had been secured.

If a court determines that it is appropriate to grant a confiscation order following a conviction, it is required to assess the level of benefit which an offender has received from general or particular criminal conduct and to order that the offender pay that amount.

If the court decides that an offender has a criminal lifestyle, in determining whether he has benefited from general criminal conduct, and in assessing the level of that benefit, it is required to assume that property which came into the offender’s possession up to six years before the date on which criminal proceedings were commenced (and any time after the date of conviction) represents the proceeds of his general criminal conduct.

Criminal lifestyle is defined in Section 75 POCA by reference to the nature of the offence of which the offender has been convicted. A conviction for drug trafficking, money laundering or any other prescribed lifestyle offence is conclusive evidence that the offender has a “criminal lifestyle”.\(^{82}\) Otherwise, a criminal lifestyle is deemed where the offence is one of at least three offences for which the offender has been convicted in the past six years and from which he has obtained a benefit, or where the offence was committed over a period of at least six months. An offender will not be deemed to have a criminal lifestyle unless the benefit obtained from those offences is at least £5,000.\(^{83}\)

Once granted, SOCA will ensure that an offender complies with a confiscation order, and may ask the court to make further enforcement orders if necessary.

1.6.2.4 Serious crime prevention orders

The serious crime prevention order (“SCP Order”) was introduced by Section 1 of the SCA with effect from 6 April 2008. The SCA enables SOCA and other law enforcement agencies to apply to the High Court for an SCP Order to be imposed on an individual pursuant to which conditions, restrictions or reporting requirements will apply with the purpose of restricting that individual’s involvement in serious crime.
For the purposes of imposing an SCP Order, a person has been involved in serious crime if he:

> has committed a serious offence (whether in England and Wales or elsewhere);

> has facilitated the commission by another person of a serious offence (whether in England and Wales or elsewhere); or

> has conducted himself in a way that was likely to facilitate the commission by himself or another person of a serious offence (whether in England and Wales or elsewhere and whether or not such an offence was committed).

A serious offence in England and Wales means an offence under the laws of England and Wales which, at the time when the court is considering the matter in question falls within a description specified in the SCA or which the court considers sufficiently serious to be treated as such. The offences specified in the act include, inter alia, various drug offences, people trafficking offences, arms trafficking offences, prostitution and child sex offences and the primary money laundering offences under POCA.

A person is treated as committing a serious offence outside England and Wales if: (a) he has committed a serious offence in a country outside England and Wales; (b) he has facilitated the commission by another person of a serious offence in a country outside England and Wales; or (c) he has conducted himself in a way that was likely to facilitate the commission by himself or another person of a serious offence in a country outside England and Wales (whether or not such an offence was committed).

An offence is treated as having been committed outside England and Wales if it is an offence in that other jurisdiction and, had it been committed in England and Wales, would have been a serious offence here, or is considered by the court to be sufficiently serious to be treated as if it would have been a serious offence here.

Section 1 of the SCA is drafted widely and enables the High Court to make an order containing “such prohibitions, restrictions or requirements; and such other terms; as the court considers appropriate for the purpose of protecting the public”. An SCP Order can only be made if the High Court is satisfied that the relevant individual has been involved in serious crime and if the High Court has reasonable grounds to believe that the order would protect the public by preventing, restricting or disrupting involvement by the individual in serious crime.

Typically an SCP Order would be used to restrict the ability of an individual to travel, or the persons with whom an individual may associate, but given the wide wording of the statutory provisions it is possible that an SCP Order could be used to restrict the ability of an individual to access certain assets or financial services.

An SCP Order may only be imposed on individuals who are over the age of 18 and are represented at the proceedings at which the SCP Order is made, and a notice setting out the terms of any SCP Order which is made must be served in person on the individual concerned.
1.6.2.5 Civil recovery and taxing powers

In addition to powers of seizing and confiscating the property of suspected and convicted criminals, SOCA also inherited from the ARA standing to bring a civil action to recover property which is or represents the proceeds of criminal conduct regardless of whether a criminal prosecution has been brought for an offence in connection with that property, and to exercise a taxation function in respect of income or gains which it reasonably believes to have arisen or accrued as a result of criminal conduct.

Part 5 of POCA sets out the civil recovery regime, which enables SOCA to apply to the High Court for a recovery order against any person whom “the authority thinks holds recoverable property.”

SOCA may wish to undertake civil recovery proceedings against a person’s property because that person cannot be tried for a criminal offence in the UK (and as such the court could not issue a confiscation order), for instance, because the person has died since the commission of the offence giving rise to the recoverable property, or because the person had no direct connection with the commission of the offence (for instance organised criminals may procure others to commit offences from which they ultimately obtain the benefit).

Essentially, the process of civil recovery involves an application to the court, pre-empted, if necessary, by an application for the appointment of an interim receiver over particular assets. The court may appoint an interim receiver if it is satisfied that “there is a good arguable case” that the property to which the application relates “is or includes recoverable property” or an interest in recoverable property. The function of the interim receiver is to prevent persons dealing with that property and, where necessary, to investigate whether particular property is recoverable property.

If an interim recovery order is subsequently given by the court, it must appoint a trustee for civil recovery, nominated by SOCA, whose function is to secure and preserve any recoverable property vested in him by the recovery order and to realise non-cash recoverable property. The proceeds of the recovery process are held by the trustee ultimately for the benefit of SOCA. Property ceases to be recoverable, by virtue of the Limitation Act, twelve years after the date on which it was obtained.

POCA enables SOCA to apply tracing provisions to recoverable property so that, for instance, the proceeds of a sale of recoverable property can in some circumstances be recoverable even if those proceeds do not themselves directly represent the proceeds of criminal conduct.

Part 6 of POCA sets out SOCA’s revenue functions. Section 317 provides that if SOCA has reasonable grounds to suspect that “income arising or a gain accruing to a person in respect of a chargeable period is chargeable to income tax or is a chargeable gain (as the case may be) and arises or accrues as a result of the person’s or another’s criminal conduct (whether wholly or partly and whether directly or indirectly)” it may notify HMRC that it intends to exercise revenue functions in respect of that person. SOCA can then exercise the revenue powers which could
otherwise be exercised by HMRC and demand that an individual pay tax on particular income or capital gains. SOCA’s assumption of revenue powers can be undertaken in respect of corporate entities as well as individuals.  

1.6.3 Freezing orders and sanctions legislation

"Asset freezing makes an important contribution to national security, by helping to prevent funds being used for terrorist purposes; and it is central to our obligations under successive UN Security Council Resolutions to combat global terrorism." (Kitty Ussher MP, Economic Secretary to the Treasury, June 2008)

UK financial institutions will be familiar with the orders which the Treasury has for some time issued to implement sanctions imposed by UN Security Council Resolutions against particular governments, territories, regimes or individuals.

The Government is also required to give effect to European Union measures imposing financial sanctions or other restrictive measures. Such measures are typically made pursuant to European Regulations, which are directly-effective in each Member State but require implementation into domestic legislation in order to impose criminal sanctions (European legislation cannot impose criminal sanctions into national laws). The European Union implements sanctions imposed by the UN Security Council, but may also impose other wider restrictive measures.

The Al-Qa’ida and Taliban (United Nations Measures) Order 2006 (the “Al-Qa’ida Order”) is an example of a far-reaching UK sanctions measure which implements both UN and EU sanctions.

