CHAPTER 2

UK Part II: UK law and practice

Arun Srivastava
Paul Hastings (Europe) LLP

INTRODUCTION

2.1 This chapter considers money laundering law and practice in the UK. The emphasis is on the legal and regulatory framework rather than practice, which is covered in detail in Chapter 3. This chapter does not consider confiscation and forfeiture in the UK, which are covered in Chapter 4.

2.2 The UK consists of England, Wales, Scotland and Northern Ireland. The Channel Islands (including Jersey and Guernsey) and the Isle of Man are not part of the UK and have their own legislature and courts. The anti-money laundering frameworks in these jurisdictions and certain of the UK's Overseas Territories,[1] are covered in dedicated chapters later in this book.

2.3 The UK has for many years recognised the effectiveness of anti-money laundering legislation as a tool against drug trafficking and terrorist

1 Bermuda, the British Virgin Islands and Cayman Islands.

financing. The Drug Trafficking Offences Act 1986 was the first UK legislation to specifically criminalise money laundering. The Prevention of Terrorism (Temporary Provisions) Act 1989 specifically addressed terrorist financing. Recent years have seen a rapid development in the UK's anti-money laundering and terrorist financing framework. The current UK anti-money laundering (AML) and counter-terrorism financing (CTF) framework has, of course, been shaped to a large extent by the four European Money Laundering Directives,[2] which have in turn sought to implement the recommendations made by the Financial Action Task Force (FATF). A Fifth Money Laundering Directive[3] is now in force but has not yet been transposed. The Fifth Money Laundering Directive will result in changes to the UK's money laundering framework to bring certain FinTech-related activities (operators providing exchange services between virtual and fiat currencies and custodian wallet providers) within the scope of money laundering regulation. It will also make additional provision in relation to the performance of enhanced due diligence measures.

2.4 The Abacha case marked a watershed in the approach to money laundering compliance in the UK. General Sani Abacha was alleged to have laundered US$1.3 billion through accounts held with banks in London. The UK Financial Services Authority (the FSA) carried out an investigation into this matter which focused on the AML controls at 23 banks in the UK where accounts linked to Abacha family members and close associates were identified. The investigation found that 15 of the banks had significant control weaknesses. The Abacha case drew attention to the fact that UK financial institutions were vulnerable to money laundering. It also reminded institutions that they were exposed to the possibility of regulatory and law enforcement action. The terrorist attacks on the United States on 11 September 2001 reinforced the focus on AML and CTF compliance measures. More recently the issues highlighted through the Panama Papers have focused attention on tax evasion and the use of offshore centres to facilitate money laundering.

2.5 It is against this backdrop that in April 2016 the Home Office and HM Treasury jointly published an Action Plan for Anti-Money Laundering and Counter-Terrorist Finance (the Action Plan). The Action Plan set out a broad range of proposals for the overhaul of the UK's AML and CTF framework. The Action Plan proposed changes to UK laws which were subsequently implemented through the Criminal Finances Act 2017. These included changes to the consent regime in the UK and the introduction of powers to obtain unexplained wealth orders intended to facilitate and expedite the recovery of assets without, for example, needing to rely on a conviction for a predicate offence in an overseas jurisdiction or assistance from other jurisdictions which might be reluctant or unable to assist a UK investigation. These powers were used for the first time in late 2018 against Samira Hajiyeva, the wife of the former Chairman of the

2 Directives 91/308/EEC, 2001/97/EC, 2005/60/EC and Directive 2015/849/EU.
3 Directive 2018/843.

International Bankan Azeri state-bank, who famously spent £16 million in Harrods.

2.6 The Action Plan was framed in anticipation of the Mutual Evaluation Report carried out by FATF on the UK which reported back in December 2018. While finding that 'the UK aggressively pursues money laundering and terrorist financing investigations and prosecutions, achieving 1400 convictions each year for money laundering. UK law enforcement authorities have powerful tools to obtain beneficial ownership and other information, including through effective public-private partnerships, and make good use of this information in their investigations', FATF also observed that the UK needed to increase the resources available to its Financial Intelligence Unit, the National Crime Agency (NCA), reform its suspicious activity reporting regime and ensure consistency of supervision for money laundering compliance across all of the regulated sectors.

2.7 Billions of pounds are laundered through the UK each year. The UK Government's National Risk Assessment of Money Laundering and Terrorist Financing 2017 (the National Risk Assessment) found that high end money laundering is one of the greatest risks in the UK. It is estimated that £10 billion a year is laundered through the regulated sector alone, and that £3 billion of criminal profits is moved out of the UK annually. In addition to the laundering process, organised crime is believed to be involved in 'criminal capital formation' in much the same way as legitimate businesses. Assets of this nature are estimated to be in the region of £5 billion in seizable form. The overall cost to the UK from organised crime is estimated as being between £20 billion to £40 billion annually.

2.8 The National Risk Assessment key findings included the following:

- high-end money laundering and cash-based money laundering remain the greatest areas of money laundering risk. New typologies continue to emerge, including risks of money laundering through capital markets and increasing exploitation of technology;
- law enforcement agencies see criminal funds progressing from lower level laundering before accumulating into larger sums to be sent overseas through more sophisticated methods, including retail banking and money transmission services;
- professional services are a crucial gateway for criminals looking to disguise the origin of their funds;
- cash, alongside cash intensive sectors, remain the favoured method for terrorists to move funds through and out of the UK. The UK's terrorist financing threat largely involves low levels of funds being raised by UK individuals to send overseas, fund travel or fund attack planning. The primary means of doing this are through cash, retail banking or money service businesses.

2.9 The developments in the AML and CTF framework form part of a broader thrust to combat organised crime. The AML framework provides governments with a tool to combat other types of criminal activity. Accordingly, FATF has been asked by the G20 to '… help detect and deter the proceeds of corruption by prioritising work to strengthen standards on customer due diligence, beneficial ownership and transparency'.

OVERVIEW AND THE FUTURE

2.10 The UK's money laundering legislation originally developed in a piecemeal way. The primary offences of money laundering were found in various different statutes and there were inconsistencies between the various offences. The Criminal Justice Act 1988[4] set out the UK's primary anti-money laundering offences.[5] However, it applied only to the proceeds of indictable offences and did not apply to the proceeds of drugs trafficking or to terrorist funds. The proceeds of drug trafficking were instead dealt with by the Drug Trafficking Act 1994, and terrorist financing by the Prevention of Terrorism (Temporary Provisions) Act 1989 and the Northern Ireland (Emergency Provisions) Act 1996. The scope of the offences and obligations under these statutes varied in material respects. This fragmented structure was replaced by the Proceeds of Crime Act 2002 (POCA 2002) and the Terrorism Act 2000 (TA 2000). Both of these Acts have themselves been the subject of amendment, in particular through the Serious Organised Crime and Police Act 2005, the Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007[6] and the Criminal Finances Act 2017.[7]

2.11 POCA 2002 came into force in February 2003 and created a single set of money laundering offences applicable to the proceeds of all crimes (thus doing away with the distinctions between drugs and non-drugs proceeds and indictable and summary offences). In addition, it introduced a new offence of failure of the regulated sector to report suspicions of money laundering relating to any crime (not just drugs and terrorism). These changes were set in train by the Cabinet Office Performance and Innovation Unit Report (PIU Report) published in June 2000, which raised the political importance of the fight against money laundering. The PIU Report concluded that although the UK regime at that time led to an annual average of 15,000 suspicious activity reports, the number of prosecutions for money laundering was in fact very low. The PIU Report recommended the consolidation and simplification of UK money laundering offences. The TA 2000 entered into force in the UK in February 2001. Provisions

4 As amended by the Criminal Justice Act 1993.

5 The Criminal Law (Consolidation) (Scotland) Act 1995 contained provisions relating to Scotland and the Proceeds of Crime (Northern Ireland) Order 1996 contained provisions relating to Northern Ireland.

6 SI 2007/3398.

7 The Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007 implemented in part the EU's Third Money Laundering Directive (2005/60/EC), to bring POCA 2002 and the TA 2000 in line with Chapter 3 of that Directive.

directed against terrorist financing are contained in Part III of that Act. The AML and CTF framework set out in POCA 2002 and TA 2000 is underpinned by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017[8] (the MLR 2017), which give effect to the EU's Fourth Money Laundering Directive in the UK. POCA 2002 and the TA 2000 establish the substantive criminal law offences of money laundering and terrorist financing, whereas the MLR 2017 impose requirements on firms operating in certain regulated sectors, establish and maintain policies, controls and procedures to mitigate and manage risks of money laundering and terrorist financing.

2.12 The MLR 2017 apply to certain categories of persons acting in the course of certain regulated businesses carried on by them in the UK. The categories of persons covered are specified in reg 8 of the MLR 2017[9] and such persons are defined as 'relevant persons'.

2.13 As considered in further detail below, the MLR 2017 impose various risk-sensitive AML and CTF compliance regulations on relevant persons, which include customer due diligence, monitoring, reporting and record keeping obligations. The MLR 2017 contain a specific requirement under reg 18 for relevant persons to perform a risk assessment taking into account risk factors relating to: (i) their customers; (ii) the countries or geographic areas in which they operate; (iii) their products or services; (iv) their transactions; and (v) their delivery channels.

2.14 Under the MLR 2017, reg 7, various bodies are appointed as Supervisory Authorities for the purpose of monitoring and securing compliance by relevant persons with the requirements of the MLR 2017.

2.15 The Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) are regulators of the UK banking, insurance and financial services industries. The PRA and FCA assumed responsibilities for these industries with effect from 1 April 2013 and replaced the Financial Services Authority, the former statutory regulator. The changes to the UK's regulatory architecture introduce a 'twin peaks' approach. Certain firms will be dual-regulated, so that for prudential purposes they will be regulated by the PRA and for conduct purposes they will be regulated by the FCA. Broadly, such dual-regulated firms will be made up of banks, insurers and larger investment firms. Other regulated firms will be regulated for both prudential and conduct purposes by the FCA. In performing its general functions under the Financial Services and Markets Act 2000 (FSMA 2000) the FCA must so far as reasonably possible act in a way which advances one or more of its operational objections. These include the 'integrity objective', which is an objective of protecting and enhancing the integrity of the UK financial system. Integrity for these purposes includes the requirement that the financial system is not being used for a purpose connected

8 SI 2017/692.

9 Under reg 8 'relevant persons' are: credit institutions, financial institutions, auditors, insolvency practitioners, external accountants, tax advisers, independent legal professionals, trust or company service providers, estate agents, high value dealers and casinos.

with financial crime. Financial crime is defined as including the handling of the proceeds of crime. In addition to this, the FCA is required to have regard to the importance of taking action intended to minimise the extent to which it is possible for regulated firms and businesses to be used for a purpose connected with financial crime. Under the Memorandum of Agreement between the FCA and PRA, the PRA is required to inform the FCA of any evidence which it believes may materially affect the FCA's function in relation to financial crime.

2.16 The FCA is a Supervisory Authority under the MLR 2017, reg 7(1)(a) for a range of businesses as specified in reg 7(1)(a)(i)–(vii). Broadly, these are banking and financial services businesses for which the FCA is the statutory regulator. Under the MLR 2017, reg 76 a 'designated supervisory authority' has the power to impose a penalty on persons who fail to comply with certain of the requirements under the MLR 2017. The FCA has been designated for these purposes. The FCA has also become the supervisory authority for credit and financial institutions under the Counter-Terrorism Act 2008, Sch 7. This means that the FCA is responsible for monitoring institutions for their compliance with directions made under Sch 7 to that Act.

2.17 The Gambling Commission is the Supervisory Authority for casinos, and the Commissioners for Her Majesty's Revenue and Customs (HMRC) is the Supervisory Authority for the businesses specified in reg 7(1)(c)(i)–(vii). Broadly, these are high value goods dealers and various other businesses such as estate agency businesses and trust or company service providers who are not regulated by the FCA or a professional body. Various professional bodies are specified in the MLR 2017, Sch 1 as the Supervisory Authorities for professional services firms who are relevant persons under the MLR 2017. These are principally lawyers, accountants and tax advisers. The Office for Professional Body Anti-Money Laundering Supervision (OPBAS) is a new regulator set up by the government to strengthen the UK's AML supervisory regime and ensure the professional body AML supervisors (listed in the MLR 2017, Sch 1) provide consistently high standards of AML supervision. OPBAS was set up pursuant to The Oversight of Professional Body Anti-Money Laundering and Counter Terrorist Financing Supervision Regulations 2017.[10] The role of the OPBAS is performed by the FCA, which has also issued an OPBAS Sourcebook to inform professional body supervisors as to how they might meet their obligations in relation to AML supervision. OPBAS does not supervise the Gambling Commission or the HMRC. Instead, its role is limited to improving consistency of professional body supervision in the accounting and legal sectors.

2.18 POCA 2002, the TA 2000 and the MLR 2017 enable HM Treasury to approve guidance issued by a supervisory or other relevant body in relation to compliance with AML and CTF legal requirements. The most long-standing approved guidance is that issued by the Joint Money Laundering Steering Group (JMLSG), which is directed at the financial sector. The JMLSG's Guidance

10 SI 2017/1301.

(the Guidance) was originally published in 1990 and has been amended on a number of occasions since. Guidance issued by the Consultative Committee of Accounting Bodies, HMRC and the Legal Sector Affinity Group, amongst others, has also been approved by HM Treasury.

2.19 Under POCA 2002, s 330(8), in determining whether an offence of failure to disclose suspicions of money laundering has been committed, the court must have regard to guidance issued by a supervisory or other relevant body that has been approved by HM Treasury. Similar to the position under POCA 2002, under the MLR 2017, regs 76(6)(b) and 86(2)(b) respectively, regard will be had to guidance issued by the FCA or issued by another Supervisory Authority and approved by HM Treasury in determining whether to impose a civil or criminal penalty for breaches of the MLR 2017.

2.20 The NCA acts as the UK's financial intelligence unit (FIU). Each EU Member State is required to establish an FIU to combat money laundering and terrorist financing. A function of the FIU (and accordingly the NCA) is to manage disclosures of information which concern potential money laundering or terrorist financing. The NCA was established in December 2013 pursuant to reforms introduced by the Crime and Courts Act 2013. It replaced the Serious Organised Crime Agency. The NCA has a Consent Team which manages suspicious activity reports made to it which seek a consent to act under POCA 2002.

2.21 FATF undertakes a mutual evaluation process, which is intended to monitor the implementation of FATF's Recommendations and assess the effectiveness of AML and CTF systems in FATF member jurisdictions including the UK.

2.22 FATF carried out an onsite visit to the UK in March 2018 and published its Mutual Evaluation Report on the UK in December 2018. This found that the UK had significantly strengthened its AML/CFT framework since its last evaluation, particularly in relation to operational co-ordination among law enforcement agencies, stronger investigative tools, mechanisms to facilitate public/private information sharing, and the creation of an authority to address inconsistencies in the supervision of lawyers and accountants (the OPBAS referred to above). FATF identified certain areas for improvement, including the resourcing of the UK's FIU, the supervision of the regulated sector and the reporting and investigation of suspicious transactions.

2.23 Also at an international level, the Organisation for Economic Co-operation and Development (the OECD) has emphasised the need for tax haven jurisdictions to facilitate the exchange of information with tax authorities and to remove impediments to cooperation, such as bank secrecy laws. The OECD's work in this area may have implications for the UK's Crown Dependencies and Overseas Territories, which are legally separate jurisdictions from the UK. In April 2009, the OECD published a Progress Report on the Implementation of the Internationally Agreed Tax Standards. This Progress Report listed various offshore jurisdictions (including certain of the UK's Overseas Territories) as having failed to substantially implement the internationally agreed standards. Progress in

this area has been rapid in recent times and a number of such jurisdictions have since taken steps to ensure they are treated as having substantially implemented the international tax standards. All jurisdictions surveyed by the OECD Global Forum have now committed to implementing the international standards for exchange of information in tax matters. The focus on these issues has also impacted on the work of FATF, one of whose priorities is a review of financial institution secrecy laws and the cross border exchange of information. FATF will in particular consider the cross border exchange of information within financial services groups and between regulators.