The Al-Qa’ida Order prohibits persons from dealing with the funds or economic resources of any person who has been specifically designated in a direction issued by the Treasury, and from making funds or economic resources available to any such designated persons, unless authorised by licence granted by the Treasury to do so. There is a specific exemption for banks to permit interest to be credited to an account which has been frozen pursuant to the Al-Qa’ida Order, although such interest must also remain frozen in any such account once credited.

The Al-Qa’ida Order also imposes a positive notification obligation on financial institutions which are authorised for the purposes of FSMA. Any such “relevant institution” must inform the Treasury if it knows or suspects that any person who is its customer or with whom it has had dealings in the course of its business is a person designated by a UN Security Council Resolution, a person owned or controlled by a designated person or any person who has committed an offence under the Al-Qa’ida Order (i.e. a person who has made funds available to a designated person).

The Al-Qa’ida Order empowers the Treasury to request any person (including an authorised financial institution) in the UK to produce any information or document which the Treasury may require in connection with implementing or enforcing the sanctions made under it. Disclosure of such information is specifically exempted from statutory and common law protections relating to data security and confidentiality. The Treasury cannot, however, compel disclosure of legally privileged information or documents.
Offences under the Al-Qa’ida Order can be punishable by a fine and up to seven years’ imprisonment.

The Treasury’s exercise of its sanctions and asset freezing powers in these cases is, however, limited to circumstances where either or both of the UN Sanctions Committee and the Council of the European Union have imposed sanctions or other restrictive measures.

Separately, the ATCSA and the CTA have provided powers for SOCA and the Treasury to take action to freeze assets and impose a range of other sanctions on their own initiative.

1.6.3.1 Orders under the Anti-Terrorism, Crime and Security Act 2001

The ATCSA built on the UN sanctions powers by giving the Treasury the power to issue freezing orders on its own initiative.

The ATCSA freezing orders prevent UK persons (including UK nationals and bodies corporate situated outside the UK) from making funds available to or for the benefit of a specified resident or government of a country or territory outside the UK.

The Treasury may make an ATCSA freezing order if it reasonably believes that “action to the detriment of the United Kingdom’s economy (or part of it)” or “action constituting a threat to the life or property” of one or more nationals or residents of the UK “has been or is likely to be taken by a person or persons”. A freezing order could, for instance, require a bank to prevent withdrawals and block cheques or a broker-dealer to prevent further dealings in investments by its customers. An order could also extend to the overseas branches of a UK-incorporated regulated sector firm, and could potentially even require the freezing of the assets of an overseas entity which are held in an overseas jurisdiction by the overseas branch of a UK-incorporated firm.

The Treasury used its power to make an ATCSA freezing order to issue the Landsbanki Freezing Order 2008 which was used to freeze the UK branch assets of Landsbanki Islands hf, the Icelandic bank which ran into difficulties in 2008. The purpose of the Landsbanki Freezing Order was to freeze the UK assets of Landsbanki Islands hf on the grounds that action to the detriment of the UK’s economy had been or was likely to be taken by the government of Iceland or persons resident in Iceland. The action was taken in order to protect the depositors of the UK internet banking operations of Landsbanki known as Icesave.

The Landsbanki Freezing Order was expressed to apply to any person in the UK and any person elsewhere who is either a British citizen (including, among others, British Overseas citizens and British overseas territories citizens) or a body incorporated under the law of any part of the UK. Accordingly, the Landsbanki Freezing Order applied to all banks, financial institutions, charitable organisations and non-governmental organisations in the UK or established under UK law. It would not, however, apply to non-UK subsidiaries of UK parent companies where the non-UK subsidiary operates wholly outside of the UK and does not have UK legal personality.
Though each order made under the ATCSA must specify the consequences of breach, failure to comply with a freezing order is likely to give rise to criminal liability with an ultimate punishment of up to two years’ imprisonment. This was the case in the Landsbanki Freezing Order¹⁰¹.

1.6.3.2 Directions under the Counter-Terrorism Act 2008

The anti-money laundering provisions set out in the CTA came into force on 27 November 2008. The CTA confers on the Treasury the power to make directions in connection with terrorist financing, money laundering and certain other activities, together with a provision for enforcement.

The anti-money laundering provisions contained in the CTA were a late addition during the passing of the Counter-Terrorism Bill and were introduced without consultation. The reason for this addition was, reportedly, to cure a perceived defect in the Treasury’s powers to implement recommendations which are expected to be made in 2009 by the Financial Action Task Force in relation to Iran.

A direction may be made by the Treasury under Schedule 7 to the CTA if one or more of the following conditions are satisfied:

- the FATF has advised that measures should be taken against a country because of the risk of terrorist financing or money laundering being carried on in that country, by the government of that country or by persons resident in that country;
- the Treasury reasonably believes that terrorist financing or money laundering is being carried on in a country, by the government of that country or by persons resident in that country; or
- the Treasury reasonably believes that either (i) the development or production of nuclear, radiological, biological or chemical weapons, or (ii) the doing in the country of anything that facilitates the development or production of such weapons, poses a significant risk to the national interests of the United Kingdom.

If one or more of those conditions is satisfied, the Treasury may issue a direction which applies to a particular person operating in the UK financial sector, any description of persons operating in that sector¹⁰², or all persons operating in that sector (for these purposes “affected persons”).

A CTA direction can apply requirements in relation to transactions or business relationships with a particular person carrying on business in a specified country, the government of that country, or a person resident or incorporated in that country¹⁰³ (for these purposes “prescribed persons”). Such a direction may also impose requirements in relation to a particular prescribed person, any description of prescribed persons or all prescribed persons¹⁰⁴. The Treasury may not for these purposes prescribe a person in another EEA Member State.
Requirements can be imposed as follows:

> to require affected persons to carry out increased customer due diligence (either generally or in a specified manner) in relation to prescribed persons; and/or

> to require affected persons to perform additional ongoing monitoring (either generally or in a specified manner) in relation to prescribed persons; and/or

> to require affected persons to provide specified information or documentation to a person specified in the direction on a periodic or regular basis; and/or

> to prohibit affected persons from dealing with prescribed persons.

Failure to comply with an order made under the CTA will constitute an offence punishable by a fine and up to two years’ imprisonment.

The introduction of the CTA directions regime represents another substantial widening of the UK Government’s powers to restrict or prohibit dealings by financial institutions with countries, governments, firms or persons on its own initiative.

### 1.6.3.3 Rights to challenge sanctions measures

The CTA introduced, with effect from 27 November 2008, the right for any person affected by a UK sanctions measure made under the CTA, the ATCSA or pursuant to United Nations sanctions legislation, to apply to the High Court to have that sanction set aside. In considering any such application, the court will apply the principles relevant to an application for judicial review and may consequently quash any order or direction made by the Treasury under that legislation.

The introduction of this challenge procedure follows a high profile case in the Court of Appeal in which a group of individuals subjected to sanctions measures in the UK successfully challenged directions made under the Terrorism (United Nations Measures) Order 2006 and the Al-Qa’ida and Taliban (United Nations Measures) Order 2006 both of which are Orders in Council made under the United Nations Act 1946.

The individuals had originally challenged the validity of the two Orders on the grounds, inter alia, that no proper procedural safeguards had been put in place to protect persons subject to directions made under the Orders. Although ultimately the Court of Appeal did not find that a lack of procedural safeguards was sufficient to quash either the Orders or the directions made thereunder, the court found that some safeguards were necessary in respect of any directions made and, where no such safeguards are provided, that it would be for the court to appoint a special advocate to consider that direction’s validity. Clearly any such appointment could create uncertainty for the Treasury as to whether directions it has made are valid. The Treasury’s response to mitigate the concern expressed by the court is to ensure that the CTA contains provision to allow applications to set aside a sanction measure.
1.7 Conclusion

In recent years, the existing UK statutory framework has remained broadly unchanged, having undergone a substantial consolidation and development between 2000 and 2003. There have certainly been technical changes to the way in which some of the key anti-money laundering and terrorism-related offences operate, but mostly to iron out issues which became apparent in their first few years of operation. The greatest area of change has been the enactment of the Money Laundering Regulations 2007 and the wholesale revision of the JMLSG Guidance Notes.

The Government has consolidated anti-money laundering and terrorist finance expertise in SOCA, which is now the core investigatory and asset seizure authority around which the UK statutory framework is constructed and, having made a considerable effort to work through early teething troubles, is now a more efficient and generally more helpful organisation for regulated sector firms to deal with.

The Government has also continued to widen the scope of the investigatory and enforcement powers available to SOCA and other supervisory and investigatory authorities, as well as extending its own powers to apply sanctions on a unilateral basis. It may in the years to come now seek to make greater use of those powers, which undoubtedly have the potential to impact significantly on the operations of financial sector firms conducting business in the UK.

Some will consider that such measures are necessary and invaluable in the national and international fight against criminal and terrorist enterprises. Others may be more sceptical, seeing the continued extension of significant, and in some cases arguably draconian, powers for Government and law enforcement authorities to seize property and restrict the freedom of individuals and firms to pursue business activities freely as a negative which in the long term risks making the UK a less attractive place in which to do business.
2. PART 2: THE ROLE OF THE FSA IN THE UK MONEY LAUNDERING REGIME

2.1 Background

Under FSMA, the FSA – the single statutory regulator for the whole of the UK financial services sector – is given four regulatory objectives, one of which is the reduction of the extent to which it is possible for a business carried on by a regulated person (or by a person who ought to be regulated) to be used for a purpose connected with financial crime.

Financial crime for these purposes is stated to include any offence involving:

(a) fraud or dishonesty;
(b) misconduct in, or misuse of information relating to, a financial market; or
(c) handling the proceeds of crime.

The FSA is required, in pursuance of this objective, to have regard in particular to the desirability of:

*(a) regulated persons being aware of the risk of their businesses being used in connection with the commission of financial crime;
(b) regulated persons taking appropriate measures (in relation to their administration and employment practices, the conduct of transactions by them and otherwise) to prevent financial crime, facilitate its detection and monitor its incidence;
(c) regulated persons devoting adequate resources to the matters mentioned in paragraph (b)*109.

For the purpose of these provisions, "regulated person" means any authorised person and any recognised investment exchange or recognised clearing house. That is, all banks, investment firms (including investment advisors, investment managers, stockbrokers, corporate finance firms and others involved in providing professional services in relation to investments) and insurance companies whose activities require authorisation by the FSA pursuant to the requirements of FSMA come within the FSA’s jurisdiction for these purposes110.

Most, if not quite all, of these institutions will, of course, be regarded as carrying on relevant business for the purposes of the Money Laundering Regulations 2007 and will therefore in any event be required to comply with the requirements of the 2007 Regulations (and would have been required to comply with the requirements of the predecessor Regulations from 1994 and 2003). Prior to the establishment of the FSA, the Money Laundering Regulations stood alone as the source of requirements as to anti-money laundering procedures for financial sector firms. Although investment firms, in particular, were subject to extensive conduct of business rules prescribed by the self-regulatory organisations111 which existed under the regulatory regime created by the Financial Services Act 1986, none of those organisations wrote separate rules to address anti-money laundering procedures. Rather, they simply required their members to comply with the Money Laundering Regulations.
FSMA gives the FSA power to make rules specifically in relation to the prevention and detection of money laundering in connection with the carrying on of regulated activities by authorised persons. In a Consultation Paper (“CP”) published in April 2000, before the new legislation was enacted, the FSA noted that FSMA would give it a role in relation to money laundering which differed from the roles of its predecessors by being “explicit and adequately empowered”, involving both the setting and enforcing of standards. In deciding how it should perform this new role, the FSA noted that it was not the function of the regulator to perform the investigatory or prosecutorial role of the law enforcement authorities, but that it could best add value by concentrating on the systems and controls inside regulated businesses whilst at the same time actively pursuing cooperation between the law enforcement authorities, the industry and financial regulators. It apparently regarded its new role as being not the setting of new standards, but primarily the increasing of confidence that the industry “is consistently and effectively meeting existing standards”.

Against this background, the FSA focused upon what it regarded as the essential systems and controls which a financial services business should have in order to be vigilant and effective against money laundering. It identified these as being:

- to take care when commencing business with a new customer;
- at that stage, and subsequently, to give alert and informed consideration to the possibility of money laundering by a customer or prospective customer;
- where suspicions of money laundering arise, to communicate them to the authorities;
- to ensure senior management oversight and control (without impeding the communication of individual suspicions to the authorities);
- to secure and maintain the informed participation in these systems of all relevant employees of the business; and
- to keep records which may prove significant for subsequent criminal investigations and prosecutions.

The FSA noted that these issues were already recognised as constituting best practice in the industry (perhaps, at least in part, because they mirror fairly closely the requirements of the Money Laundering Regulations to which the industry had then been subject for some time).

During the consultation process which followed the publication of CP 46, issues were raised as to whether the FSA’s “parallel but separate” approach in the area of anti-money laundering procedures (that is, writing its own set of rules to exist alongside the Money Laundering Regulations) was in fact the right one, given the existing complexity of the law in this area and a doubt as to whether the imposition of a new set of regulatory requirements would add proportionately to the effectiveness of the regime as a whole. Notwithstanding those doubts, the FSA stuck to its original approach, and the ML Sourcebook ("ML Sourcebook") came into being as
an additional layer of anti-money laundering regulation for the financial sector, covering much of
the same ground as the Money Laundering Regulations but with some differences of detail, and
bringing with it a separate set of regulatory sanctions.

The ML Sourcebook contained eight separate chapters dealing, in quite specific terms, with
matters such as client identification (including detailed provisions reflecting the Government’s
concerns about financial exclusion), the reporting of suspicious transactions (including provisions
requiring a firm to give its MLRO access to “know your business” information which might be
relevant to a decision as to whether a transaction was indeed suspicious), the use of national
and international findings of material deficiency in the anti-money laundering arrangements
in any other state or jurisdiction, staff awareness and training and the appointment and role of
the MLRO (including requirements as to his level of seniority within the organisation and the
resources available to him to perform his functions effectively).

It was recognised at the time that, in addition to the specific provisions of the ML Sourcebook,
it was also necessary for firms to bear in mind that failure to operate appropriate anti-money
laundering procedures might result in breaches of provisions elsewhere in the FSA Handbook of
Rules and Guidance (“FSA Handbook”). The Principles for Business, which are set out in the High
Level Standards block of the Handbook (and which constitute FSA “Rules”, the breach of which
can give rise to disciplinary proceedings notwithstanding the high-level and generalised way in
which they are expressed) require a firm to take reasonable care to organise and control its affairs
responsibly and effectively, with adequate risk management systems. This requirement is
developed in more detail in the Senior Management, Systems and Controls (“SYSC”) Sourcebook
which provides, for example, that a firm must take reasonable care to establish and maintain such
systems and controls as are “appropriate to its business”, and that a firm must take reasonable
care to establish and maintain effective systems and controls for compliance with applicable
requirements and standards under the regulatory system and for countering the risk that the
firm might be used to further financial crime. It was noted by the FSA in CP 199, published
in September 2003, that the reference in SYSC to the ML Sourcebook had been misinterpreted
as meaning that the Sourcebook was an exhaustive statement of its requirements in respect
of money laundering, as a result of which an amendment was made to make clear that firms
were required to read the Sourcebook alongside all other FSA requirements and the criminal law.
Clearly, in circumstances where no breach of a specific requirement of the ML Sourcebook had
occurred but the FSA took the view that a firm had allowed itself to be used for the purposes of
financial crime, disciplinary action could be taken for breaches of the more general obligations
elsewhere in the FSA Handbook.