PROCEEDS OF CRIME ACT 2002

2.24 The principal UK criminal offences of money laundering are contained in POCA 2002. This is a lengthy Act and the money laundering offences are to be found in Pt VII (POCA 2002, ss 327–340). The intention of POCA 2002 was to consolidate the fragmented legislative structure referred to above and to reform the offences relating to money laundering on a UK-wide basis.

Corporate liability

2.25 The offences created by POCA 2002 may be committed by a person. The Interpretation Act 1978 defines 'person' to include 'a body of persons corporate or unincorporated' unless the contrary appears. Thus, the offences are capable of being committed by both natural persons and companies. Generally, a company can only be criminally liable if those who constitute its directing mind (for example, its directors) are proved to have the requisite involvement in the offence.[11] However, it is also recognised that the Board of Directors may delegate some part of their functions of management and that different persons may for different purposes satisfy the requirements of being a company's directing mind and will,[12] so that a delegate can be put in the place of the Board and act as the company. This may be relevant in the context of liability for money laundering offences, where the Board may have delegated relevant functions to a nominated officer for money laundering purposes. The trend in the UK, which has been evidenced by the Bribery Act 2010 and the Criminal Finances Act 2017, has been to impose corporate liability for the failure to prevent various financial crimes. The UK Government is currently consulting on the introduction of a 'composite' offence of failure to prevent economic crime.

The principal laundering offences and consent regime

2.26 POCA 2002 sets out three 'principal' money laundering offences, which are:

11 *Tesco Supermarkets Ltd v Nattrass* [1972] AC 153.
12 *El Ajou v Dollar Holdings* [1994] 2 All ER 685.

- concealing, disguising, converting or transferring criminal property (POCA 2002, s 327);
- becoming concerned in arrangements that facilitate the acquisition, retention, use or control of criminal property (POCA 2002, s 328); and
- acquiring, possessing or using criminal property (POCA 2002, s 329).

2.27 In order to avoid the commission of one of the above principal money laundering offences, a party may make a disclosure[13] of its knowledge or suspicion of money laundering and request a consent[14] to carry out an act that would otherwise constitute a principal money laundering offence. In practice such disclosures and requests for consent are made to NCA, although under POCA 2002, s 338 they may be made to any constable or customs officer. POCA 2002, s 335(5) and (6) set out a timetable within which NCA must respond to a request for consent. Section 335(5) establishes an initial period of seven working days in which NCA must respond if it intends to refuse consent to a particular transaction. If consent is refused in this period, under s 335(6) there is a further 31-day moratorium period in which no transactions may take place. NCA accordingly has up to 40 days to determine an application for consent, although it must keep a refusal of consent under review during the moratorium period[15] and, as explained below, this time period can be extended upon application to the Court. The purpose of the moratorium period is to provide an opportunity for the matters reported to NCA to be investigated. If during this moratorium period it appears that it is necessary to start a criminal investigation, an application may be made to the Crown Court for a restraint order under POCA 2002, s 41, prohibiting dealings with any realisable property of the alleged offender. The period of time for the moratorium under POCA 2002, s 335(6) can be extended by Court order for up to a total of 186 days where an investigation is being carried out into a disclosure and further time is needed to conduct that investigation. The process for such an application is set out in POCA 2002, s 336A. To grant such an order, the Court must be satisfied that the investigation is being conducted diligently and expeditiously, that further time is needed for conducting the investigation and that it is reasonable in all the circumstances for the moratorium period to be extended.

2.28 Together, the principal money laundering offences and the consent regime operate to exert pressure on third parties, such as banks, who develop suspicions of money laundering to disclose those suspicions and to seek a consent from NCA to carry out the suspect transaction.

2.29 The reporting regime under POCA 2002 is considered in more detail below at para 2.55.

13 Under POCA 2002, s 338.
14 Under POCA 2002, s 335.
15 *R (on the application of UMBS Online Ltd) v SOCA* [2007] EWCA Civ 406.

Criminal conduct and criminal property

2.30 The focus of POCA 2002's principal money laundering offences is on 'criminal property'. In order for one of the principal money laundering offences to be committed some act must be carried out in relation to criminal property. Under POCA 2002, s 340(3), criminal property is defined as property that constitutes a person's benefit from criminal conduct or that represents such a benefit in whole or in part. For property to constitute criminal property, a person must know or suspect that the property constitutes or represents such a benefit.

Criminal conduct

2.31 In order for criminal property to exist, there must be some underlying criminal conduct that gives rise to a benefit. Sometimes referred to as the predicate offence, criminal conduct is defined under POCA 2002, s 340(2) as conduct that constitutes an offence in any part of the UK or conduct which would constitute an offence in any part of the UK if it occurred there. The definition of criminal conduct therefore includes conduct committed abroad, provided that this would have resulted in the commission of an offence if carried on in the UK.

2.32 On a prosecution it is sufficient to prove the category of criminal conduct that has generated the alleged criminal property, if not the specific offence. In the case of *R v W*[16] the court found that on a prosecution for a breach of POCA 2002, ss 327 and 328, there had to be proof of at least the class of offence said to constitute the alleged underlying criminal conduct.

2.33 The definition of 'criminal conduct' applies a test of single criminality. Conduct – wherever it occurs – is judged against the requirements of UK criminal law. The place where the underlying criminal conduct is engaged in is irrelevant. Accordingly, a UK bank could commit an offence under POCA 2002 where it operates a customer's account which it suspects contains the proceeds of foreign corruption or foreign tax evasion. Likewise, a UK company could commit an offence under POCA 2002 where it facilitates the commission of a customs or tax offence in relation to the importation of goods into another jurisdiction or acquires the shares in a business that is carried on unlawfully in another jurisdiction.

Double criminality – overseas conduct

2.34 The effect of this broad definition of criminal conduct under POCA 2002, s 340(2) has, however, been limited by amendments to the POCA 2002 made by the Serious Organised Crime and Police Act 2005, s 102 and by the Proceeds of Crime Act 2002 (Money Laundering: Exceptions to Overseas Conduct Defence) Order 2006.[17] The purpose of these amendments was to address circumstances in

16 [2008] EWCA Crim 2.
17 SI 2006/1070.

which the underlying conduct is lawful in the jurisdiction in which it takes place, but would be unlawful if carried on in the UK. This issue is often illustrated by reference to the position of the Spanish bullfighter, whose income would be treated as criminal property under POCA, even though his occupation was perfectly legal in Spain. The effect of the amendment is to introduce a double criminality defence in certain limited circumstances. In other words, in some cases the fact that conduct was not unlawful in the jurisdiction in which it occurred will be a relevant consideration in determining whether a money laundering offence has been committed under POCA 2002.

2.35 Under the amendments introduced by the Serious Organised Crime and Police Act 2005, it is a defence, in certain circumstances, for an alleged offender to establish that the conduct engaged in was not unlawful under the criminal law of the country in which it occurred. In order to make out this defence the alleged offender must show:

- that he knew or believed on reasonable grounds that the relevant criminal conduct occurred outside the UK; and
- that the conduct was not at the relevant time unlawful in the jurisdiction in which it in fact occurred.

2.36 The defence is subject to certain qualifications imposed by the Proceeds of Crime Act 2002 (Money Laundering: Exceptions to Overseas Conduct Defence) Order 2006. The effect of these qualifications is that the double criminality defence will only be available in cases where the conduct in question would be punishable by a maximum term of imprisonment of one year or less in the UK. Accordingly, the defence will not be available in the case of more serious criminal conduct, such as corruption or tax evasion, which is punishable by terms of imprisonment exceeding one year. An exception to this is provided for certain offences relating to the carrying on of unauthorised banking or financial services business and gaming. Where the conduct engaged in outside the UK would constitute an offence under the FSMA 2000, s 23 or 25, an offence under the Gaming Act 1968 or an offence under the Lotteries and Amusements Act 1976, a defence will be available if the conduct is legal in the jurisdiction in which it occurs.

2.37 The double criminality defence applies in respect of each of the principal money laundering offences under POCA 2002, ss 327–329 of and is contained in, respectively, ss 327(2A), 328(3) and 329(2A). A similar but not identical defence is provided in the case of the failure to report offence contained in POCA 2002, s 330. This is considered further below.

Small value transactions

2.38 The definition of criminal conduct in POCA 2002, s 340(2) does not establish a *de minimis* threshold as to the types of underlying criminal conduct that will give rise to criminal property and therefore a money laundering offence. The definition of criminal conduct was designed to capture money laundering

carried on in relation to the proceeds of any crime, irrespective of the seriousness of the crime. In contrast, the Criminal Justice Act 1988 applied a *de minimis* threshold so that it criminalised money laundering in relation to the proceeds of indictable offences only. The breadth of definition of criminal conduct under POCA 2002 means that money laundering issues can arise even in the case of what may be considered to be minor or technical breaches of the criminal law. To mitigate the effect of the absence of a *de minimis* threshold on banks (ie authorised deposit taking institutions) and to enable them to process small value transactions, POCA 2002 was amended[18] to provide that a deposit taking body will not commit a principal money laundering offence if it does an act operating an account maintained with it and the value of the criminal property concerned is less than a threshold amount, which is currently specified to be £250.[19] The deposit taking body may nevertheless be under an obligation to make a suspicious activity report under POCA 2002, s 330.

Criminal property

2.39 Criminal property is defined in POCA 2002, s 340(3). There are two main elements to this definition:

(i) the property[20] must constitute a person's benefit from criminal conduct or it must represent such a benefit (in whole or in part, directly or indirectly);

(ii) the alleged offender must know or suspect that the property constitutes criminal property. The definition of criminal property therefore establishes the *mens rea* of the principal money laundering offences, requiring a state of mind of 'knowledge or suspicion'.[21] Under s 340(4) it is immaterial who carried out the conduct, who benefited from it and when the conduct was engaged in. The definition specifically includes criminal conduct committed before the passing of POCA 2002. The section is aimed at laundering activity that takes place after POCA 2002 entered into force in relation to criminal property derived from crimes committed before the Act. Property must be criminal property at the time of commission of the principal money laundering offence.[22] For example, in relation to the offence of transferring criminal property under POCA 2002, s 327, if the property is not criminal property at the time of the transfer, the offence is not committed.

2.40 As indicated, the definition of criminal property expressly provides that it is immaterial who carried out the criminal conduct. Thus the definition extends

18 The relevant amendments are contained in POCA 2002, ss 327(2C), 328(5) and 329(2C).

19 POCA 2002, s 339A.

20 Property is defined in POCA 2002, s 340(9) as all property wherever situated, including cash, things in action and other intangible or incorporeal property.

21 Although the terms of the offence under POCA 2002, s 328 provide that a person must know or suspect that the relevant arrangements facilitate the acquisition, retention, use or control of criminal property.

22 *R v Loizou* [2005] EWCA Crim 1579.

to property in the hands of the predicate offender and anyone else. In *R v Chen,*[23] for example, the defendant was convicted under POCA 2002, s 327 on the basis that he had concealed, disguised, converted or transferred the benefit that he had received as a result of his own criminal conduct (being payments received through the submission of false timesheets).

2.41 POCA 2002, s 340(5)–(10) further clarifies the meaning of criminal property. The sub-sections provide as follows:

- a person benefits from criminal conduct if he obtains property as a result of or in connection with conduct (s 340(5));
- if a person obtains a pecuniary advantage as a result of or in connection with conduct, he is to be taken to obtain as a result of or in connection with the conduct a sum of money equal to the value of the pecuniary advantage (s 340(6));
- references to property or a pecuniary advantage obtained in connection with conduct include references to property or a pecuniary advantage obtained in both that connection and some other (s 340(7));
- if a person benefits from criminal conduct his benefit is the property obtained as a result of or in connection with the conduct (s 340(8));
- property is all property wherever situated (s 340(9));
- property is obtained by a person if he obtains an interest in it (s 340(10)).

2.42 The issue of what constitutes a pecuniary advantage for the purpose of POCA 2002, s 340(6) has been considered in the context of whether the proceeds of tax evasion constitute criminal property for the purpose of POCA 2002. Sums that a taxpayer does not declare or account to the relevant revenue authorities for tax purposes may in many cases constitute profits or income from legitimate trading and are not inherently in the nature of criminal property (in the sense that they are not derived from criminal conduct). However, in *R v K*[24] the court found that a person who cheats HMRC obtains a pecuniary advantage as a result of criminal conduct within the meaning of POCA 2002, s 340(6). The advantage obtained is a sum equal to the value of the amount by which HMRC has been cheated.

Acts in relation to the criminal property

2.43 As noted above, there are three principal money laundering offences in POCA 2002. These offences will be committed where an act falling within POCA 2002, ss 327–329 is carried on in relation to criminal property. The principal money laundering offences are considered below.

23 [2008] EWCA Crim 1141.
24 [2007] EWCA Crim 491.

Concealing, disguising or converting

2.44 Under POCA 2002, s 327(1) a person commits an offence if he conceals, disguises, converts, transfers or removes criminal property from England and Wales, from Scotland or from Northern Ireland. Concealing or disguising criminal property includes concealing or disguising its nature, source, location, deposition, movement or ownership or any rights with respect to it.[25]

2.45 Prosecutions brought under POCA 2002, s 327 cover a wide variety of factual circumstances. These range from cases involving[26] employees of an investment management firm who set up bogus accounts into which they received proceeds from the redemption of customers' investments, to cases involving[27] the conversion of cash from the sale of drugs.

2.46 The UK courts will have jurisdiction provided that either the criminal property enters the country or some element of the offence takes place within the country. The element of the offence that needs to be committed within the country could be quite small, and could include giving or accepting banking instructions regarding criminal property which is physically located elsewhere.

Concerned in arrangements

2.47 Section 328(1) of POCA 2002 makes it an offence for a person to enter into or become 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. This offence may typically be committed by a third party such as a bank, which unwittingly becomes involved in another person's wrongdoing.[28] The concept of being 'concerned in an arrangement' is broad and is capable of capturing virtually any form of involvement, direct or indirect, with criminal property.

2.48 The courts have, however, placed an important limitation on the scope of s 328. In *Bowman v Fels*[29] the Court of Appeal found that POCA 2002, s 328 was not intended to cover the ordinary conduct of litigation by legal professionals. The Court held in that case that when legislating, Parliament could not have intended that action taken by lawyers in order to determine or secure legal rights or remedies for their clients should involve them becoming 'concerned in an arrangement' involving criminal property within the meaning of POCA 2002, s 328.

Acquisition, use and possession

2.49 Under POCA 2002, s 329 it is an offence to acquire, use or have possession of criminal property. As noted above, an offence can be committed

25 POCA 2002, s 327(3).
26 *R v Price* [2008] EWCA Crim 590.
27 *R v Rouke* [2008] EWCA Crim 233.
28 See, for example, *K Ltd v National Westminster Bank* [2006] EWCA Civ 1039.
29 [2005] 2 Cr App R 19.

by a person where he acquires, uses or has possession of the proceeds of his own criminal conduct. A defence is provided in s 329(2)(c) so that an offence is not committed where a person acquires, uses or has possession of property for adequate consideration. The Home Office has stated[30] that this defence '… is necessary in order to protect persons, such as tradesmen, who are paid for ordinary consumable goods and services in money which they know or suspect comes from crime'. The defence is not available[31] where a person provides goods or services which he knows or suspects may help another to carry out criminal conduct.

Mens rea: knowledge or suspicion

2.50 The mens rea requirement is found in the definition of criminal property in POCA 2002, s 340(3). It requires the alleged offender to know or suspect that property constitutes or represents the benefit of criminal conduct.[32]

2.51 Knowledge for these purposes means 'actual' knowledge. The Guidance states that 'having knowledge means actually knowing something to be true … that said, knowledge can be inferred from the surrounding circumstances; so for example, a failure to ask obvious questions may be relied upon by a jury to imply knowledge'. In the *El-Kurd*[33] case the judge held that the jury was entitled to draw appropriate inferences. What this means in practice is not entirely clear, but it is very likely to be analogous to cases involving handling stolen goods (where inferences can be drawn as to a person's knowledge that the goods were stolen from the circumstances in which the goods were bought). Proving a person's level of knowledge is usually difficult.

2.52 Suspicion is a much easier test and presents a greater risk. The meaning of the word 'suspicion' has been considered in a number of cases both under the predecessor to POCA 2002 (the Criminal Justice Act 1988) and under the 2002 Act itself.

2.53 The case of *R v Da Silva*[34] concerned a prosecution under the Criminal Justice Act 1988, s 93A(1)(a), which was the predecessor to POCA 2002, s 328. The Court of Appeal was required to consider the meaning of 'suspicion' and found that:

> 'It seems to us that the essential element in the word "suspect" and its affiliates, in this context, is that the Defendant must think that there is a possibility, which is more than merely fanciful, that the relevant facts exist. A vague feeling of unease will not suffice. But the statute does not require the suspicion to be "clear" or "firmly grounded and targeted on specific facts" or based on "reasonable ground"'.

30 Home Office document: Proceeds of Crime Consultation on Draft Legislation.
31 POCA 2002, s 329(3)(c).
32 See para 2.25 above.
33 *R v El-Kurd* [2000] All ER (D) 1446, CA.
34 [2006] EWCA Crim 1654.

The definition of suspicion used in *R v Da Silva* was adopted in *K Ltd v National Westminster Bank plc*,[35] which addressed the position of a bank that had refused to implement a customer order to transfer funds on the basis of a suspicion of money laundering. The issue arose as to what constituted a proper suspicion in law. The court found that the existence of a suspicion is a subjective fact and that there is no legal requirement that there should be reasonable grounds for a suspicion. The issue was also considered in *Shah v HSBC Private Bank (UK) Ltd*.[36] In that case the court rejected a contention that a suspicion should be a 'rational' suspicion and said that the decision in *K Ltd* clearly established that a suspicion under POCA 2002 is a subjective one.

Comparison with the knowledge needed to establish civil liability

2.54 The ingredients of civil liability (for dishonest assistance) are similar to those for criminal liability for assistance. The level of knowledge needed for civil liability for knowing assistance is considered below. Civil liability is unlikely to arise simply where the launderer merely suspects (unless coupled with a decision not to make obvious enquiries). It seems arguable that criminal liability may be more easily incurred on the same facts than civil liability. In principle, a lesser degree of knowledge or suspicion should not suffice to establish criminal liability. The two liabilities have very different legal and political backgrounds, but it may be difficult to avoid the conclusion that the criminal liability provides a greater danger in this area.

DISCLOSURE AND THE CONSENT REGIME

2.55 Under POCA 2002, a person may choose or be required to report a knowledge or suspicion of money laundering either where a consent is required in order to avoid the commission of a principal money laundering offence or where a proactive reporting obligation applies. In the former case where consent is required, a person makes an Authorised Disclosure under POCA 2002, s 338 seeking an appropriate consent under POCA 2002, s 335. In the latter case of a proactive report, a disclosure is made under POCA 2002, s 330.

2.56 Between October 2015 and March 2017 a total of 634,113 Suspicious Activity Reports (SARs) were made. Of these, 27,471 were for a defence against a money laundering offence under POCA 2002 and 422 were for a defence against a terrorist financing case. Consent was refused in 5.67% of cases in respect of a POCA 2002 offence and in 6.87% of cases in a TA 2000 offence. Statistics published by the NCA in its SARs Annual Report for 2017 show a clear upward trend of around 9% in the making of SARs. In its Circular on the operation of the consent regime, the Home Office has stated that the consent regime has

35 [2006] EWCA Civ 1039.
36 [2009] EWHC 79 (QB) and [2010] EWCA Civ 31.

two purposes: first, to offer law enforcement agencies the opportunity to gather intelligence or to intervene in advance of potentially suspicious activity taking place; second, to allow individuals and institutions who make reports to seek consent to proceed with a prohibited act. The operation of the consent regime and the submission of suspicious activity reports are subject to review at the time of writing. The Law Commission has been mandated with reviewing the consent regime in order to make it more effective. The Law Commission is, in particular, considering how defensive reporting can be minimised and the quality of suspicious activity reports improved.

Regulated sector – failure to disclose

2.57 POCA 2002, s 330 introduced a new offence for persons in the regulated sector of failing to report a knowledge or suspicion of money laundering as soon as reasonably practicable. The offence in POCA 2002, s 330 replaced the offence previously contained in the Drug Trafficking Act 1994, s 52.[37] Section 330 widened the scope of the offences it replaced, beyond drug money laundering to the laundering of the proceeds of any criminal conduct. Moreover, controversially at the time, POCA 2002, s 330 introduced criminal liability in circumstances where a person in the regulated sector acted negligently in failing to disclose a suspicion of money laundering.

2.58 The offence of failure to disclose under s 330 may be committed where a person knows or suspects or has reasonable grounds to know or suspect that another person is engaged in money laundering. The standard of 'reasonable grounds' is an objective standard, so that liability could arise under s 330 even where a person does not in fact know or suspect the relevant matters. It is sufficient for the prosecution to show that a person 'should have' known or suspected. In the case of *R v Sally Lane and John Letts*[38] the Supreme Court considered the meaning of the analogous term 'reasonable cause to suspect' under the TA 2000, s 17(b). The Court found that this required that there exists objectively assessed cause for suspicion, which would be satisfied when, on the information available to the accused, a reasonable person would suspect that the money might be used for terrorism. The Supreme Court's judgment supports the approach that under POCA 2002 as well, the requirement is for objective grounds to suspect. The UK Government[39] justified this standard of liability on the basis that '… persons who are employed in the regulated sector should be expected to exercise a higher level of diligence in handling transactions than those employed in other businesses'.

2.59 The introduction of such a wide failure to disclose offence was resisted by the British Bankers Association and other industry bodies. The Association's

37 In Northern Ireland, the Proceeds of Crime (Northern Ireland) Order 1996, art 44.
38 [2018] UKSC 36.
39 Home Office – Proceeds of Crime Consultation on Draft Legislation.

objections are indicated in the following extract taken from their response to the consultation paper on the legislation:

> '… reporting suspicion goes one step further than reporting knowledge; having reasonable grounds for suspicion goes one step further still. Whilst it is easy for anyone using hindsight or working in an investigative role to decide that an action is suspicious, it will not necessarily be so apparent to a member of staff in a line role. Such staff have many day to day pressures and may rarely ever come across a criminal activity'.

As indicated, an offence is committed where a person has reasonable grounds to know or suspect that another person is engaged in money laundering. Money laundering is defined under POCA 2002, s 340(11) as an act that constitutes an offence under POCA 2002, ss 327, 328 or 329 and extends to inchoate offences such as conspiracy. The definition of money laundering also covers acts carried on outside the UK that would constitute money laundering if done in the UK.

2.60 The information or other matter on which the alleged offender's knowledge or suspicion is based, or that gives rise to reasonable grounds for suspicion, must come to him in the course of a business in the regulated sector. The regulated sector is defined[40] to have a very similar scope to the sectors covered by the MLR 2017 and defined under those Regulations as a business carried on by a 'relevant person'. Where a firm carries on activities some of which are in the regulated sector and some of which are not, only the employees carrying on the regulated sector activities are intended to be caught by the failure to disclose offence. The knowledge or suspicion may relate to a client, counterparty or any other person, provided that the information or other matter giving rise to the knowledge or suspicion comes to a person in the course of the firm's regulated sector business.

2.61 The alleged offender must be able to identify the person suspected of money laundering or the whereabouts of the laundered property or must believe that, or it is reasonable to expect him to believe that, the information or matter will assist in identifying the person suspected of money laundering or the laundered property. This requirement was introduced by an amendment made under the Serious Organised Crime and Police Act 2005, s 104. The purpose of the requirement is to reduce the volume of SARs made which contain no useful information (for example, reports by card issuers relating to stolen cards, where no information is available in relation to the identity of the person who has stolen the card or the whereabouts of the proceeds of the offence).

2.62 In order to avoid the commission of an offence a person employed in the regulated sector must make the required disclosure[41] to a 'nominated officer' or NCA as soon as is practicable. A nominated officer is a person nominated by the

40 POCA 2002, Sch 9.
41 Defined in POCA 2002, s 330(5).

alleged offender's employer to receive disclosures under POCA 2002, s 330.[42] The policy intention is that disclosures in the regulated sector should be made directly to NCA rather than through a constable or customs officer. However, employees of a regulated sector firm may make a disclosure either directly to NCA or to the firm's Nominated Officer. The role of the Nominated Officer is to act as a filter for disclosures to NCA.

2.63 Section 330 contains certain exceptions to liability for the failure to disclose offence. Under POCA 2002, s 330(7A) the offence of failure to disclose is not committed where a person in the regulated sector believes on reasonable grounds that the money laundering of which he has knowledge or suspicion is occurring outside the UK and is not unlawful under the criminal law of the jurisdiction in which it is taking place. As with the double criminality defence under POCA 2002, ss 327(2A), 328(3) and 329(2A), limits may be placed on the scope of this defence. However, for the purpose of the failure to disclose defence, at present, no such limitation has been put in place.

2.64 Under POCA 2002, s 330(6)(a) an offence is not committed where a person has a reasonable excuse for not making the required disclosure. There is considerable uncertainty as to what would constitute a reasonable excuse, so care would need to be exercised in seeking to rely on this provision.

2.65 Where an employee in the regulated sector has not received training on identifying suspicious transactions, this may found the basis of a defence for that employee. Under POCA 2002, s 330(7), where the person concerned has not been provided with suitable training by his employer and did not have actual knowledge or suspicion of money laundering, no offence will be committed. However, a failure by a regulated sector firm to provide training to employees may mean that the firm is in breach of its obligations under the MLR 2017.

2.66 According to POCA 2002, s 330(10), information or other matters that come to a professional legal adviser or 'relevant professional adviser' do not need to be disclosed if communicated in privileged circumstances. A relevant professional adviser is an accountant, auditor or tax adviser who is a member of a relevant professional body. The scope of the exemption for information communicated in privileged circumstances was expanded to cover such relevant professional advisers following requests from the accountancy profession. The exemption may, however, be of limited use since it only applies where information is communicated in connection with the giving by the adviser of legal advice to the client or by a person seeking legal advice or by a person in connection with legal proceedings or contemplated legal proceedings. The privilege exemption does not apply to information which is communicated or given with a view to furthering a criminal purpose.

42 POCA 2002, s 330(9).

Nominated Officers – regulated sector

2.67 A SAR may be made externally to the NCA or internally to the regulated sector firm's Nominated Officer. In most cases disclosures will in the first instance be made internally to the Nominated Officer. From the perspective of the employee of the regulated sector firm, disclosure to the Nominated Officer will be sufficient to discharge the employee's duties under POCA 2002, s 330. Once a disclosure has been made to the Nominated Officer, he must consider whether it is necessary to make an onward disclosure to NCA.

2.68 The role of the Nominated Officer in this connection is governed under POCA 2002, s 331. This section sets out a specific offence for Nominated Officers who will themselves be guilty of an offence if after having received a SAR pursuant to s 330, they fail to make a report to NCA, where the SAR gives rise to reasonable grounds for knowing or suspecting money laundering.

Authorised disclosures and consent to a prohibited act

2.69 As noted above, disclosures may also be made in order to obtain a consent under POCA 2002, s 335, where a person is concerned that he would commit a principal money laundering offence without the consent. In such circumstances an authorised disclosure would be made to obtain an appropriate consent under POCA 2002, s 335 to do a prohibited act (being an act that would otherwise constitute an offence under POCA 2002, ss 327(1), 328(1) and 329(1)).

2.70 The courts have noted that the POCA 2002 regime exerts pressure on persons (particularly banks) to disclose information to enable authorities to obtain information about criminal activity and to increase the prospects of being able to detect and freeze criminal property. In *Shah v HSBC Private Bank (UK) Ltd* the court stated that

> 'POCA places the requisite pressure on the bank by exposing it to the risk of criminal liability for carrying out a prohibited act. A bank can only raise a defence to doing a prohibited act under s 327, 328 or 329 POCA by, prima facie, breaching the banking contract. First by breaching the duty to maintain secrecy by making an authorised disclosure. Secondly, by failing to carry out the customer's instruction (or mandate) until it has received appropriate consent or the notice and moratorium provisions are exhausted (see s 335 POCA)'.

2.71 Section 338(1) of POCA 2002 provides that a disclosure is an authorised disclosure if it is a disclosure to a constable (including NCA), a customs officer or a Nominated Office that property is criminal property. An authorised disclosure may therefore be an external disclosure (to NCA or Customs) or an internal disclosure to a Nominated Officer. It is important to note that the disclosure must be to the effect that property is criminal property. In the *Shah* case the bank's client claimed damages from the bank on various grounds where the bank had made an authorised disclosure and sought an appropriate consent. These grounds

included a challenge on the basis that the disclosure made by the bank was not an authorised disclosure as it did not specifically disclose that property was criminal property.

2.72 An authorised disclosure will in most cases need to be made prior to the carrying out of the prohibited act. However, the disclosure may in certain limited circumstances be made while doing the prohibited act or afterwards, as follows:

- the disclosure may be made while doing the prohibited act provided that the person concerned had started to do the act at a time when he did not know or suspect that the act was a prohibited act. In such circumstances, the disclosure must be made on the person's own initiative as soon as practicable after first knowing or suspecting that property constitutes or represents a person's benefit from criminal conduct (POCA 2002, s 338(2A));
- the disclosure may also be made after the person carries out the prohibited act. In order for this to apply, the person must have a reasonable excuse for failing to make the disclosure before doing the act and the disclosure must be made as soon as it is practicable for the person concerned to make it.

2.73 Upon the making of a disclosure, the NCA has an initial notice period of seven working days, starting with the first working day after the disclosure is made, in which to consider the request for consent. Consent must either be given or refused within this seven-day notice period. If consent is not refused within this period, there will be a deemed consent to the carrying out of the prohibited act. If consent is refused, a further 31-day moratorium period will apply. Unless consent is refused again within this period, there will be a deemed consent to the carrying out of the act. As explained further below, where consent has been refused, NCA must keep its decision under review during the moratorium period and must give a consent where there is no longer any good reason for withholding it. As noted above, this period of time may now be extended on application to the Court under POCA 2002, s 336A.

2.74 Where a disclosure is made to a Nominated Officer[43] POCA 2002, s 336 will apply to the circumstances in which the Nominated Officer may grant a consent to the doing of a prohibited act. The Nominated Officer must not give the appropriate consent to the carrying out of a prohibited act unless the Nominated Officer has made a disclosure to NCA and consent has been provided, or either the notice period or moratorium period referred to above have expired without NCA refusing consent. A Nominated Officer commits an offence (liable to a term of imprisonment of up to five years and/or an unlimited fine) if he provides an appropriate consent without having himself obtained a consent from NCA or without a deemed consent by virtue of the expiration of either the notice period or moratorium period without NCA refusing consent. An offence may also be

43 Under POCA 2002, s 338(5) a nominated officer is a person nominated to receive authorised disclosures by the employer of the person making the disclosure.

committed under POCA 2002, s 332 where the Nominated Officer fails to make a disclosure to the NCA, where he acquires knowledge or a suspicion that another person is engaged in money laundering in consequence of a disclosure made under POCA 2002, s 338.

Effect of a consent

2.75 A consent to perform a prohibited act will only protect the person making the disclosure from otherwise committing a principal money laundering offence. A consent will not provide protection from civil claims against the firm, so that if – following a consent – a firm transfers property that is suspected to be criminal property (for example, because it suspects the property to be the proceeds of a fraud or other misappropriation of assets) the firm might be liable to the owner of the assets. The fact that the firm had made the SAR would mean that it at least had a suspicion of the tainted origin of the property in question.