Further, individuals appointed to perform “controlled functions” involving the exercise of
“significant influence” in an authorised firm (such as directors, the chief executive and the
individuals in charge of compliance and of money laundering reporting) might themselves be
personally liable to disciplinary action by the FSA in respect of failures in the firm’s anti-money
laundering procedures. Such individuals are required to observe the FSA’s Statements of Principle
for Approved Persons. Principle 7 requires an approved person who performs a “significant
influence function” to take reasonable steps to ensure that the business of the firm for which he
is responsible complies with the relevant requirements and standards of the regulatory system.
The Code of Practice for Approved Persons\textsuperscript{120} states that the FSA expects approved persons performing significant influence functions to take reasonable steps to ensure that the business for which they are responsible has operating procedures and systems which include well-defined steps for complying with the detail of relevant requirements and regulatory standards. As originally written, it noted specifically that failure by a firm’s MLRO to discharge the obligations imposed on him by the ML Sourcebook would constitute a failure to comply with Principle 7, but it was also clear that other individuals could also be regarded as liable for failures under the more general wording. The FSA may take disciplinary action against approved persons in respect of misconduct, which includes failure to comply with any statement of principle (such as Principle 7)\textsuperscript{121}.

It was also notable that, in addition to the regulatory sanctions arising out of the requirements of the ML Sourcebook and other parts of the FSA Handbook, third parties might also have had rights of action against firms which failed to observe the FSA’s Rules. Section 150 of FSMA provides that a contravention by an authorised person of a Rule is actionable by a private individual who suffers loss as a result of that contravention. The section may be disapplied by the FSA in respect of contraventions of particular Rules, and has been disapplied, for example, in respect of breaches of the Principles and the high level Rules contained in the SYSC Sourcebook. Despite the close connection between those Rules and the ML Sourcebook noted above, however, the FSA elected not to extend disapplication to the ML Sourcebook. Thus, where a failure by a financial institution to comply with its ML Sourcebook obligations could be shown to have caused a loss to a private individual (e.g. where the victim of a fraud could show that his funds would have been recoverable but for the failure of a firm to detect and report a suspicious transaction on the part of the fraudster, where that failure arose out of systems and procedures which did not comply with ML Sourcebook requirements) that individual could have had the right under Section 150 to sue the financial institution for his loss. Fears were expressed during the consultation process that the FSA’s decision not to disapply Section 150 in relation to the ML Sourcebook would expose financial institutions to unjustified claims because of their perceived “deep pockets”, but the FSA did not accept that this was in itself grounds for disapplication.

With effect from 1 March 2006, however, there has been a fundamental change in the approach of the FSA to anti-money laundering provisions in the Handbook (although not, the FSA would be keen to emphasise, in its determination properly to perform its statutory obligations in relation to the prevention of this particular type of financial crime).

In CP 05/10, published in July 2005, the FSA set out its proposals for a review of its anti-money laundering regime. This was part of the wider Handbook simplification project on which the FSA was then embarking, moving generally towards regulation based on a greater extent on high-level principles and less on detailed and prescriptive rules. The FSA set out in that Consultation Paper the guiding principles for the project:

\begin{itemize}
\item focussing on making changes in areas where it could have a real impact and only responding to suggestions to make changes to individual Handbook provisions where the benefits were clear;
\end{itemize}
As the first step in the Handbook review, the FSA proposed in CP 05/10 (among other less far-reaching changes relating to approved persons and training and competence) the complete deletion of the ML Sourcebook and its replacement with a small number of high-level provisions in SYSC, building on the pre-existing provisions of SYSC 3.2.6R noted above. This, it was said, would better reflect the FSA’s focus on risk management and systems and controls as well as its desire to encourage a more flexible, risk-based approach to anti-money laundering safeguards in firms and a clearer focus on the oversight responsibility of senior management.

It was also noted, in passing, that the changes would remove duplication with legal obligations and radically simplify anti-money laundering rules. Perhaps understandably, no reference was made to the fact that the duplication and complexity now being addressed were largely the result of the creation of the ML Sourcebook at the time when the Handbook was first developed, despite the views of commentators and many firms that it was unnecessary.

Sir Callum McCarthy, then Chairman of the FSA, explained the shift in thinking at the time:

“The specialist Money Laundering Sourcebook underpinned our efforts in the early years to set requirements and raise standards in firms, at a time when implementation of the necessary standards across the industry was patchy. But the Sourcebook does not fit today’s needs. It gives firms some very specific requirements in areas such as customer identification and training, yet is silent over the use of other tools such as monitoring and Know Your Customer. It also has little to say about the assessment and mitigation of risk. And it is largely a duplication of the legislation and the Joint Money Laundering Steering Group’s Guidance.”

The creation of new high-level rules in SYSC also affected the application of Section 150 of FSMA. Since the new rules were inserted in the general rules on systems and controls, Section 150 no longer applies to the FSA’s money laundering regime. This means that private individuals no longer have a right to sue financial institutions for loss arising from a failure to comply with the money laundering requirements of the Handbook. This reversal of policy by the FSA was not discussed in CP 05/10 nor in the subsequent Policy Statement but was no doubt reassuring for those firms which had previously expressed disquiet over the situation under the ML Sourcebook (although it is fair to say that there do not seem to have been any instances of actions being brought under Section 150 in this context).

### 2.2 The SYSC rules and guidance on Money Laundering

The final version of the new SYSC rules and guidance was published in January 2006 and came into force with effect from 1 March 2006 (with a transitional period expiring on 31 August 2006).
The rules and guidance seek to encourage a risk-based approach, where firms actively identify and then manage the particular money laundering risks they are likely to face, rather than simply attempting to meet a series of formal regulatory obligations. This move to a risk-based approach is in keeping with the FSA’s general move from a regime founded on detailed rules and guidance towards a more principles-based approach to regulation. John Tiner, the former Chief Executive of the FSA, described the approach as follows:

“In essence it’s about regulating with the emphasis on principles and high level rules, not prescription of processes; it relies on setting out the outcomes we want to see achieved in the financial services market and then directing our supervision to assessing how they are being achieved.”

This focus on outcomes rather than on detailed processes is intended by the FSA to give a degree of flexibility, allowing firms to tailor their approach to their particular circumstances, and also placing a greater emphasis on the responsibility of senior management to establish and maintain effective systems and controls.

Aside from this move away from detailed rules, the two major changes brought about by the new SYSC rules and guidance were a far more explicit reliance on the JMLSG Guidance Notes, and the creation of a new post of anti-money laundering director or senior officer.

An understanding of the relationship between SYSC and the JMLSG Guidance Notes is crucial in order for firms to comply with the FSA’s requirements as set out in SYSC. Although the legal basis for the relationship is unchanged, the deletion of the ML Sourcebook has meant that firms in the regulated sector now have to rely largely on industry guidance outside the FSA Handbook in order to interpret and apply the FSA’s requirements as set out in the SYSC rules and guidance.