2.76 Accordingly, a consent from the NCA will not necessarily protect a person from the risk of constructive trust liability. In such situations, it may be prudent to approach the court for directions and/or a declaration under CPR 40.20 as a person who acts in accordance with the court's direction will not have acted dishonestly. Directions and/or a declaration may be sought in order to avoid constructive trust liability under the civil law. Moreover, the fact that the firm has made a SAR and received a consent to act may in itself be sufficient to rebut an assertion that it had somehow acted dishonestly in transferring assets or funds.

Operation of the consent regime – practical issues

2.77 The operation of the consent regime has given rise to considerable practical problems, particularly for banks. Once a bank makes a SAR in relation to a client, it is unable to operate the client's account as this could constitute a principal money laundering offence and potentially expose the bank to civil liability as a constructive trustee. On the other hand, a failure to implement a client's instructions could constitute a breach of the client's mandate with the bank and result in legal action being taken against the bank for an injunction requiring the bank to comply with the mandate or for damages. These issues have now been considered closely by the English courts in the context of the various applications in *Shah v HSBC Private Bank (UK) Ltd*.[44]

2.78 These difficulties were more acute under the Criminal Justice Act 1988, which did not impose the timetable for the notice and moratorium periods now contained in POCA 2002. Accordingly, under the pre-POCA 2002 regime, NCIS was not under the same time pressures to which NCA is now subject. The two

44 [2012] EWHC 1283 (QB).

leading cases on these issues under the Criminal Justice Act 1988 are *C v S*[45] and *Bank of Scotland v A Ltd.*[46] The timing pressure created under the statutory timetable for dealing with consents resulted in the amendment of POCA 2002 by the Criminal Finances Act 2017 to allow the extension of the moratorium period.

2.79 In the *Bank of Scotland* case the bank suspected that an account in the name of A Ltd was being used to launder criminal property. It was concerned that paying funds in accordance with A Ltd's instructions could result in a money laundering offence and possible civil constructive trust liability. On the other hand, refusal to pay could result in a tipping off offence as well as a civil claim from A Ltd. Accordingly, the Bank of Scotland applied for directions. On that application, the judge made an interim order restraining the bank from making any payments from the account without the court's permission. The judge also made an unusual order that the customer should not be told of the existence of the order. The bank informed the customer that it was not going to permit any further transactions on the account. The customer instituted its own proceedings against the bank for an order that the bank pay the monies in the account to the customer's solicitors. When the matter came before the court, the bank informed the judge, in private, of the order that had already been made and the matter was adjourned. Subsequently the matter came back before a different judge, who discharged the original order, holding it should never have been made. Thereafter the matter came before the Court of Appeal.

2.80 The Court of Appeal held that:

- the judge had been wrong to grant an injunction preventing the bank from paying monies out from its account to the customer;
- the appropriate course would have been to seek directions from the court with the Serious Fraud Office, rather than the customer, as respondent. If the Serious Fraud Office and the bank could not, between themselves, agree on what information could be disclosed to the customer, the court would have to resolve the dispute;
- the court would use its powers to grant interim declarations in proceedings, setting out the extent of the information which could be revealed to the customer.

2.81 Similar issues have also now been considered in a number of cases under POCA. The cases brought by clients of banks have sought the enforcement of the client's mandate with the bank and have attacked banks on the basis that banks had made SARs in circumstances which they did not have proper 'suspicions' to justify the making of the SAR. The role of the NCA in dealing with consent applications has also been the subject of review. Certain of the relevant cases are mentioned below.

45 [1999] 1 WLR 1551.
46 [2001] EWCA Civ 52.

- in *Squirrell v National Westminster Bank plc*[47] a bank's client applied to unfreeze its account with the bank, which had been frozen on the basis of concerns by the bank that the account contained the proceeds of crime and that the continued operation of the account would result in the bank committing an offence under POCA 2002, s 328. The bank had filed a SAR with Customs. The court refused the application made by the bank's client, finding that once the bank suspected that the client's account contained the proceeds of crime, it was obliged to report that suspicion and not to carry out any transaction on the account or make any disclosure which could affect any inquiries the authorities might make. Mr Justice Laddie stated that the course adopted by the bank was 'unimpeachable' and that there was no question of the court ordering the bank to operate the account in accordance with the client's instructions, as to do so would be to require the bank to commit an offence;
- in *K Ltd v National Westminster Bank plc*[48] the court was required to consider an application by a bank's customer for an interim injunction requiring the bank to comply with certain payment instructions. The bank had declined to comply with its client's instructions on the grounds that it would become concerned in an arrangement contrary to POCA 2002, s 328. The bank made a disclosure to Customs in order to obtain a consent. The Court of Appeal found that the effect of POCA 2002 was to render it temporarily illegal to perform the contract with the customer and that the contract would be suspended until any illegality was removed. During the period of suspension of the contract, no legal right existed on which a claim to an injunction could be brought. The court was also required to consider what constituted a 'suspicion' under POCA 2002, and found that a suspicion was a matter of subjective fact. On this basis, it did not matter whether or not there were reasonable grounds for a suspicion, provided that the bank's suspicions were genuinely held. The court stated that

  > 'The truth is that Parliament has struck a precise and workable balance of conflicting interests in the 2002 Act. It is, of course, true that to intervene between a banker and his customer in the performance of the contract of mandate is a serious interference in the flow of trade. But Parliament has considered that a limited interference is to be tolerated in preference to allowing the undoubted evil of money-laundering to run rife in the commercial community'.

- in *Shah v HSBC Private Bank (UK) Ltd* the bank's client brought an action for damages in respect of delays on the client's account consequential upon the firm freezing the account due to concerns that the bank would be committing an offence under POCA 2002, s 328. The bank suspected that funds in the client's account were criminal property and made a disclosure to SOCA seeking an appropriate consent. It was subsequently accepted by the bank that the funds concerned did not constitute criminal property. Amongst other things, the claimant contended that the bank

47 [2005] EWHC 664 (Ch).
48 [2006] EWCA Civ 1039.

was under a duty of care in maintaining its account and in complying with instructions, including the making of SARs under POCA 2002. The claimant alleged that the bank had breached this duty by failing to make the SAR as soon as practicable, that there were no rational grounds to suspect money laundering and that there was a failure to refer to 'criminal property' in the SAR. The court rejected these contentions, but did accept that it was certainly arguable that the bank's duty to its customer was not completely excluded by POCA 2002. On this basis the court said that if a bank delays unreasonably in processing a transaction following receipt of a consent, or unreasonably delays in making a disclosure, then a breach of duty may be involved. However, on the facts of the *Shah case*, the court found that there had not been any breach of any such duty. At trial the court accepted the bank's case that a term would be implied in the contract with the customer to the effect that the bank could refuse to execute a payment instruction in the absence of an appropriate consent. The court also agreed with the bank that 'suspicion' under POCA 2002 is a subjective suspicion, so that the claimant was unsuccessful in his attempts to undermine the suspicion held by the bank on the grounds that it was irrational or negligently held;

- *R (on the application of UMBS Online Ltd) v Serious Organised Crime Agency* concerned a judicial review of SOCA's refusal of consent. In broad terms the court found that SOCA should not withhold consent without good reason to do so. Moreover, once consent has been refused, SOCA should keep its decision under review and must give a consent where there is no longer any good reason for withholding it.

2.82 In some cases a bank may be left holding money which it suspects constitutes the proceeds of crime. In *Commerzbank Aktiengesellschaft v IMB Morgan plc*[49] the court was required to deal with the distribution of funds in correspondent bank accounts maintained by Commerzbank's London branch. Commerzbank held two correspondent bank accounts in the name of a Nigerian stockbroker. Commerzbank terminated its relationship with its client following a number of incidents relating to the operation of the account and a subsequent police investigation which concluded that there was strong evidence that the accounts were being used for money laundering. In particular, there was evidence that a significant number of payments into the account were the result of 'advance fee' or '419' frauds. Commerzbank reported their suspicions relating to the account to NCIS, who declined consent to deal. Commerzbank was left holding balances on the accounts and had to determine what to do with these funds. Commerzbank brought High Court proceedings (interpleader proceedings), essentially with a view to leaving the court to determine the appropriate distribution of funds. An investigation carried out by Commerzbank sought to identify potential claimants to the funds, who were given notice of the court proceedings and required to submit a claim if appropriate.

49 [2004] EWHC 2771 (Ch).

DOES DISCLOSURE RESULT IN A BREACH OF CLIENT CONFIDENTIALITY?

2.83 A bank owes a duty of confidentiality to its customer not to disclose details about the customer or their affairs. The duty arises from implied obligations arising out of the banker-customer relationship. A duty of confidentiality may well be implied into other analogous relationships.

2.84 POCA 2002 provides, in ss 337(1) and 338(4), that a disclosure shall not breach any restriction on the disclosure of information howsoever imposed. The immunity given to protected disclosures (made by persons in the regulated sector) is wider than that in relation to authorised disclosures. Protected disclosures attract immunity if there are reasonable grounds for suspicion. Reasonable grounds (as distinct from actual suspicion) will not be sufficient to attract immunity for authorised disclosures.[50] The reason for this is that authorised disclosures are connected with the principal money laundering offences, for which there is a subjective mens rea. Protected disclosures are connected primarily to the failure to report offence, for which there is an objective mens rea. The provisions of POCA 2002, ss 337(1) and 338(4) do not abrogate legal privilege.

2.85 In addition to the explicit protection contained in POCA 2002, banks and others enjoy immunity under the common law. It has long been established that the duty of confidentiality is a qualified duty. The most important qualification, for present purposes, is that a bank is at liberty to disclose information where such disclosure is under compulsion of law. Thus a bank may disclose to a third party confidential details relating to a customer, where it is required to do so by a statutory provision or by order of the court. The failure to disclose offence is a clear instance where this exception to the implied duty of confidentiality will be available.

2.86 It is implicit in relation to both types of disclosure that the discloser must act in good faith. Some have suggested that similar statutory protections under the previous law would not extend to liability for defamation or negligence. This does not appear to have been tested but it seems likely that disclosure reports will attract qualified privilege.

2.87 The protection is confined to the information which is provided in the disclosure report (together with additional information requested in accordance with POCA 2002, s 339(2) and (3)). The firm (through its MLRO) is likely to be approached by an investigating officer who may ask for additional information and documents. There is a risk that provision of additional information or documents on a voluntary basis falls outside the scope of the protection afforded by POCA 2002, ss 337 and 338. Therefore, it is prudent to refuse to release any documents or information until an appropriate production order is obtained.

50 POCA 2002, s 338(4).

COULD A DISCLOSURE REPORT BE USED TO FOUND A DEFAMATION ACTION?

2.88 In the unlikely event that a disclosure report comes to the attention of the subject of suspicion, the subject may seek redress by bringing proceedings for defamation. A disclosure report may attract qualified privilege, which provides a defence to an action in defamation unless the claimant can prove malice, such as that the person who published the statement did not honestly believe it to be true. The case of *Mahon v Rahn (No 2)*[51] raised similar issues. It concerned information provided to a regulator in the course of an investigation into whether officers of a bank were fit and proper. The court found that the information supplied was privileged:

> 'A document created during the course of an investigation by a financial regulator attracted absolute privilege. It was not possible to make a logical distinction between the situation in which a criminal investigator sought evidence to support a criminal charge and a situation in which a financial regulator sought evidence to put before a tribunal to the effect that someone was not a fit and proper person to conduct investment business. The flow of information to financial regulators might be seriously impeded if informants feared that they might be harassed by libel proceedings. It followed that the letter had been published on an occasion of absolute privilege'.

The issue of defamation in the context of a SAR was the subject of proceedings between David Lonsdale and National Westminster Bank plc, with which Mr Lonsdale held bank accounts. The bank froze Mr Lonsdale's account with the bank. Mr Lonsdale issued a claim against the bank for breach of contract, breach of the Data Protection Act 1998 and defamation. In relation to the claim in defamation, Mr Lonsdale alleged that the bank had in a SAR submitted to the NCA defamed him by suggesting that money in his accounts may have been derived from crime and/or that it genuinely suspected that the money was derived from crime and that it had reasonable grounds for so suspecting. The bank relied on qualified privilege in relation to the SAR but Mr Lonsdale relied on certain other communications including internally within the bank. The bank applied to strike out Mr Lonsdale's claim but the Court declined to do so.[52] The Court took the approach that it was for the bank to prove that qualified privilege applied. Mr Lonsdale was also granted an order for the inspection of the SAR that the bank had made. At the time of writing the case has not been resolved substantively. However, it illustrates the practical issues that can arise when dealing with SARs and the care with which such issues should be handled by banks.

TIPPING OFF AND SUPER-SARS

2.89 POCA 2002, s 333A sets out an offence for persons in the regulated sector to 'tip off' once a SAR has been made. The scope of this offence was amended in

51 [2000] 4 All ER 41, CA.

52 See the judgment of Karen Steyn QC at [2018] EWHC 1843.

2007 to limit it to the regulated sector in line with the UK's obligations under the Third Money Laundering Directive. An offence[53] is committed if a disclosure has been made under Part 7 of POCA to a constable, the NCA, an officer of HMRC or a Nominated Officer and a person then makes a disclosure to a third person which is likely to prejudice any investigation which might be conducted following the initial disclosure. As indicated, since 2007, when POCA 2002 was amended, this offence is committed only where the information on which the initial disclosure is based came to the person in the course of business in the regulated sector. POCA 2002, ss 333B–333D contain exemptions that permit disclosures to be made in certain circumstances – for example, between employees, officers and partners of the same undertaking, between credit institutions, between financial institutions and between professional legal advisers. The risk of committing a tipping off offence has created a practical impediment to financial institutions sharing information in order to resolve concerns around transactions or clients. This position has been addressed through the introduction of so called 'super-SARs', which provide a framework within which institutions can exchange information in circumstances that might otherwise result in a disclosure that could amount to a tipping off offence.

2.90 While the tipping off offence is limited to the regulated sector, a separate offence under POCA 2002, s 342 applies generally and makes it an offence to 'prejudice an investigation'. An offence is committed under s 342 if a person knows that an investigation is being conducted, and makes a disclosure which is likely to prejudice that investigation.

2.91 The investigation may be for the purposes of confiscation, civil recovery or money laundering.[54] In addition, under POCA 2002, s 342 it is an offence where a person falsifies, conceals, destroys or otherwise disposes of documents relevant to an investigation knowing or suspecting that an investigation is being or about to be conducted.[55]

2.92 Disclosure obviously includes informing any person (and would include the customer/client as well as other parties such as the possible victim of any wrongdoing). The maximum penalty for tipping off or prejudicing an investigation is five years' imprisonment and/or a fine. POCA 2002, s 342(3)–(5) provides that a person does not commit the offence of making a disclosure that is likely to prejudice an investigation if any of the following apply:

- the person did not know or suspect that the disclosure was likely to be prejudicial;
- the disclosure is made in carrying out a function that he has relating to the enforcement of any provisions of POCA 2002 or of any other Act relating to criminal conduct or the benefit of criminal conduct; or

53 POCA 2002, s 333A.
54 POCA 2002, s 342(1).
55 POCA 2002, s 342(2) and (6).

- he is a professional legal adviser and the disclosure is made in circumstances that would attract legal professional privilege. It is emphasised that this defence is only available to professional legal advisers and not, for example, to accountants. Privilege attaches to lawyer/client communications connected with the giving of legal advice and to communications with other persons in connection with legal proceedings or contemplated legal proceedings. Privilege is not available if the disclosure is made to further a criminal purpose.

2.93 It is not clear whether disclosure for these purposes includes so called constructive disclosure, which might arise, for example, where an intermediary terminated the client's retainer or refuses to action instructions, or delays carrying out those instructions, or asks over-zealous questions. It is difficult to give specific guidance and each case is likely to turn on its own particular facts.