The FSA made clear that it did not intend formally to approve the JMLSG Guidance Notes since this is the role of the HM Treasury. Nor, it claimed, would compliance with the JMLSG Guidance Notes become compulsory since firms must exercise their judgement in applying them.

However, it is clear that a firm needs to consider the JMLSG Guidance Notes and be prepared to justify its actions in the event that it does not follow them. According to the JMLSG Guidance Notes, “departures from this guidance, and the rationale for doing so, should be documented, and may have to be justified, for example, to the FSA.” Furthermore, Philip Robinson, the FSA’s Financial Crime Sector Leader, in a speech in November 2005, said:

“I have to say that I find it difficult to see how firms will be able to maximise their contribution to the fight against money laundering and terrorist financing without at least making reference to the Guidance. So if a firm does not have a well thumbed copy, or whatever is the www. equivalent of that (!), our supervisors may well want to know why.”

In order to give a fuller picture of the wider implications of the regulatory requirements in SYSC, brief references to the JMLSG Guidance Notes have been included in the following description of the SYSC provisions where appropriate.
2.2.1 SYSC 1 – Application and purpose

The SYSC rules and guidance which replaced the ML Sourcebook apply to all authorised firms other than those whose only regulated activities consist of certain types of insurance business (essentially, general insurance, broking in relation to general insurance and pure protection, long-term insurance business falling outside the Consolidated Life Directive collective insurance, insurance relating to certain Lloyd’s business and mortgage broking and administration).

The rules also apply to UK branches of passporting EEA firms to the extent that they cover matters responsibility for which is not reserved to the relevant home state regulator. As, under the single market directives, prudential matters are reserved to home state regulators, in practice this means that the rules (with the express exception, in the case of MiFID firms, of the SYSC record keeping requirements) do not apply to UK branches of EEA firms. EEA firms which are operating on a services only basis in the UK are not required to comply with the relevant parts of SYSC.

The rules do not apply to sole traders, Undertakings for Collective Investment in Transferable Securities ("UCITS") qualifiers (operators, trustees or depositaries of recognised collective investment schemes authorised under Schedule 5 FSMA) or authorised professional firms.

The exclusion of certain types of insurance business, which mirrors similar exclusions previously set out in the ML Sourcebook, stems from a mismatch between the scope of FSMA and the scope of the 2007 Regulations. The latter apply to most financial institutions, but not to companies conducting insurance business of a type referred to in SYSC 1.1.3AR. At the time when the exclusion in respect of these companies was made, the FSA took the view that its Rules should not apply more widely than the Money Laundering Regulations. It did, however, issue a warning that it would reconsider the position if that seemed necessary, and might at the same time ask HM Treasury to consider extending the scope of the Money Laundering Regulations (then the 2003 Regulations) to cover general insurance so as to maintain the connection between the two sets of requirements. However, the 2007 Regulations similarly do not apply to insurance companies other than insurance companies which are duly authorised in accordance with the Consolidated Life Directive when they carry out activities covered by that directive, and insurance intermediaries acting in respect of long-term contracts of insurance.

It is to be noted, however, that there are other mismatches which are outside the power of the FSA to remedy. For example, bureaux de change activities are not regulated under FSMA, with the result that the SYSC rules do not apply to them, but they are subject to the 2007 Regulations and, as a result, to the parallel regulatory regime overseen by HM Revenue and Customs. In this connection the FSA has noted that when activity of this type is carried on by an authorised person or by a subsidiary of an authorised person, it will regard that activity as relevant to the performance of the FSA’s authorisation and supervision functions in relation to the authorised person because of the reputational, managerial, financial or other exposure which could arise from carrying on those activities even though the FSA will not have formal supervisory powers in respect of those activities. Under the 2007 Regulations, any authorised person proposing to carry on (or cease to carry on) bureaux de change business must first inform the FSA.
In general, SYSC applies only in relation to activities carried on from an establishment in the UK. The FSA has, however, noted that where a UK authorised firm is able to exercise control over business carried on outside the UK (e.g. through an overseas branch or subsidiary), it will look at how that control is exercised in the prevention and detection of money laundering in the non-UK business. Once again, it cites reputational, managerial, financial or other exposure of the relevant firm as the justification for this broad approach. It is not clear whether the FSA regards compliance with host state rules as sufficient in these circumstances.

Three of the stated purposes of SYSC, which pre-date the introduction of the high-level rules on money laundering, are:

(a) “to encourage firms’ directors and senior managers to take appropriate practical responsibility for their firms’ arrangements on matters likely to be of interest to the FSA”;

(b) to increase certainty by amplifying Principle 3 under which a firm must “take reasonable care to organise and control its affairs”;

(c) “to encourage firms to vest responsibility for effective and responsible organisation in specific directors and senior managers”.

With the implementation of MiFID in November 2007, SYSC has undergone some restructuring. In particular, SYSC 4 to 18 were inserted to implement the MiFID requirements in respect of the organisation and management of relevant firms. These sections initially applied only to “common platform firms” (that is, firms which are subject either to MiFID or to the Capital Requirements Directive). For these firms, SYSC 6.3 set out the requirements relevant to anti-money laundering procedures, in terms which were essentially identical to the equivalent provisions of SYSC 3.2.6R which then applied to all other regulated firms subject to the exclusions set out above. With effect from 1 April 2009, however, SYSC is again amended so that the “common platform” requirements (including SYSC 6) apply to all firms other than insurers, managing agents and Lloyd’s, with some modifications for firms which are not common platform firms. This paper refers in most cases primarily to the requirements of SYSC 6.3, since these are with effect from 1 April 2009 the provisions which apply to most regulated firms, but reference is also made to the equivalent provisions of SYSC 3.2.6, which remain relevant for insurers, managing agents and Lloyd’s.

2.2.2 SYSC 6.1.1R/SYSC 3.2.6R – Adequate practices and procedures

The pre-existing rule at SYSC 3.2.6R is the cornerstone of the rules and guidance which replaced the ML Sourcebook. This rule required a regulated firm to take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm will be used to further financial crime. The rules and guidance at SYSC 3.2.6AR to 3.2.6JC were essentially treated as an amplification of this rule.
SYSC 6.1.1R is the equivalent provision in the post-MiFID regime. It is expressed as an absolute obligation (rather than a “reasonable care” obligation) on firms to establish, implement and maintain adequate practices and procedures sufficient to ensure compliance under the regulatory system and for containing the risk that the firm might be used to further financial crime.

It should be noted that SYSC 6.1.1R, as with SYSC 3.2.6R in its original form, does apply to general insurance and mortgage intermediary firms. Accordingly, even though they are not obliged to comply with the 2007 Regulations, these firms must have appropriate systems and controls in place to comply with the regulatory system and to counter the risk that they will be used to further financial crime.

2.2.3 SYSC 6.3.1R/SYSC 3.2.6AR – Adequacy of systems and controls

This rule requires a firm to ensure that the systems and controls established and maintained under SYSC 6.1.1R/SYSC 3.2.6R enable it to identify, assess, monitor and manage money laundering risk. The systems and controls must be comprehensive and proportionate to the nature, scale and complexity of the firm’s activities.

This rule aims to encourage firms to adopt the FSA’s risk-based approach, and is discussed in slightly more detail in the guidance contained in SYSC 6.3.6G/SYSC 3.2.6FG. However, the interpretation of the rule must necessarily rely upon the detailed provisions of the JMLSG Guidance Notes, which describe the steps a firm should take in order to follow a risk-based approach137. A firm should:

(a) identify the money laundering and terrorist financing risks that are relevant to the firm;

(b) assess the risks posed by the firm’s particular customers, products, delivery channels, geographical areas of operation;

(c) design and implement controls to manage and mitigate these assessed risks;

(d) monitor and improve the effective operation of these controls; and

(e) record appropriately what has been done and why.