2.94 As pointed out above, a recent innovation has been the super-SAR. This was introduced by the Criminal Finances Act 2017. The 2017 Act introduced new ss 339ZB–339ZG into POCA 2002, and new ss 21CA–21CF into the TA 2000. The purpose of such super-SARs is to allow banks and other businesses in the regulated sector to share information with each other on a voluntary basis in relation to a suspicion that a person is engaged in money laundering, suspicion that a person is involved in the commission of a terrorist financing offence, or in relation to the identification of terrorist property or its movement or use. The new provisions in POCA 2002 and the TA 2000 allow information sharing to be instigated either by a regulated sector entity or the NCA. This can be done where the disclosure of the information will or may assist in determining any matter in connection with a suspicion that a person is engaged in money laundering. The provisions in POCA 2002 are supplemented by a Home Office Circular on the CFA.

2.95 In practical terms, where a regulated sector firm suspects money laundering, the super-SAR process allows it to send a request for disclosure to another regulated sector firm. The firm seeking disclosure will also need to notify the NCA of the intention to share information and indicate which regulated sector entities will be involved in the information sharing process. Once there is agreement between the parties to share information, information is disclosed to the party making the request. The party making the disclosure must be satisfied that the requested information will assist in determining any matter relating to a suspicion that a person is engaged in money laundering.

PENALTIES

2.96 The maximum penalty for the principal laundering offences (contained in POCA 2002, ss 327, 328 and 329) varies according to whether the prosecution has been conducted summarily or on indictment. Where a defendant is convicted summarily the maximum penalty is six months' imprisonment or a fine not

exceeding the statutory maximum, or both. Where a defendant has been convicted on indictment, the maximum penalty is 14 years' imprisonment or a fine, or both.[56]

TERRORISM

2.97 The UK has been at the forefront of the international impetus created by the terrorist attacks of 11 September 2001 to combat terrorist financing. There have been a number of legal developments both within the UK and internationally and legislation in this area broadly falls into two categories: legislation which provides for the imposition of penalties on those engaged in terrorist financing; and legislation which aims to combat terrorism by freezing terrorist assets. One key difference between terrorist financing and money laundering is that money laundering relates to the proceeds of crime, whereas a terrorist money laundering offence may be committed in relation to the funds which have a legitimate source.

2.98 The UK has assisted in developing international standards for combating terrorist financing, which includes the FATF's Special Recommendations on Terrorist Financing. The recent developments in the UK's legislation in this area reflect the Government's commitments.

Terrorism Act 2000

2.99 The TA 2000 consolidates the previously piecemeal offences under former legislation. It came into force on 19 February 2001. The Act includes a number of provisions relating to money laundering and, in particular, makes it an offence to enter into or become 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.

The terrorist money laundering offence

2.100 There are two elements to the main offence.[57] First, terrorist property, which is defined[58] to mean:

> '(a) money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation),
>
> (b) proceeds of the commission of acts of terrorism, and
>
> (c) proceeds of acts carried out for the purpose of terrorism'.

56 POCA 2002, s 334.
57 TA 2000, s 18.
58 TA 2000, s 14(1).

It includes property which is wholly or partly directly or indirectly terrorist property.

2.101 Terrorism is defined widely in TA 2000, s 1(1) as the use or threat of action where:

> '(a) the action falls within subsection (2),
>
> (b) the use or threat is designed to influence the government or to intimidate the public or a section of the public, and
>
> (c) the use or threat is made for the purpose of advancing a political, religious or ideological cause'.

2.102 An action falls within TA 2000, s 1(2) if it:

> '(a) involves serious violence against any person,
>
> (b) involves serious damage to property,
>
> (c) endangers a person's life, other than that of the person committing the action,
>
> (d) creates a serious risk to the health or safety of the public or a section of the public, or
>
> (e) is designed seriously to interfere with or seriously to disrupt an electronic system'.

2.103 The Secretary of State for the Home Department is given wide powers in TA 2000, s 3 to proscribe certain organisations which he believes commit or participate in terrorism, prepare for terrorism, promote terrorism or are otherwise concerned in terrorism.

2.104 Actions which are threatened or take place both within and outside the UK which fulfil the criteria laid down in TA 2000, s 1(1), (2) or (3) are terrorist actions for the purpose of TA 2000. Acts that take place abroad directed against foreign governments are capable of constituting acts of terrorism for the purpose of the definition.

2.105 This is a significant expansion to the previous definition of terrorism and has caused some concern. Potentially, it could include organisations which are not widely regarded as being terrorists, such as Greenpeace. The difficulty for financial institutions is monitoring a wide range of social and political organisations which have banking facilities.

2.106 The second element of the offence created by TA 2000, s 18 is entering into an arrangement which facilitates the retention or control of terrorist property. Unlike the other offences relating to terrorist fundraising and the use of terrorist property under TA 2000, ss 15–17 (discussed below), the s 18 offence is a strict liability offence, which means the prosecution does not have to prove any mental state on the part of the defendant. However, it is a defence for the defendant

to show that he did not know, and there were no reasonable grounds to cause the defendant to suspect, that the arrangement related to terrorist property. In practice, therefore, if the defendant became involved with terrorist property completely unknowingly, then criminal liability may not result. The maximum penalty is 14 years' imprisonment and/or an unlimited fine.

Other offences

2.107 TA 2000 also makes it an offence to provide or receive, or invite another person to provide, money or other property, intending or having reasonable cause to suspect that it may be used for the purposes of terrorism.[59] Other offences created by TA 2000 relate to the use and possession of terrorist property[60] or the entering into of arrangements as a result of which money or other property is made available to another person for the purposes of terrorism.[61] These three offences include a mental element (in contrast to the strict liability money laundering offence under s 18).

2.108 Defences are available which apply to any of the offences under TA 2000, ss 15–18 (ie both the terrorist financing and the terrorist money laundering offences) where persons obtain consent from a police constable or from the NCA to be involved in arrangements relating to terrorist property, provided that the consent is obtained either prior to becoming involved in the relevant arrangements, or as soon as reasonably practicable after becoming so involved, provided that the disclosure is made on the person's own initiative.[62] Disclosures to a constable and to the NCA are addressed under different provisions of TA 2000 and, whilst similar, contain certain differences, which are, in part, reflective of the fact that they have been introduced and enacted at different times.

2.109 The defences can also apply where a person did not make the relevant disclosure and obtain the appropriate consent from the NCA, but intended to do so and had a reasonable excuse for not doing so.[63] The various defences, which are similar to the equivalent Authorised Disclosure/consent defences under POCA 2002, provide for consent to be obtained either from a constable or from the NCA (although, where a disclosure is made to a constable, the constable is then under an obligation to notify the disclosure to NCA). Where a request for consent is made to the NCA, the NCA has seven working days to object. As under POCA 2002, once this time period has expired, the applicant is entitled to assume that consent has been granted. By contrast, however, there is no prescribed time limit during which a constable is required to give consent under s 21.

59 TA 2000, s 15.
60 TA 2000, s 16.
61 TA 2000, s 17.
62 TA 2000, ss 21, 21ZA and 21ZB.
63 TA 2000, ss 21 and 21ZC.

Disclosure obligations

2.110 Section 19 of TA 2000 imposes a general duty on any person to disclose a belief or suspicion that arises during the course of a trade, profession, business or employment that another has been involved in terrorism. This offence has survived the amendments to TA 2000, and failure to disclose in such circumstances, as soon as reasonably practicable, is a criminal offence, punishable by a fine and imprisonment for up to five years. The relevant mental threshold for an offence to be committed in such circumstances is limited to actual, subjective, suspicion or belief.

2.111 Amendments made to TA 2000 since it came into force have had the effect of imposing additional disclosure obligations on persons within the 'regulated sector' which are similar to the corresponding requirements imposed on those persons under POCA 2002 discussed above. In particular, TA 2000, s 21A (introduced by amendments made to the Act through the Anti-Terrorism, Crime and Security Act 2001) creates an offence applicable to regulated sector firms where there are reasonable grounds to suspect that another person has engaged in conduct that would constitute a terrorist financing or terrorist money laundering offence under TA 2000, ss 15–18 (where the relevant information came to the firm in the course of 'regulated sector' business).[64]

2.112 The mens rea threshold for this offence is objective (being the same as the test for the equivalent offence under POCA 2002), and could, therefore, effectively be committed through negligence. The reporting obligation operates in the same way as that under POCA 2002, meaning that for an employee of a regulated firm, the obligation to report a suspicion is discharged by informing the firm's MLRO by means of the firm's internal reporting procedures. If the MLRO believes that the internal report contains grounds for suspicion, the MLRO has an obligation to report to the NCA. The offence of failing to disclose by persons in the regulated sector is punishable by a fine, or imprisonment for up to five years. Compliance by a firm with the JMLSG Guidance receives equivalent statutory recognition under TA 2000 to that under POCA 2002, so that a court must take any such compliance into account when deciding whether a terrorist financing offence has been committed.[65]

2.113 TA 2000 is broadly similar to POCA 2002 in applying a single criminality test for its offences, ie an offence will be committed if a person has reasonable grounds to suspect that another person has engaged in money laundering or terrorist financing conduct either in the UK or overseas; unlike POCA 2002, there is no exception requiring dual criminality for lesser offences. Equivalent defences to those under POCA 2002 exist, however, for legal and certain other professional advisers where the information giving rise to suspicion is received in privileged circumstances. As for the general defences of consent described

64 TA 2000, s 21A.
65 TA 2000, s 21A.

above, there is a defence where a person can show that he had a reasonable excuse for not making a disclosure.[66]

Tipping off and prejudicing an investigation

2.114 An offence of 'tipping off' exists under TA 2000 that applies to regulated sector firms and their employees and which is equivalent to that contained in POCA 2002, s 333A.[67] There are two separate offences of tipping off that exist under TA 2000, s 21D. The first is committed where a person has made a disclosure to the NCA, a constable, a firm's nominated officer otherwise in accordance with the firm's internal procedures and the fact that such a disclosure has been made is disclosed to another person, and is likely to prejudice a resulting investigation. The second offence applies where a person discloses that an investigation into a TA 2000 offence is being contemplated or is taking place. The offences are committed only where the information on which the disclosure is based came to the person in the course of regulated sector business and are punishable by imprisonment of up to two years and/or a fine. There are specific provisions under TA 2000 which allow certain specified disclosures to be made in limited circumstances (equivalent to the permissible disclosures provisions under POCA 2002).[68]

2.115 In line with the amendments made to POCA 2002 in 2007, the previous equivalent offence for tipping off that applied to persons outside the regulated sector has been removed. However, the offence of prejudicing an investigation under TA 2000, s 39 remains, which contains an offence applicable where a person outside the regulated sector engages in conduct which is likely to prejudice an investigation. The relevant provision provides that an offence is committed where a person knows or has reasonable grounds to suspect that an investigation into terrorist offences is being, or is proposed to be, conducted, or if the person knows or has reasonable grounds to suspect that a disclosure has been or will be made to the NCA under the disclosure provisions of TA 2000, and the person discloses anything which is likely to prejudice the investigation, or interferes with material that is likely to relevant to an investigation.[69] The offence is punishable by imprisonment for five years and/or a fine. It is a defence for a person to show that he neither knew, nor had reasonable grounds to suspect that, a disclosure or interference would be likely to prejudice an investigation, and a 'reasonable excuse' defence is also available.[70] There is also a defence that allows a legal adviser to make a disclosure to his client in connection with the provision of legal advice, or to any person for the purpose of actual or contemplated legal proceedings, in either case provided that the disclosure is not made with a view to furthering a criminal purpose.[71]

66 TA 2000, s 21A(5)(a).
67 TA 2000, s 21D.
68 See TA 2000, ss 21E–21H.
69 TA 2000, ss 39(2) and 39(4).
70 TA 2000, ss 35(a) and 35(b).
71 TA 2000, s 39(6).

Financial sanctions and asset freezing – overview

2.116 Sanctions of various descriptions are imposed under international and domestic initiatives. These can include trade bans, travel restrictions and arms embargoes. This section focuses on financial sanctions and asset freezing. The UK has in place a range of financial sanctions to give effect to UN and EU sanctions. The UK also has a domestic designation regime. The Foreign and Commonwealth Office is responsible for the policy on international sanctions. The Treasury is responsible for the implementation and control of international financial sanctions in the UK and domestic designated targets as well for licensing exemptions. The Office of Financial Sanctions Implementation (OFSI) is part of HM Treasury and was established under the Policing and Crime Act 2017. The role of OFSI is to ensure that financial sanctions are properly understood, implemented and enforced in the UK. The Policing and Crime Act 2017 provided OFSI with a range of enforcement powers to sanction breaches of financial sanctions. These include the power to impose monetary penalties on offenders. Various trade sanctions are also in place and this regime falls under the responsibility of the Department of Business, Energy & Industrial Strategy. In light of Brexit, The Sanctions and Anti-Money Laundering Act 2018 received Royal Assent in May 2018 to ensure continuity in the sanctions regime in the UK. This will provide the legal framework for the UK's sanctions policy and implementation.

2.117 The UN's powers to impose financial sanctions are derived from Chapter VII of the UN Charter, under which the Security Council can take enforcement measures to maintain or restore international peace and security. The EU's role in relation to financial sanctions comes from the Common Foreign and Security Policy, set out in the Treaty of the EU. The EU applies sanctions to implement UN sanctions, but it may also impose sanctions on a unilateral basis.

2.118 The UK has enacted various legislative provisions to give power to the government to freeze the assets of individuals and other persons in relation to involvement in terrorist and certain other activities. The principal measures are as follows:

- the Counter-Terrorism Act 2008, Sch 7 provides the Treasury with the power to give directions to financial institutions in the UK to cease dealing with designated non-EEA persons for reasons, amongst others, relating to terrorism, money laundering and proliferation financing;
- the Anti-Terrorism Crime and Security Act 2001, Part II confers powers on the Treasury to freeze assets of persons where the Treasury reasonably believes that there is a threat to UK nationals, residents or the economy that emanates from a foreign government or resident. This power is also not confined to terrorism related matters;
- The Al-Qaida and Taliban (Asset Freezing) Regulations 2010[72] give effect to EU level sanctions pursuant to Council Regulation 2580/2001, which

72 SI 2010/1197.

in turn gives effect to UN sanctions imposed under UN Security Council Resolution 1267 (1999);

- The Terrorist Asset-Freezing Act 2010 (TAFA 2010) gives effect to UN Security Council Resolution 1373 (2001). TAFA 2010 replaces earlier Orders made by the UK Government under the United Nations Act 1946, s 1, which were held by the Supreme Court to be ultra vires in the case of *HM Treasury v Ahmed*.[73] The earlier orders were required to be replaced by primary legislation in the form of TAFA 2010.

Counter-Terrorism Act 2008

2.119 The Counter-Terrorism Act 2008 (CTA 2008) confers on the Treasury powers to issue directions to the UK financial sector with regard to business with persons in non-EEA countries and whom the Treasury identifies as posing concern in relation to money laundering, terrorist financing, or proliferation financing. The powers under the CTA 2008 are exercisable in a broad range of circumstances and not just for reasons related to terrorism. For example, the powers under the CTA 2008 have been exercised in circumstances in which Iranian entities have been suspected of involvement in proliferation. The CTA 2008 also gives the Treasury a broader range of powers, such as the power to direct financial institutions to monitor or even cease business relations with particular parties. Accordingly, the CTA 2008 is not concerned exclusively with the freezing of assets. The CTA 2008 was introduced in part owing to concerns that powers set out under the Money Laundering Regulations 2007, which also conferred powers on the Treasury to issue directions to regulated firms, were inadequate. The powers under the 2007 Regulations were only exercisable where FATF had applied counter-measures against a person situated or incorporated in a non-EEA state.

2.120 The CTA 2008, which came into force on 27 November 2008, provides the Treasury with the power, and sets out the conditions under which HM Treasury can exercise such power, to issue direction notices to UK credit institutions and financial institutions. The conditions which the Treasury can impose on those institutions under the CTA 2008 include placing requirements on firms to:

- carry out customer due diligence before entering into or during a business relationship or transaction with designated persons;
- perform ongoing monitoring of a business relationship with designated persons;
- carry out systematic reporting (for example, by providing specified information and documents relating to transactions and business relationships); and

73 [2010] UKSC 2.

- not enter into new business relationships, or cease existing relationships, with designated persons.