2.2.4 SYSC 6.3.2G/SYSC 3.2.6BG – Definition of “money laundering risk”

This guidance defines “money laundering risk” as the risk that a firm may be used to further money laundering, and notes that a failure to manage this risk effectively will increase the risk to society of crime and terrorism.

From a technical point of view, this definition indicates a distinction between the rules and guidance in SYSC and the JMLSG Guidance Notes. Although SYSC 6.1.1R/SYSC 3.2.6R requires firms to establish systems and controls to counter the risk that they will be used to further financial crime, the further rules and guidance in SYSC, strictly speaking, only deal with the risk of
money laundering. SYSC 3.2.7R formerly contained a description of “financial crime” to support the rule in SYSC 3.2.6R, but this was deleted when the new rules came into force. According to the FSA Glossary, “financial crime” is defined widely and encompasses any kind of criminal conduct relating to money or to financial services or markets. “Money laundering”, on the other hand, relates only to the offences in POCA and the money laundering offence in Section 18 of the Terrorism Act.

The result is that the bulk of the rules and guidance in SYSC deal only with money laundering. By contrast, the JMLSG Guidance Notes deal with terrorist financing, an approach made explicit in both the 2006 and 2007 editions, both of which are entitled “Prevention of money laundering/Combating the financing of terrorism – Guidance Notes for the UK Financial Sector”. The Third Money Laundering Directive also covers terrorist financing as well as money laundering. The difference is, however, unlikely to be important in practice, given that the general obligation in SYSC 6.1.1R/SYSC 3.2.6R requires that a firm’s systems and controls counter the risk that a firm is used to further financial crime, which would include terrorist financing.

2.2.5 SYSC 6.3.3R/SYSC 3.2.6CR – Regular assessment

This rule requires a firm to carry out regular assessments of the adequacy of its systems and controls to ensure continued compliance with SYSC 6.3.1R/SYSC 3.2.6AR. This requirement is similar to the recommendation that firms monitor the effective operation of their controls set out in the JMLSG Guidance Notes.

2.2.6 SYSC 6.3.4G/SYSC 3.2.6DG – Other legal obligations

This guidance states that a firm may have separate obligations to comply with relevant legal requirements, including the Terrorism Act, POCA and the Money Laundering Regulations. It also states that the new rules and guidance in SYSC are not relevant guidance for the purposes of Section 330(8) POCA, Section 21A(6) of the Terrorism Act or regulation 3(3) of the 2003 Regulations, which has been replaced by the equivalent regulation 42(3) of the 2007 Regulations.

This repeats the guidance which was previously set out in the ML Sourcebook and maintains the relationship between the FSA rules and guidance and the JMLSG Guidance Notes. The JMLSG Guidance Notes are “relevant guidance”, having been approved by HM Treasury in relation to this primary and secondary legislation.

2.2.7 SYSC 6.3.5G/SYSC 3.2.6EG – Relationship with the Guidance Notes

SYSC 6.3.5G/SYSC 3.2.6E states that, when considering whether a firm has breached the FSA’s rules on systems and controls in relation to money laundering, the FSA will have regard to whether the firm has followed the JMLSG Guidance Notes.

This guidance restates the FSA’s policy as previously set out in the ML Sourcebook. However, the deletion of the ML Sourcebook has lent even greater weight to the JMLSG Guidance Notes since the level of specific requirements imposed by the FSA itself has reduced dramatically.
2.2.8 SYSC 6.3.6G/SYSC 3.2.6FG – Identifying money laundering risk

This guidance recommends that, in identifying money laundering risk and in establishing the nature of the systems and controls required, a firm should consider a range of factors, including:

(a) its customer, product and activity profiles;
(b) its distribution channels;
(c) the complexity and volume of its transactions;
(d) its processes and systems; and
(e) its operating environment.

This guidance provides slightly more detail to support the requirement in SYSC 6.3.1R/SYSC 3.2.6AR to identify money laundering risk. Although the guidance remains high level, the JMLSG Guidance Notes cover the topic in more detail[141]. However, neither the FSA rules and guidance nor the JMLSG Guidance Notes explain what is meant by the "operating environment". In the absence of further explanation from the FSA, firms may choose to define this term widely, bearing in mind that in the Prudential Sourcebook for Insurers, a similar expression – “business operating environment” – is described as including “political, legal, socio-demographic, technological and economic factors as well as the competitive environment and market structure”[142].

2.2.9 SYSC 6.3.7G/SYSC 3.2.6GG – Nature of systems and controls

The guidance in SYSC 6.3.7G/SYSC 3.2.6GG covers five different components of the required systems and controls.

> A firm should ensure that the systems and controls include appropriate training for that firm’s employees in relation to money laundering.

This single sentence effectively replaces all of the detailed rules previously set out in the ML Sourcebook in respect of training. It is more broadly targeted than the wording was in the ML Sourcebook and is aligned more closely with statutory requirements. For example, the ML Sourcebook referred to awareness and training specifically for staff who handle, or who are managerially responsible for, transactions which may involve money laundering, whereas the offence of failing to report in Section 330 of POCA applies to all persons who come into contact with relevant information in the course of their business in the regulated sector, and makes no reference to whether or not these staff handle or are managerially responsible for such transactions. Given that a person who fails to report has a defence if he has not been provided with training by his employer[143], the deletion of the reference to training for particular staff helps to avoid the risk of a mismatch between the FSA Rules and legislation.
The JMLSG Guidance Notes deal with staff awareness, training and alertness, providing additional detail on this topic. Some of the wording in the JMLSG Guidance Notes repeats verbatim certain provisions which were previously in the ML Sourcebook, demonstrating that the training and awareness regime has not changed in substance under the new rules and guidance.

> A firm should ensure that the systems and controls include appropriate provision of information to that firm’s governing body and senior management, including a report at least annually by that firm’s MLRO on the operation and effectiveness of those systems and controls.

This guidance aims to ensure that senior management are given adequate information in order to perform their function in line with the FSA’s increased focus on senior management responsibility. The content of the MLRO’s annual report is briefly elaborated in the JMLSG Guidance Notes.

> A firm should ensure that the systems and controls include appropriate documentation of its risk management policies and risk profile in relation to money laundering, including documentation of its application of those policies (SYSC 9/SYSC 3.2.20R to SYSC 3.2.22G).

This guidance clearly demonstrates the FSA’s risk-based approach to money laundering. The terms “risk management policy” and “risk profile” are not defined in this context.

Guidance refers to the high-level record-keeping requirements in SYSC 9/SYSC 3.2. According to these requirements, a firm must take reasonable care to make and retain adequate records of matters and dealings (including accounting records) which are the subject of requirements and standards under the regulatory system. In general, and subject to other Handbook requirements, all records must be capable of being reproduced in English on paper. However, if a firm’s records relate to business carried on from an establishment in a country or territory outside the UK, an official language of that country or territory may be used instead of English.

Furthermore, guidance in SYSC 9/SYSC 3.2 indicates that a firm should have appropriate systems and controls in place to fulfil its regulatory and statutory obligations with respect to the adequacy of the records, access to such records, the periods of retention for the records and their security. The general principle is that records should be kept for as long as is relevant for the purposes for which they were made. The guidance also refers to the detailed record-keeping requirements for different types of firm, which are located in Schedule 1 to each module of the Handbook.