2.121 Since the coming into force of the CTA 2008, the power to issue directions has been used on a number of occasions. In October 2009, for example, the Treasury issued the Financial Restrictions (Iran) Order 2009 due to concerns relating to proliferation. This order directed that all persons in the financial sector could not enter into or participate in any transaction or business relationship with Bank Mellat and/or the Islamic Republic of Iran Shipping Lines (IRISL) or their branches. This direction was issued on the grounds that Iran had facilitated the development or production of nuclear weapons. Bank Mellat was stated to have provided banking services to proscribed organisations and IRISL was alleged to have transported parts for Iranian missile and nuclear programmes. This Order was successfully challenged by Bank Mellat, although EU asset freezing restrictions remain in place against the Bank.

2.122 As already noted, reg 18 of the Money Laundering Regulations 2007 also contained a power to issue directions. The Treasury's powers were considered too restrictive, on the basis that it was restricted to situations where FATF had imposed 'counter-measures' (a term that the FATF does not always use in its announcements in relation to specific jurisdiction). Additionally, the pre-existing powers did not address proliferation financing. Therefore, provisions were included in the CTA 2008 to extend the powers of the Treasury in this respect; in particular, the imposition of counter-measures by FATF is not a prerequisite to a direction by the Treasury under the CTA 2008.

2.123 The CTA 2008 sets out provisions dealing with money laundering in Part 5 and provisions relating to financial restriction proceedings in Part 6. The relevant provisions in relation to terrorist financing and money laundering are set out in Sch 7 (which is incorporated into the Act by way of s 62). Schedule 7 comprises eight Parts, and includes: an exposition of the conditions for giving a direction; persons to whom a direction may be given; requirements that may be imposed on relevant persons; procedural provisions; offences; and licensing and enforcement provisions.

2.124 The main offence is set out in para 30 of Sch 7, and is committed where a relevant person fails to comply with a requirement imposed by a direction made under the Schedule. There are two elements to this offence. First, the Treasury may give a direction to:

- a particular person; or
- a description of persons; or
- all 'persons operating in the financial sector'.[74]

74 CTA 2008, Sch 7, para 3.

2.125 A 'person operating in the financial sector' means a 'credit institution' (as defined in Sch 7, para 5(1)) or a 'financial institution' (as defined at para 5(2)) that is a UK person, or when acting in the course of a business carried on by it in the UK, as well as branches of those institutions located in EEA States, or branches of equivalent institutions that have their head office outside the EEA. 'Credit institutions' are, broadly, deposit-taking banks falling under the EU's Capital Requirements Directive (Directive 2013/36/EU). 'Financial Institutions' cover a broad range of institutions including investment firms, certain money service businesses and insurers. Certain insurers (broadly, those engaged in general insurance) are excepted from the application of certain directions under Sch 7, paras 10(5) and 11(4).

2.126 The Treasury may give a direction in relation to any country (other than an EEA State) under one (or more) of three circumstances where:

- FATF has advised that measures should be taken because of the risk of terrorist financing or money laundering being carried on in the country, by the government of the country, or by persons resident/incorporated in the country; or
- the Treasury holds a reasonable belief that there is a risk of terrorist financing or money laundering being carried on in the country, by the government or by persons resident/incorporated in the country and that this poses a significant risk to the UK's national interests; or
- the Treasury holds a reasonable belief that the development or production of nuclear, radiological, biological or chemical weapons in the country, or the doing of anything in the country that facilitates the development or production of any such weapons, poses a significant risk to the UK's national interests.[75]

2.127 Money laundering in the CTA 2008 is defined by reference to POCA 2002, s 340(11). The terrorist financing definition is, however, different from the definition contained in the TA 2000, and is defined in CTA 2008 as:

> 'the use of funds, or the making available of funds, for the purposes of terrorism, or the acquisition, possession, concealment, conversion or transfer of funds that are (directly or indirectly) to be used or made available for those purposes'.[76]

2.128 A direction may be imposed in respect of transactions or business relationships with a person carrying on business in the country, the government of the country, or a person resident or incorporated in the country.[77]

2.129 The second element of the main offence provided for under Sch 7 is a failure to comply with the requirements imposed by a direction. There are

75 CTA 2008, Sch 7, para 1.
76 CTA 2008, Sch 7, para 2.
77 CTA 2008, Sch 7, para 9.

four requirements which could be imposed on a person. First, the Treasury may order that a financial institution conducts enhanced CDD before entering into or during a transaction or business relationship with a designated person. The onus is on the relevant financial institution to assess the risk of the designated person being involved in relevant activities. Second, the Treasury may order that a financial institution conduct enhanced ongoing monitoring of any business relationship with a designated person. Part of this requirement includes keeping the CDD information up to date and scrutinising transactions. Third, the Treasury may impose an obligation on a relevant person to provide information and documents relating to transactions and business relationships with designated persons at certain intervals, as prescribed. This requirement must be proportionate and the direction must explain how it is to be complied with, and highlight persons to whom information and documents must be provided. A current question however, is whether the relevant financial institution would be required to provide privileged documents or confidential information.

2.130 Fourthly, the Treasury may give a direction for the relevant person or persons not to enter into or continue to participate in a specified business relationship or transaction.[78] On its face, this is the most draconian of the powers contained in Sch 7 but, where a direction to this effect is given, HM Treasury may grant a licence to exempt acts specified in the licence from the requirements under the direction; a licence may be a general licence, or may be granted to a particular person or description of persons.[79]

2.131 There is a defence to the offence of failing to comply with a requirement. This is that the defendant took all reasonable steps and exercised all due diligence to ensure that the direction should be complied with.[80] There is also a provision equivalent to those under POCA 2002 and TA 2000, which provides that in proceedings relating to an alleged offence, the court must have regard as to whether the person complied with any guidance approved by HM Treasury. The offence is punishable by two years' imprisonment and/or a fine. Should the offence be committed *by* a body corporate*, officers of the body corporate* can be concurrently liable *if* the offence *was* committed with *their* consent or connivance, or which can be attributed to *their* neglect.[81]

2.132 Under the CTA 2008, Sch 7, para 15, where the Treasury issues a direction to a particular firm, notice of the direction is required to be given to that person. Where the direction is of broader application, for example, to the banking and financial sector generally or to a group of firms, the direction is required to be set out in an order which must be laid before Parliament. The making of the order must be publicised.

78 CTA 2008, Sch 7, paras 10–13.
79 CTA 2008, Sch 7, para 17.
80 CTA 2008, Sch 7, para 30(2).
81 CTA 2008, Sch 7, para 36.

2.133 There is a separate offence under Sch 7 that is committed where, for the purpose of obtaining a licence from HM Treasury in circumstances where a direction has been issued restricting the carrying on of business with a person, the person attempting to obtain a licence knowingly or recklessly provides information that is false in a material respect or provides a document that is not what it purports to be. This offence is also punishable by up to two years' imprisonment and/or a fine.[82]

2.134 Jurisdiction is provided for proceedings to be taken in the UK in relation to offences committed under Sch 7 outside the UK.[83] Schedule 7 to the CTA 2008 also provides for civil enforcement penalties to be imposed by enforcement authorities.[84] Additionally, the FCA and HMRC are appointed under the CTA 2008 as Supervisory Authorities responsible for monitoring persons operating in the financial sector. The FCA is responsible for authorised credit institutions and financial institutions (except money service businesses that are not authorised by the FCA) and HMRC is responsible for money service businesses that are not FSMA 2000 authorised persons.[85]

2.135 The CTA 2008 also contains provisions relating to financial restriction proceedings in Part 6. Under Part 6, any person affected by a decision of the Treasury in connection with the exercise of any of their functions under Part 2 of the Anti-terrorism, Crime and Security Act 2001 (freezing orders), or Sch 7 to the CTA 2008 (terrorist financing, money laundering and certain other activities: financial restrictions) may apply to set aside the direction. In determining whether to set aside the direction, the court may apply judicial review principles and may ultimately quash the Treasury direction.

Freezing assets

2.136 Another closely related measure used in the UK to combat terrorist financing is the freezing of terrorist assets. The powers to forfeit and/or freeze terrorist assets have been enhanced by the Anti-Terrorism, Crime and Security Act 2001. Under s 4 of the 2001 Act, the Treasury has the power to make freezing orders either against overseas governments or persons resident overseas whom the Treasury reasonably believes have taken, or are likely to take, action to the detriment of the UK's economy, or who constitute a threat to the life or property of UK nationals or residents.[86] The freezing orders may name individual persons or describe such persons and will bind all persons in the UK and UK nationals (including companies) overseas. Orders made under this power are limited in duration of up to two years.

82 CTA 2008, Sch 7, para 31.
83 CTA 2008, Sch 7, para 34.
84 CTA 2008, Sch 7, para 25.
85 CTA 2008, Sch 7, para 39.
86 Anti-Terrorism, Crime and Security Act 2001, s 4.

Landsbanki Freezing Order 2008

2.137 A notable case of the UK Government exercising this power was on 8 October 2008, when the Government passed the Landsbanki Freezing Order 2008 (the Landsbanki Order), thereby freezing an estimated £4 billion of British assets belonging to the Icelandic bank Landsbanki Island hf, some of them held by the Icelandic Financial Services Authority, the Central Bank of Iceland and the Government of Iceland.

2.138 The Landsbanki Order was passed the day after Landsbanki and its online branch were placed in receivership, and was a precautionary measure taken by the British Government after it had failed to obtain assurances that an estimated 300,000 UK savers with deposits at Icelandic banks would receive compensation from the Icelandic Government on an equal footing with Icelandic depositors. As a result of the Landsbanki Order, no person in the UK could release or deal with the frozen assets without a licence from the Treasury. Anyone who held assets that had been frozen by the Landsbanki Order was required to inform the Treasury and provide it with all relevant information necessary for ensuring compliance.

2.139 The passing of the Landsbanki Order however, has raised some wider concerns around the use of the Anti-Terrorism, Crime and Security Act 2001. Whilst the Landsbanki Order was strictly within the law, which itself was widely drafted, it was considered in some quarters as a signal that the UK Government can, and may in the future, invoke legislation for entirely different purposes than those for which it was adopted. Not only could the Anti-Terrorism, Crime and Security Act 2001 be used in future against other financial institutions, but this turn of events may have opened the way for it to be used more widely to protect the UK's commercial and political interests, rather than concerns over terrorism. The Landsbanki Order was subsequently revoked by the Landsbanki Freezing (Revocation) Order 2009.

Financial sanctions

Introduction

2.140 In recent years, the UK has increasingly legislated to combat terrorism and behaviour by 'rogue states' through the imposition of financial sanctions. The UK's financial sanctions regimes derive from UN Security Council Resolutions and also the EU financial sanctions regimes. Broadly, there are three main offences covered under the UK sanctions regimes:

- making funds available either directly or indirectly to or for the benefit of a target;
- dealing with funds owned, held or controlled, directly or indirectly by a target, or a person acting on behalf of a target;

- knowingly and intentionally participating in activities to directly or indirectly circumvent the prohibitions on making funds available and dealing with funds; or to enable or facilitate the commission of the above offences.

The international framework

2.141 Under the UN Charter the UN's Security Council can take action to maintain or restore international peace and security. Under art 41 of the UN Charter, the Security Council may decide on the measures, not involving the use of armed force, that are to be employed to give effect to its decisions. This gives the power to the UN's Security Council to impose a broad range of sanctions. These can include matters such as arms embargoes and travel bans as well as financial sanctions. The international framework for imposing financial sanctions is founded largely on UN Security Council Resolutions 1267 (1999) 1333 (2000), 1373 (2001), 1390 (2002), and 1452 (2002). In December 1994 the General Assembly of the UN passed a resolution approving a Declaration of Measures to Eliminate International Terrorism. This was directed at the role of states in supporting terrorist activities. An International Convention for the Suppression of the Financing of Terrorism was agreed in December 1999 which was also directed at the financing of terrorism. Since then, international sanctions have become more sophisticated and 'smarter' as they become directed at individuals and entities as opposed to states. UN Security Council Resolution 1267 (1999) required Member States to freeze the funds and other financial resources owned or controlled directly or indirectly by the Taliban regime. While aimed at the Taliban regime, a Sanctions Committee was established for the purpose of designating parties whose funds were to be frozen. Resolution 1267 was supplemented by UN Security Council Resolution 1333 (2000) which expanded the scope of sanctions under Resolution 1267 to cover the assets of Osama Bin Laden and individuals and entities associated with him. UN Security Council Resolution 1373 (2001), passed in the aftermath of the 11 September 2001 terrorist attacks, requires States to freeze terrorist assets.

2.142 The EU has the power under Treaties to adopt sanctions on behalf of Member States and it has done so through Council Regulation 2580/2001. The Terrorist Asset-Freezing etc Act 2010 implements in the UK the terrorist asset freezing requirements of UNSC Resolution 1373 (2001). The Al Qaida and Taliban (Asset Freezing) Regulations 2010 establish criminal penalties for breaches of sanctions made under Council Regulation (EU) No 2580/2001.

2.143 Enforcement action taken in the US and in the UK has highlighted the compliance risks in this area. In 2009 Lloyds TSB agreed to pay the US authorities US$350 million in respect of alleged breaches of US sanctions requirements. In the UK in August 2010 the FSA fined members of the RBS Group £5.6 million for systems and controls failing in relation to financial sanctions.

UK sanctions regimes

2.144 The UK list of financial sanctions targets has expanded greatly since 2001, and in the UK, responsibility for the overall implementation and supervision of the financial sanctions regime has been transferred from the Bank of England's Financial Sanctions Unit to the Asset Freezing Unit at HM Treasury and now to OFSI. There are currently 31 different sanctions 'regimes' in place that fall within the jurisdiction of the Treasury. The relevant regimes, which target 'designated parties', 'restricted parties' and 'blacklisted parties', are:

- Afghanistan;
- Belarus;
- Burma;
- Burundi;
- Central African Republic;
- chemical weapons;
- Democratic Republic of Congo;
- Egypt;
- Eritrea;
- financial sanctions, UK freezing order;
- Iran (Human Rights);
- Iran (Nuclear Proliferation);
- Iraq;
- Lebanon and Syria;
- Libya;
- Mali
- North Korea (Democratic People's Republic of Korea);
- Republic of Guinea;
- Republic of Guinea-Bissau;
- Republic of Maldives;
- Somalia;
- South Sudan;
- Sudan;
- Terrorism and terrorist financing;
- The ISIL (Da'esh) and Al-Qaida organistions;
- Tunisia;

- Ukraine (misappropriation);
- Ukraine (sovereignty);
- Venezuela;
- Yemen;
- Zimbabwe.

The different regimes are governed by different statutory instruments, and directions made thereunder. However, a consolidated list of the persons designated as targets under the above regimes is maintained and regularly updated by the Treasury and can be found on the HM Treasury website.

UK financial sanctions legislation – terrorism

2.145 The principal piece of financial sanctions legislation that relates to terrorist financing is TAFA 2010. Under the TAFA 2010 the Treasury has the power to issue a direction to designate a person if specific conditions are fulfilled and the Treasury considers that the direction is necessary to protect members of the public from a risk of terrorism. The conditions are that the Treasury must have reasonable grounds to suspect that the person is:

- a person who commits, attempts to commit, participates in or facilitates the commission of acts of terrorism;
- a person owned or controlled, directly or indirectly, by a designated person; or
- a person acting on behalf of or at the direction of a designated person.

2.146 Additionally, the Treasury must consider that the direction is necessary for purposes connected with protecting the public from a risk of terrorism. 'Designated persons' for the purposes of the TAFA 2010 also include persons identified pursuant to art 2(3) of Council Regulation (EC) No 2580/2001. Persons who are designated under the TAFA 2010 can take advantage of the right to apply to have the direction set aside, provided for under the CTA 2008.