> A firm should ensure that the systems and controls include appropriate measures to ensure that money laundering risk is taken into account in its day-to-day operation, including in relation to:
(a) the development of new products;
(b) the taking on of new customers; and
(c) changes in its business profile.

This guidance elaborates the requirement in SYSC 6.3.1R/SYSC 3.2.6AR to identify money laundering risk by ensuring that it is considered on a day-to-day basis.

> A firm should ensure that the systems and controls include appropriate measures to ensure that procedures for identification of new customers do not unreasonably deny access to its services to potential customers who cannot reasonably be expected to produce detailed evidence of identity.

This guidance effectively replaces the much more detailed guidance in relation to financial exclusion previously contained in the ML Sourcebook.

Although the FSA included dealing with financial exclusion as part of the wider initiative of “defusing the ID issue” – the drive launched in 2004 to reduce unnecessary documentation required to verify customers’ identities in the context of money laundering – it appears that the requirements have not changed substantially. The deletion of the ML Sourcebook places greater emphasis on the JMLSG Guidance Notes, which detail alternative identification procedures for individuals without access to the normal documentation required.

### 2.2.10 SYSC 6.3.8R/SYSC 3.2.6HR – Senior management responsibility

This rule requires a firm to allocate to a director or senior manager the overall responsibility within the firm for the establishment and maintenance of effective anti-money laundering systems and controls.

Previously, the MLRO was the sole individual required by the rules to take particular responsibility within the firm for money laundering policy and procedures. Under the revised rules, as part of the FSA’s aim of making senior management more accountable, a director or senior manager must be responsible for the firm’s approach to money laundering. Following criticism of the original proposal during the consultation process, the rule now states that a firm’s MLRO can also be its director or senior manager responsible for oversight of money laundering systems and controls.

### 2.2.11 SYSC 6.3.9R/SYSC 3.2.6I – The Money Laundering Reporting Officer

This rule requires a firm to appoint an MLRO with responsibility for the oversight of its compliance with the FSA’s rules on systems and controls against money laundering. The firm also has to ensure that its MLRO has a level of authority and independence within the firm and access to resources and information sufficient to enable him to carry out that responsibility.
This guidance replicates the previous rules in the ML Sourcebook.

In a recent review of anti-money laundering systems and controls in the private banking sector, the FSA noted that, in most private banks, the MLRO was also head of compliance and that, as a result, the MLRO had regular and direct access to senior management and in many cases reported directly to the CEO.\footnote{151}

2.2.12 SYSC 6.3.10G/SYSC 3.2.6JG – The role of the Money Laundering Reporting Officer

This guidance aims to explain the nature of the MLRO’s role, stating that his job is to act as “the focal point for all activity in the firm relating to money laundering”. It adds that it is expected that a firm’s MLRO will be based in the UK.

The description of the MLRO highlights a possible confusion over the nature of his role in relation to the role of the director or senior manager responsible for money laundering. In the ML Sourcebook, the MLRO was “the key person” in the “implementation of anti-money laundering strategies and policies”\footnote{152}. Despite the creation of a director or senior manager responsible for money laundering, the nature of the MLRO’s role has been rephrased but not substantially redefined in the new guidance.

Chapter 3 of the JMLSG Guidance Notes deals extensively with the role and duties of the MLRO, and although it does not provide specific guidance on the nature of the relationship between the MLRO and the director responsible for anti-money laundering, paragraph 3.11 in the 2007 edition contains the following statement:

“the relationship between the MLRO and the director(s)/senior manager(s) allocated overall responsibility for the establishment and maintenance of the firm’s AML/CTF [anti-money laundering combating terrorist financing] systems is one of the keys to a successful AML/CTF. It is important that this relationship is clearly defined and documented, so that each knows the extent of his, and other’s, role and day-to-day responsibilities.”

2.3 Conclusion

The replacement of the detailed ML Sourcebook with the limited number of relatively high-level provisions now contained in SYSC, and the accompanying move towards a much closer relationship between the FSA’s own requirements and the detailed guidance set out in the JMLSG Guidance Notes, represents a significant change in the approach of the FSA to the way in which it seeks to discharge its statutory objective in relation to financial crime. The change is a welcome one, removing a layer of complexity in an area where a perceived need for the authorities to improve their rates of prevention and detection has arguably led to an unhelpful proliferation of regulation, burdensome for financial institutions without necessarily assisting in the achievement of its objectives.
This is not to say, however, that the changes noted above reflect any lessening of the FSA’s resolve in this area. All of the commentary from the FSA in relation to the changes has explained that the risk-based approach, with its focus on the achievement of outcomes rather than prescriptive processes and on the responsibility of senior management for identifying and combating the particular money laundering rules which their businesses face, is not to be considered as a lightening of the regulatory touch. Recent commentary has identified financial crime, including money laundering, as one of the major threats to confidence in the UK markets and has emphasised the importance, for the purposes of market stability, of ensuring that the markets are seen to be clean and transparent. There is a continuing focus on working with the industry, with overseas regulators and with academics in order to improve understanding of the methodologies of money launderers and thus to use the available resources effectively to defeat them.

Against this background, it is clear that firms in the regulated sector must expect to continue to devote significant financial and managerial resources to ensuring that they both implement and observe the procedures, and also the culture, necessary to ensure compliance in this area.
Including credit institutions; investment firms; long-term insurers and their intermediaries; collective investment undertakings; auditors, insolvency practitioners, accountants and tax advisers; many (but not all) lawyers; trust or company service providers; estate agents; dealers in high value goods; and casino operators.

When a fine is imposed upon conviction for any offence under POCA or the Terrorism Act, the level of the fine is determined by the court, taking into account the seriousness of the offence and the financial circumstances of the offender.

Article 3, SI 2003/120.

Subsection 340(3)(a), POCA.

Subsection 340(2), POCA.

Subsection 340(6), POCA.

Subsection 340(3)(b), POCA.

The disclosure obligations under POCA relate to all persons of whom an individual or firm has knowledge or suspicion of involvement in money laundering.

Subsection 340(3)(b), POCA.

Subsections 327(2A), 328(3), 329(2A), POCA.

But not for the Section 330 failure to disclose offence.

Subsections 327(2C), 328(5), 329(2C) and 339A, POCA.

Under Section 338, POCA.

Subsection 335(5), POCA.

Subsection 335(2)-(3), POCA.

Subsection 335(6), POCA.

Section 340(11), POCA.


Sections 517 and 519, Companies Act 2006.

Subsection 338(3), POCA.

The terms credit institution and financial institution are defined in subsection 333E(2) by reference to the regulated sector as described in Schedule 9 to POCA.

Subsection 333E(2), POCA.

Section 333C, POCA.

Subsection 333D(2), POCA.

2005 EWHC 664 (ch).

2006 EWCA Civ 1039.


Subsections 1(1) and (2), Terrorism Act, as amended by Section 34, Terrorism Act 2006.

Section 75, Counter-Terrorism Act 2008.

Subsection 1(4), Terrorism Act.

Section 14, Terrorism Act.

Regulation 21, 2007 Regulations.

Subsection 21(1), Terrorism Act.

Section 21C, Terrorism Act.

By SI 2007/3398.

Subsections 21(2) to (4) and 21ZB(3), Terrorism Act.

Though not for the offence under Section 15(1) of inviting another person to provide money or other property and intending, or having reasonable cause to suspect, that it may be used for the purposes of terrorism.

Subsection 21(5) and Section 21ZC, Terrorism Act.

Subsections 21Z(2) to (4), Terrorism Act.

Defined in Schedule 3A to the Terrorism Act, but equivalent to the regulated sector for POCA purposes as defined in Schedule 9 of

POCA.

Subsection 21A(11), Terrorism Act.

At paragraphs 6.13-6.15 of Part I.

Subsection 21A(5)(a), Terrorism Act.

By SI 2007/3398.

At Sections 21E to 21H, Terrorism Act.

Subsection 39(5)(a), Terrorism Act.

Subsection 39(5)(b), Terrorism Act.


The Wire Transfer Regulation does not apply, for example, to certain transfers of funds that represent a low risk of money laundering or terrorist financing. This includes, provided certain conditions are satisfied, transfers using debit or credit cards.

Paragraphs 5.2.12 and 5.2.13 of Part I.

SI 2007/3298.

Regulation 14, Transfer Regulations.

The Serious Fraud Office, for instance, has had extensive investigatory powers since 1988: under Section 2 Criminal Justice Act 1987, on its own initiative (i.e. without involving the courts) the SFO has been able to order any person to answer questions, furnish information or produce documents with respect to any matter relevant to the investigation of a serious or complex fraud. The FSA also has extensive powers to compel persons to answer questions, disclose information and produce documents in pursuance of their statutory functions. The Government has confirmed that it intends to grant the FSA additional powers to grant immunity from prosecution to individuals who are prepared to provide evidence of serious misconduct to the regulator; it remains to be seen how the FSA will make use of this power if granted but it certainly raises some potentially rather difficult questions of policy for FSA-authorised firms, and of liability for those firms, for the individuals concerned and even for the FSA.

The ATCSA introduced the account monitoring order into the Terrorism Act in December 2001; prior to that, the Terrorism Act made provision for customer information orders to be made, though on a slightly more restricted basis (Section 38A and Schedule 6A, Terrorism Act, introduced by Schedule 2, Part 1, ATCSA).

Paragraph 2(1), Schedule 6A, Terrorism Act.

Sections 370 to 375, POCA.

Section 371, POCA.

Section 38 and Schedule 6, Terrorism Act, as amended by Schedule 2, Part 4, ATCSA.
Sections 363 to 369, POCA.

Paragraph 5, Schedule 6, Terrorism Act.

Section 365, POCA.

Sub-paragraphs 1(3) and 1(5) of Schedule 6, Terrorism Act and subsections 366(1) and (2), POCA.

Subsections 366(3) and (4), POCA.

Section 23 and Schedule 4, Terrorism Act.

Paragraph 5, Schedule 4, Terrorism Act, introduced by Section 3 and Schedule 2, ATCSA.

Section 358, POCA.

Paragraph 5, Part 1, Schedule 4, Terrorism Act and subsection 40(2), POCA.

Sections 34-38, CTA.

Section 23, Terrorism Act as substituted by Section 34 of the CTA once brought into force.

Subsection 23(7), Terrorism Act, as substituted by Section 34 of the CTA once brought into force.

Section 6, POCA.

Schedule 2 of POCA contains a full list of offences, conviction for which will be conclusive evidence of a criminal lifestyle.

Subsection 75(4), POCA.

Section 243, POCA.

Section 246, POCA.

Subsections 246(4) to (6), POCA.

Section 27A, Limitation Act 1980, inserted by subsection 288(1), POCA.

Sections 304 to 310, POCA.

Subsection 317(1)(b), POCA.


HM Treasury has powers under the United Nations Act 1946 to implement resolutions of the United Nations Sanctions Committee by statutory instrument. The Treasury’s Asset Freezing Unit is responsible for implementing sanctions orders and provides firms with a consolidated list of all subjects of sanctions currently in force.

For further information on the EU sanctions regime, see http://ec.europa.eu/external_relations/cfsp/sanctions/.

SI 2006/2952.

Other key sanctions orders are (i) the Terrorism (United Nations Measures) Order 2001, SI 2001/3365; (ii) the Al-Qa’ida and Taliban (United Nations Measures) Order 2002, SI 2002/111; (iii) the Terrorism (United Nations Measures) Order 2006, SI 2006/2657.

Articles 7 and 8, the Al-Qa’ida Order.

Article 10, the Al-Qa’ida Order.

Schedule 1, the Al-Qa’ida Order.

Section 4 and Schedule 3, ATCSA.

Subsection 4(2), ATCSA.

The Landsbanki Freezing Order 2008 (SI 2008/2668) and subsequent licences made thereunder.

Section 9, Landsbanki Freezing Order 2008.

Paragraph 3, Schedule 7 of the CTA.

Paragraph 9(1), Schedule 7 of the CTA.

Paragraph 9(2), Schedule 7 of the CTA.

Under Section 63, CTA.

Section 63, CTA.

Section 2(2)(d), FSMA. The other three regulatory objectives are: maintaining confidence in the financial system; promoting public understanding of the financial system; and securing the appropriate degree of protection for consumers.

Section 6(2), FSMA.

The FSA’s jurisdiction, and thus the application of its anti-money laundering requirements, was extended with effect from October 2004 to cover mortgage lenders and brokers and, with effect from January 2005, to cover general insurance brokers.

The Securities and Futures Authority, the Investment Management Regulatory Organisation and the Personal Investment Authority.

Section 146, FSMA.

CP 46.

Although it has in fact subsequently taken on a prosecutorial role in relation to breaches of the Regulations by financial sector firms.

PRIN 2.1.1R, Principle 3.

SYSC 3.1.1R.

SYSC 3.2.6R (but see also SYSC 6.1.1R, discussed at 6.2.2 below).

APER 2.1.29.

APER 3 and 4.

Section 66, FSMA.

CP 05/10, paragraph 1.12.

CP 05/10, chapter 2.

Speech by Sir Callum McCarthy at the FSA Financial Crime Conference on 15 November 2005.


Speech by John Tiner at the FSA’s conference on more principles based regulation on 23 April 2007.

Policy Statement 06/1, paragraph 2.7.


Speech by Philip Robinson at the FSA’s Financial Crime Conference on 15 November 2005.

Directive 2002/83/EC.

SYSC 1.1.3 A until 31 March 2009, then SYSC Annex 1.

A firm to which the Markets in Financial Instruments Directive (“MiFID”) applies.

CP 46, paragraph 4.10.

Regulation 3(3)(b) and 3(3)(c), 2007 Regulations.

SYSC 1.2.1G.


JMLSG Guidance Notes 2007 edition, Chapter 4, paragraph 4.2.


INSPRU 5.1.14G(4).

Section 330(7)(b), POCA.

IMPORTANT NOTE: This memorandum is intended as an introductory guide to the UK’s anti-money laundering regime. It should not be relied upon as a substitute for legal advice.

If you have specific questions relating to anti-money laundering please contact your usual adviser at Slaughter and May or speak directly to Ruth Fox or Ben Kingsley in Slaughter and May’s Financial Regulation Group on +44 (0) 20 7600 1200.
CONTACT ADDRESSES

London
One Bunhill Row
London EC1Y 8YY
United Kingdom
T +44 (0)20 7600 1200
F +44 (0)20 7090 5000

Paris
130 rue du Faubourg Saint-Honoré
75008 Paris
France
T +33 (0)1 44 05 60 00
F +33 (0)1 44 05 60 60

Brussels
Square de Meeûs 40
1000 Brussels
Belgium
T +32 (0)2 737 94 00
F +32 (0)2 737 94 01

Hong Kong
47th Floor
Jardine House
One Connaught Place
Central
Hong Kong
T +852 2521 0551
F +852 2845 2125

www.slaughterandmay.com