2.147 The TAFA 2010 imposes various restrictions on dealing with designated persons. The restrictions imposed include prohibitions on:

- dealing with funds or economic resources owned, held or controlled by a restricted person ('dealing' being widely defined);[87]
- making funds or financial services available, directly or indirectly, to a restricted person, or to another person for the benefit of a restricted person;[88] and

87 TAFA 2010, s 11.
88 TAFA 2010, s 12.

- making economic resources available, directly or indirectly, to a restricted person, or to another person for the benefit of a restricted person.[89]

2.148 A person who contravenes any of the prohibitions contained in the TAFA 2010, ss 11–15 is guilty of a criminal offence (unless he can show that he did not know and had no reasonable cause to suspect that he was dealing with funds or economic resources of, or making funds, economic resources or financial services available to, restricted persons). A person found guilty of such an offence will be punishable by up to seven years' imprisonment and/or a fine.

2.149 There is an exception provided which enables 'relevant institutions' (being, broadly, FCA and PRA authorised persons and EEA authorised persons that have obtained permission to operate in the UK) to credit frozen accounts with interest or other earnings due on the account.[90] Additionally, relevant institutions are also able to credit a frozen account with payments due under agreements, contracts or obligations that were concluded or arose before the account was frozen, and to credit a frozen account where it receives funds transferred to a frozen account by a third party; in such circumstances, the institution must inform HM Treasury without delay if it does so.[91]

2.150 The TAFA 2010 (in line with statutory instruments under other UK sanctions regimes) also contains provisions that require relevant institutions (for example, regulated firms with permission under the FSMA 2000, Part IV) to inform the Treasury as soon as practicable if they know or suspect that a current customer, a person who has been a customer within the five years prior to the relevant Treasury direction being given, or a person with whom the institution has had dealings in the course of business during that period, is a restricted person.[92]

2.151 The TAFA 2010 also contains a licensing regime, which allows the Treasury to license exemptions from the prohibitions contained in ss 11–15.[93] A licence granted under the Act can be general in application, or be granted to a particular person or category of persons, and can be of fixed or indefinite duration, and subject to conditions or otherwise. The Treasury has the power to vary or revoke a licence at any time. The Treasury advises that any person wishing to apply for a licence authorising an exemption from the prohibitions should apply to the Asset Freezing Unit, clearly setting out the grounds on which the licence is sought, and providing full details and supporting evidence.

2.152 There are two offences provided for in connection with licensing. The first offence is committed where a person knowingly or recklessly either provides materially false information for the purpose of obtaining a licence, or

89 TAFA 2010, s 13.
90 TAFA 2010, s 16(1)(a).
91 TAFA 2010, s 16(1)(b), 16(2), 16(4).
92 TAFA 2010, s 19.
93 TAFA 2010, s 17.

provides or produces a document that is not what it purports to be.[94] The second is committed where any person purporting to act under the authority of a licence fails to comply with any conditions included in the licence. Both offences are punishable by imprisonment for up to two years and/or a fine.

2.153 There is a further general offence contained in the TAFA 2010, s 18, which is committed by any person who knowingly and intentionally participates in activities the object or effect of which is, directly or indirectly, to circumvent a prohibition in ss 11–15 or to enable or facilitate the contravention of such a prohibition.[95] Should an offence under the TAFA 2010 be committed by a body corporate, officers of the body corporate can be concurrently liable if the offence was committed with their consent or connivance, or which can be attributed to their neglect.[96]

Obligations on FCA and PRA regulated firms

2.154 As set out further below, FCA and PRA regulated firms are subject to requirements under the rules applicable to those firms. At the time of legal cut over from the FSA to the FCA and PRA, the former FSA Handbook was split between the FCA and the PRA to form two new Handbooks of Rules and Guidance, one for each of the new regulations. However, the FCA is the conduct regulator for all firms, whether solo or dual-regulated. Financial crime issues are therefore primarily the responsibility of the FCA. Under provisions contained in the FCA's Senior Management Arrangements Systems and Controls part of the FCA Handbook (SYSC), 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.[97]

2.155 Chapter 7 of the FCA's Financial Crime Guide (contained in the FCA's Handbook of Rules and Guidance) specifically addresses issues relating to financial sanctions. In this the FCA state that all firms are required to comply with the UK's financial sanctions regime. The FCA's role is to ensure that the firms it supervises have adequate systems and controls to do so. The FCA states that Chapter 7 applies to all firms subject to the financial crime rules in SYSC 3.2.6R or SYSC 6.1.1R. It also applies to e-money institutions and payment institutions within the FCA's supervisory scope. The FCA goes on to state that firms' systems and controls should also address, where relevant, the risks they face from weapons proliferators. These risks are greatest for banks carrying out trade finance business and those engaged in other activities, such as project finance and insurance.

94 TAFA 2010, s 17(6).
95 TAFA 2010, s 17(7).
96 Terrorism (United Nations Measures) Order 2009, SI 2009/1747, art 20.
97 FCA Handbook, SYSC 3.2.6R.

2.156 Screening for financial sanctions compliance purposes is not a legal requirement, though a failure to do so may result in the firm contravening financial sanctions requirements and thereby committing a criminal offence. At FCG 7.2.3 the FCA states that firms should have effective, up-to-date screening systems appropriate to the nature, size and risk of their business. The FCA acknowledges that screening itself is not a legal requirement. However, they note that screening new customers and payments against the Consolidated List, and screening existing customers when new names are added to the list, helps to ensure that firms will not breach the sanctions regime.

THE FOURTH MONEY LAUNDERING DIRECTIVE

2.157 As indicated above, many recent changes in the UK's legal and regulatory framework have been derived from the EU's AML Directives. In turn, European level money laundering legislation has essentially tracked the FATF's Recommendations. The original FATF 40 Recommendations were issued in April 1990 and these were followed by the Council Directive 91/308/EEC (the First AML Directive). The First AML Directive was concerned principally with the prohibition of money laundering in relation to drugs trafficking offences and the imposition of AML compliance obligations on banks and other financial institutions.

2.158 FATF's Recommendations were revised in 1996 and an amending Directive, Directive 2001/97/EEC (the Second AML Directive), was issued in 2001. The Second AML Directive broadened the range of predicate offences to cover organised crime, fraud against the EU, corruption and serious crimes (ie going well beyond drugs trafficking) and to impose AML compliance obligations on sectors outside the banking and financial sector. FATF further revised its Recommendations in 2003 and a major objective of the Third AML Directive was to update European AML legislation to bring it in line with these revisions.

2.159 As already mentioned above, the UK AML regime now implements the EU's Fourth AML Directive. The MLR 2017 came into force in the UK on 26 June 2017, the Directive's transposition deadline. A number of key changes were introduced by the Fourth AML Directive. These included:

- the Directive specifically referred to tax crimes as constituting a predicate offence for money laundering purposes;
- the scope of application to high value goods dealers was changed to include a broader category to cover those accepting cash of €10,000;
- the application of the regulated sector was also expanded in the case of estate agents (to include performing due diligence on the buyer as well as seller) and the gambling sector (to include all gambling services and not just casinos);
- a specific requirement was introduced for firms to prepare a risk assessment;

- a person from senior management would need to be appointed as responsible for the AML issues within the firm;
- staff vetting or screening would need to be carried out;
- an internal audit of AML activities was mandated;
- customer due diligence measures were changed in many respects ruling out the carrying on of simplified due diligence. The Directive removed the default ability to apply simplified due diligence measures to certain clients with firms needing to carry out an assessment of risk and categorisation of clients on an individual basis;
- the Directive required Member States to create a directory of the beneficial owners of corporate entities incorporated in their countries;
- the definition of politically exposed person was changed to include domestic politically exposes persons (PEPs);
- the 'White List' of countries with equivalent AML laws was withdrawn meaning that firms must perform their own assessment of equivalent jurisdictions.

THE MONEY LAUNDERING REGULATIONS

Introduction to the Money Laundering Regulations

2.160 The Money Laundering Regulations 2017, which came into force on 26 June 2017, give effect in the UK to the EU's Fourth Money Laundering Directive, which is Europe's implementation of FATF's 40 Recommendations and seeks to achieve a harmonised approach to AML and CTF across Europe.

2.161 The MLR 2017 impose five main duties or obligations on firms and importantly legally enshrines the concept of a 'risk-based approach'. Regulation 18 specifically requires firms to prepare a written risk assessment which must take the EU and UK risk assessments into consideration. The other main requirements are:

- *customer due diligence measures*: firms are required to carry out customer due diligence measures on a risk-sensitive basis. These measures must involve the identification and verification of customers and beneficial owners. Firms must also obtain information regarding the purpose and intended nature of the business relationship.
- *Internal polices, controls and procedures* – Firms must develop and maintain adequate and appropriate policies, controls and procedures to mitigate money laundering risks.
- *Record keeping* – Firms must make and retain records of their customer due diligence measures and transactions carried out by the firm, as evidence that they have complied with their legal and regulatory obligations.

- *Suspicious transactions and reporting procedures* – Firms must ensure that suspicious transactions are identified and reported to the firm's MLRO, who may report the incident to NCA.
- *Education and training to employees* – Firms must ensure that employees are adequately trained to identify suspicious transactions and are aware of the firm's money laundering risks.

Each of these duties is considered further below in this Chapter and also in Chapter 3 which outlines in more detail the requirements under the MLR and discusses the JMLSG Guidance.

Scope of the Regulations

2.162 The offences under POCA 2002 apply to all persons. The MLR 2017, on the other hand, are limited in scope applying to persons engaged in certain types of activities. The rationale for this is that the specified sectors are more likely to be involved in money laundering. The MLR 2017 apply to 'relevant persons', who are the following persons acting in the course of business carried on by them in the UK:

(a) credit institutions (as defined in reg 10(1));

(b) financial institutions, which includes money service businesses (as defined in reg 10(2));

(c) auditors, insolvency practitioners, external accountants and tax advisers;

(d) independent legal professionals, when participating in financial or real property transactions concerning

  (i) the buying and selling of real property or business entities;

  (ii) the managing of client money, securities or other assets;

  (iii) the opening or management of bank, savings or securities accounts;

  (iv) the organisation of contributions necessary for the creation, operation or management of companies; or

  (v) the creation, operation or management of trusts, companies and similar structures;

(e) trust or company service providers, being persons who provide the following services to others:

  (i) forming companies or other legal persons;

  (ii) acting or arranging for another person to act as a director/secretary of a company, a partner of a partnership, or a similar position for other legal persons;

(iii) providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or arrangement;

(iv) acting, or arranging for another person to act, as:

(A) a trustee of an express trust or similar legal arrangement; or

(B) a nominee shareholder for a person other than a company whose securities are admitted to trading on a regulated market.

(f) estate agents (as defined in reg 13);

(g) high value dealers being a firm or sole trader who by way of business trades in goods (including auctioneers), who accept cash payments, in respect of any transaction, of €10,000 or more (whether the transaction is executed in a single operation or in a series of operations that appear to be linked); and

(h) casinos, being the holder of a casino operating licence.

Customer due diligence

2.163 The MLR 2017 require firms to carry out customer due diligence measures when they:

- establish a business relationship;
- carry out an occasional transaction that amounts to the transfer of funds within the meaning of art 3.9 of the Funds Transfer Regulations exceeding €1,000 or more or (other than for high value dealers and casinos) for occasional transactions that amount to €15,000 or more where they appear to be linked;
- suspect money laundering or terrorist financing; or
- doubt the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.[98]

More detailed provisions apply in relation to the performance of customer due diligence by high value dealers and casinos as specified in reg 27(3)–(7). Additionally, firms must apply customer due diligence measures on a risk-sensitive basis at 'other appropriate times'.[99]

2.164 The precise nature of the customer due diligence measures that firms must apply are outlined in further detail in Chapter 3. However, broadly, a firm must:

98 MLR 2017, reg 27.
99 MLR 2017, reg 27(8).

- identify the customer and verify the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
- identify, where there is a beneficial owner who is not the customer, the beneficial owner and take reasonable measures to verify the identity of the beneficial owner so that the firm is satisfied that it knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, taking measures to understand the ownership and control structure of the person, trust or arrangement; and
- obtain information on the purpose and intended nature of the business relationship.[100]

Beneficial owner

2.165 Broadly, a 'beneficial owner' is a person that has a 25% or higher interest in the customer, or any other person on whose behalf a transaction or activity is carried out. Regulations 5 and 6 set out the definition of a 'beneficial owner'. The definition appears capable of capturing significant clients of customers as well as owners or controllers of customers. However, as set out above, it is not necessarily clear whether indirect clients should properly be treated as customers or as beneficial owners by a firm. In any event, it is submitted that due diligence measures should be carried out on direct customers of the firm, the owners/controllers of the firm and known indirect customers of the firm.

Customer

2.166 Whilst the MLR 2017 provide a list of circumstances in which CDD must be carried out, the absence of certain definitions can cause potential problems. For instance, the term 'customer' is not defined in the MLR 2017, and the JMLSG Guidance offers little further by way of assistance in this respect, stating only that, in the absence of a specific definition in the MLR 2017, the definition must be inferred from the definitions of 'business relationship' and 'occasional transaction'. The former is defined by the MLR 2017 as a business, commercial or professional relationship between a firm and a customer, which arises out of the firm's business and is expected by the firm when contact is established to have an element of duration.[101] An 'occasional transaction' is defined as any transaction that is not carried out as part of a business relationship.[102]

2.167 However, these definitions, whilst helpful, do not appear to answer all the possible questions as to whom a firm must classify as its 'customers'. For instance, it is not explicitly clear (although, following a cautious approach,

100 MLR 2017, reg 28.
101 MLR 2017, reg 4.
102 MLR 2017, reg 3(1).

arguably it should be assumed) that the client of a customer should also be treated by a firm as its customer, and due diligence measures applied, or whether such a person would more accurately be characterised as a 'beneficial owner' (as discussed further below). The JMLSG Guidance suggests that the definition for MLR 2017 purposes may be wider than the definition used in the FCA Handbook Glossary, and that the ordinary dictionary definition may also assist. The safest approach would be to admit the broadest possible definition; however, requiring due diligence information from customers' clients may prove difficult to achieve in practice.

2.168 As well as the requirement that customer due diligence measures be carried out at the outset of a business relationship or prior to carrying out an occasional transaction, the MLR 2017 also require measures to be applied when there is doubt as to previous information supplied, or where there is reason to suspect money laundering or terrorist financing. Additionally, measures are to be applied on a 'risk-based basis' at 'other appropriate times'.[103] The MLR 2017 also require a firm to keep the information it holds on customers up-to-date. It is clear, therefore, that the obligation on firms to ensure that they know who their clients are is an on-going one. The frequency of applying due diligence measures over the course of the relationship can be determined in line with the firm's risk-based approach, the concept of which is a central approach taken under the MLR 2017 and the Fourth Money Laundering Directive (and which is consistent with the latest 40 Recommendations used by FATF). This is discussed further in Chapter 3.

Casinos

2.169 The MLR 2017 apply to persons who operate a casino by way of business. Casinos must apply customer due diligence measures in relation to any transaction identified below that amounts to €2,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked. These transactions are:

- the wagering of a stake, including:
  - (i) the purchase from, or exchange with, the casino of tokens for use in gambling at the casino;
  - (ii) payment for use of gaming machines (within the meaning of the Gambling Act 2005, s 235); and
  - (iii) the deposit of funds required to take part in remote gambling; or
- the collection of winnings, including the withdrawal of funds deposited to take part in remote gambling (within the meaning of the Gambling Act 2005, s 4) or winnings arising from the staking of such funds.

103 MLR 2017, reg 27(8).

Simplified due diligence

2.170 Regulation 37 of the MLR 2017 provides that a simplified due diligence (SDD) procedure may be carried out in relation to a particular business relationship or transaction if the firm determines that the business relationship or transaction presents a low degree of risk of money laundering and terrorist financing.

2.171 SDD is not a derogation from the need to perform customer due diligence measures. The MLR 2017 are clear that where applying SDD firms must continue to comply with customer due diligence requirements under reg 28 but that firms can adjust the extent, timing or type of measures that the firm undertakes. Firms applying SDD are also required to carry out sufficient monitoring of any business relationship or transactions which are subject to those measures, to enable firms to detect unusual or suspicious transactions.

2.172 The criteria to which firms must have regard in determining whether to apply SDD are:

(i) the firm's risk assessment carried out under reg 18(1);

(ii) relevant information made available to the firm by regulators or other bodies under regs 17(9) and/or 47; and

(iii) the following risk factors:

- customer risk factors including whether the customer:
  - — is a public administration, or a publicly owned enterprise;
  - — is an individual resident in a geographical area of lower risk;
  - — is a credit institution or a financial institution which is:
    - (A) subject to the requirements in national legislation implementing the Fourth AML Directive as an obliged entity (within the meaning of that directive), and
    - (B) supervised for compliance with those requirements in accordance with section 2 of Chapter VI of the Fourth AML Directive;
  - — is a company whose securities are listed on a regulated market, and the location of the regulated market;
- product, service, transaction or delivery channel risk factors including whether the product or service is:
  - — a life insurance policy for which the premium is low;
  - — an insurance policy for a pension scheme which does not provide for an early surrender option, and cannot be used as collateral;
  - — a pension, superannuation or similar scheme which satisfies the following conditions:

(A) the scheme provides retirement benefits to employees;

(B) contributions to the scheme are made by way of deductions from wages; and

(C) the scheme rules do not permit the assignment of a member's interest under the scheme;

— a financial product or service that provides appropriately defined and limited services to certain types of customers to increase access for financial inclusion purposes in an EEA state;

— a product where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership;

— a child trust fund within the meaning given by the Child Trust Funds Act 2004, s 1(2);

— a junior ISA within the meaning given by the Individual Savings Account Regulations 1998, reg 2B;

- geographical risk factors including where the customer is resident, established or registered or in which it operates is:

  — an EEA state;

  — a third country which has effective systems to counter money laundering and terrorist financing;

  — a third country identified by credible sources as having a low level of corruption or other criminal activity, such as terrorism (within the meaning of the TA 2000, s 1), money laundering, and the production and supply of illicit drugs;

  — a third country which, on the basis of credible sources, such as evaluations, detailed assessment reports or published follow-up reports published by the FATF, the IMF, the World Bank, the OECD or other international bodies or nongovernmental organisations:

    (A) has requirements to counter money laundering and terrorist financing that are consistent with the revised Recommendations published by the FATF in February 2012 and updated in October 2016; and

    (B) effectively implements those Recommendations.

Enhanced due diligence

2.173 In addition to carrying out customer due diligence measures, the MLR 2017 also require firms to apply enhanced due diligence measures (EDD) to a number of situations:

- where there is a high risk of money laundering or terrorist financing;
- in any business relationship or transaction with a person established in a high-risk country;
- in relation to correspondent relationships with credit institutions or financial institutions;
- where it is determined that a customer is a PEP, or a family member or known close associate of a PEP;
- in any case where a customer provides false or stolen identification documents or information, and the relevant person proposes to continue to deal with that customer;
- where a transaction is complex and unusually large or there is an unusual pattern of transactions, and the transaction or transactions have no apparent economic or legal purpose; or
- in any other case which by its nature can present a higher risk of money laundering or terrorist financing.
- where EDD is to be applied, the firm must perform the following additional measures:

  (i) examine the background and purpose of the transaction,

  (ii) increase the degree and nature of monitoring of the business relationship in which the transaction is made;

  (iii) seek additional independent, reliable sources to verify information provided or made available;

  (iv) take additional measures to understand better the background, ownership and financial situation of the customer, and other parties to the transaction;

  (v) take further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship; and

  (vi) increase the monitoring of the business relationship, including greater scrutiny of transactions.

Record keeping

2.174 The MLR 2017 require firms to make and keep records relating to their customer due diligence measures, that is, customer identification and verification procedures, and transactions carried out by the firm, as evidence that they have complied with their legal and regulatory obligations. Such evidence may also be used in any investigations conducted by the law enforcement bodies. The general rule is that all records must be retained for the 'prescribed period' of five years from the date the file is closed. Normal banking practice is to maintain ledger entries for longer than this (six years for accounting purposes).

Internal reporting procedures

2.175 The MLR 2017 require firms to ensure that any suspicious transactions identified are reported internally by staff to the firm's MLRO who must then determine whether it gives rise to knowledge or suspicion or reasonable grounds for such knowledge or suspicion. Where such knowledge or grounds of suspicion are considered to exist, the MLRO must report such suspicious activity to NCA.

Training

2.176 The MLR 2017 require firms to take appropriate measures to ensure that:

- all employees are aware of the risks of money laundering and terrorist financing the relevant legislation, and their obligations under that legislation;
- all employees are all given regular training in how to recognise and deal with suspicious transactions, and other activities or situations, that may be related to money laundering or terrorist financing; and
- the firm maintains written records of the measures taken under the two points above.

Registration requirements

2.177 Under the 2003 Money Laundering Regulations, HMRC was required to maintain a register of money service businesses and high-value dealers. This obligation continues under the MLR but has also been extended to include trust or company service providers. The result is that money service business, high-value traders and trust or company service providers must apply to HMRC to be registered. Applications must be made in the form required and contain the information requested by HMRC. Such information may include:

- the applicant's name and name of business;
- the address of the applicant's head office with its company number (in the case of a company), and of any UK branches the applicant has;
- the nature of the business;
- the name of the nominated officer;
- in relation to a money service business or trust or company service provider:
  - (i) the name of any person who effectively directs the applicant and any beneficial owner of the business; and
  - (ii) information required by HMRC to decide whether they must refuse the application on the grounds that the money service business or trust or company service provider is not fit and proper; and

(iii) such additional information as HMRC considers reasonably necessary to assist the determination of the application.

2.178 Applications for registration as a money service business or trust or company service provider are subject to the applicant satisfying the fit and proper test set out in the MLR 2017, reg 58. To satisfy the fit and proper test, each of the following people (where applicable) must meet the criteria set out in the MLR 2017, reg 58(3)–(4) (that is, each of the following people, must be fit and proper):

- the applicant;
- a person who effectively directs the applicant;
- a beneficial owner of the applicant; or
- the nominated officer of the application.

HMRC must notify an applicant of its decision within 45 days of receipt of the application, or where relevant, receipt of additional information requested.

2.179 HMRC also has powers under the MLR 2017 to cancel an existing registration. For example, HMRC is required to cancel a registration where HMRC determines that a person referred to in the MLR 2017, reg 58 is not a fit and proper person. Additionally, HMRC may also cancel a registration where it appears that HMRC would have had grounds to refuse the initial registration, for example, because information contained in the application was false or misleading.

Failure to comply with the MLR 2017

2.180 Failure to comply with the requirements of the MLR 2017 is a criminal offence which is punishable with up to two years' imprisonment, a fine or both. This offence is committed irrespective of whether any money laundering has taken place. It is also important to understand that in practice, where an offence is committed by a body corporate or partnership, for example, an offence may also have been committed by a director of the company or partner of the partnership. This will be the case where an offence is committed by a body corporate with the consent or connivance of an officer of the body corporate or can be attributed to neglect on the part of the director.

2.181 Failure to comply with the requirements of the MLR 2017 may also give rise to civil penalties imposed by the relevant supervisory authorities. We discuss the supervisory authorities further below.

2.182 The MLR 2017 provide that, in determining whether a person has complied with the requirements, the court may take account of any relevant supervisory or regulatory guidance. By far the most significant and widely followed guidance is that provided by the JMLSG. The JMLSG Guidance Notes provide guidance

regarding the UK's AML/CFT framework and interpret the requirements which firms are required to comply with under the MLR 2017. Although, importantly, failure to follow the JMLSG Guidance does not mean that a firm has breached the MLR 2017. Rather a firm must prove that it has complied with the duties under the MLR 2017. Compliance with the Guidance Notes, however, would be one means of proving a firm's compliance with the requirements under the MLR 2017. The Guidance Notes are discussed in further detail in Chapter 3.

Supervisory authorities

2.183 Supervision and monitoring of compliance with MLR 2017 is undertaken by a number of bodies. In particular, and as further discussed in Chapter 3, the MLR 2017 designate certain bodies, such as the FCA, HMRC and certain professional bodies, for example, the Law Society, as 'supervisory authorities' and impose requirements on these bodies to monitor the firms they supervise and, where necessary, to adopt measures to ensure compliance by those firms with the requirements of the MLR 2017.

THE ROLE OF THE FCA

2.184 The FCA's 'Integrity Objective' financial crime objective requires it to reduce the extent to which the financial services sector can be used for purposes connected with financial crime.[104] Money laundering falls within the scope of the FCA's 'Integrity Objective' given that 'financial crime' is defined as including the handling of the proceeds of crime.

Summary

2.185 Systems and controls requirements in SYSC relating to money laundering and financial crime are justified by the FCA on the basis that a failure by a regulated firm to manage money laundering risk effectively will increase the risk to society of crime and terrorism. The FCA notes in SYSC 6.3.4G that aside from the requirements of SYSC firms may also have separate obligations to comply with relevant legal requirements, including the TA 2000, POCA 2002 and the MLR 2017.

2.186 Systems and controls requirements relating to financial crime (including money laundering) were originally contained in SYSC 3.2.6. However, amendments to SYSC mean that for most firms the relevant systems and controls provisions will now be the financial crime organisational requirements contained in SYSC 6. The addition of these requirements to SYSC 6 forms part of the implementation in the UK of the Markets in Financial Instruments Directive,

104 FSMA 2000, s 10.

now repealed and recast by MiFID II (MiFID)[105] and the Capital Requirements Directive (CRD). In particular they give effect to the requirement under Art 16(2) of MiFID for firms to have in place adequate policies and procedures sufficient to ensure compliance of the firm (including its managers, employees and tied agents) with obligations under MiFID. New provisions were inserted in SYSC 4 to 10 for firms subject to MiFID and/or the CRD (common platform firms).

2.187 The 'common platform' introduced by SYSC 4 to 10 originally applied only to common platform firms (ie, firms subject to MiFID and/or the CRD). However, with effect from 1 April 2009, the common platform was extended to other types of FCA and PRA regulated firms with the exception of insurers, managing agents and the Society of Lloyd's.[106] The financial crime organisational requirements contained in SYSC 6.3 are similar in scope to those contained in SYSC 3.2.6. Accordingly, the FSA stated in CP 07/23 that it expected firms complying with SYSC 3.2.6 to be compliant with the new organisational requirements contained in SYSC 6.3.

Scope

2.188 The scope of application of the SYSC organisational requirements is set out in SYSC 1 Annex 1. In determining whether Chapter 6 of SYSC applies, regard must be had to the type of firm involved and then to the type of activities being undertaken. As noted above, certain firms are not covered by Chapter 6 of SYSC (or indeed, any of the other common platform provisions). Other firms fall within the scope of Chapter 6 of SYSC, but certain of the activities that they perform will not be within the scope of SYSC 6.3. Broadly, the requirements in SYSC 6.3 will not apply to firms in relation to their general insurance or mortgage mediation activities.

The Principles for Businesses

2.189 The Principles for Businesses are a general statement of fundamental obligations of firms under the regulatory system and apply in whole or in part to every firm with some modifications to certain firms (for example, firms carrying on MiFID business). Breaching a Principle makes a firm liable to disciplinary sanctions.

2.190 Under Principle 3 of the Principles for Businesses a firm must take reasonable care to organise and control its affairs responsibly and effectively with adequate risk management systems. One of the purposes of the systems and controls requirements set out in SYSC is to increase certainty by amplifying Principle 3.

105 Directive 2014/65/EU.
106 Such firms remain subject to SYSC 2 and 3, to the extent applicable.

2.191 The FCA has consistently taken action against firms for money laundering breaches. These include fining Standard Bank Plc £7,640,000 in 2014 for failing to apply enhanced due diligence consistently to corporate customers who were connected to PEPs and imposing a fine of £3,250,600 on Sonali Bank (UK) Ltd for failing to put in place and maintain adequate money laundering controls.

SYSC 6

2.192 The following section considers the requirements of SYSC 6 that relate to financial crime organisational requirements. As noted above, similar provisions are also contained in SYSC 3.2.6, which apply to a more limited range of firms.

2.193 SYSC 6.1.1R contains an overarching requirement for firms to establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm, including its managers, employees and appointed representatives (or tied agents, where applicable) with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime.

2.194 This rule accordingly expresses the risk-based nature of the policies and procedures that firms need to adopt. The focus of the risk-based approach is on ensuring the correct outcome as opposed to prescribing processes that must be followed by firms. Although more detailed guidance on the processes to be employed by firms is contained in the Guidance Notes (considered more fully below), the risk-based approach requires firms' senior management to manage risk and use their knowledge of the firm to develop systems and controls that uniquely address the specific risks that they face. The FCA had noted that firms' defences need to be flexible and dynamic enough to keep up with the changing face of money laundering and that only a risk-based approach can achieve this.

2.195 The regulator's commitment to intensive, intrusive, outcomes focused supervision, in the wake of the global financial crisis, has further emphasised the need for firms to focus on identifying and mitigating the specific risks to which they are subject. Senior management responsibility for AML compliance issues is emphasised by SYSC 6.3.8G, which provides that a firm must allocate to a director or senior manager responsibility within the firm for the establishment and maintenance of effective anti-money laundering systems and controls.

2.196 The overarching requirements of SYSC 6.1.1R are supplemented by rules and guidance contained in SYSC 6.3. These are set out below:

- SYSC 6.3.1R provides that a firm must ensure that the policies and procedures established under SYSC 6.1.1R include systems and controls that:

(i) enable it to identify, assess, monitor and manage money laundering risk;[107] and

(ii) are comprehensive and proportionate to the nature, scale and complexity of its activities;

- SYSC 6.3.3R provides that a firm must carry out a regular assessment of the adequacy of these systems and controls to ensure that they continue to comply with SYSC 6.3.1R;
- SYSC 6.3.6G states that in identifying its money laundering risk and in establishing the nature of these systems and controls, a firm should consider a range of factors, including its customer, product and activity profiles, its distribution channels, the complexity and volume of its transactions, its processes and systems and its operating environment;
- SYSC 6.3.7G states that a firm should ensure that the systems and controls include:

  (i) appropriate training for its employees in relation to money laundering;

  (ii) appropriate provision of information to its governing body and senior management, including a report at least annually by the firm's MLRO on the operation and effectiveness of those systems and controls;

  (iii) appropriate documentation of its risk management policies and risk profile in relation to money laundering, including documentation of its application of those policies;

  (iv) appropriate measures to ensure that money laundering risk is taken into account in its day-to-day operation, including in relation to the development of new products, the taking-on of new customers and changes in its business profile; and

  (v) 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;

- SYSC 6.3.8R requires a firm to allocate to a director or senior manager (who may also be the MLRO) responsibility within the firm for the establishment and maintenance of effective AML systems and controls.

The Money Laundering Reporting Officer

2.197 Under SYSC 6.3.9R firms[108] are required to appoint an individual as MLRO. The role of the MLRO is to act as the focal point for all activity within

107 'Money laundering risk' is the risk that a firm may be used to further money laundering (see SYSC 6.2.3G).

108 With the exception of a sole trader who does not employ any person who is required to be approved under FSMA 2000, s 59.

the firm relating to anti-money laundering. The FCA expects that a firm's MLRO will be based in the UK.[109]

2.198 The MLRO's specific responsibility is for oversight of the firm's compliance with the FCA's rules on systems and controls against money laundering. The firm must ensure that the MLRO has a level authority and independence within the firm and access to resources and information sufficient to enable the MLRO to carry out that responsibility. There is no requirement for mortgage or insurance intermediary firms to appoint an MLRO (although as noted above, they are subject to a high level requirement to counter financial crime).

2.199 A person who acts as the firm's MLRO will be performing the 'money laundering reporting function' which is a controlled function under the FMSA 2000, s 59, meaning that the FCA's approval will be required in order for that person to perform the role.

2.200 Rule 10A.7.10 of the FCA's Supervision Manual provides that the money laundering reporting function is that function of acting in the capacity of the MLRO of a firm. The money laundering reporting function is a required function which means that all firms (with the exception of certain categories such as general insurance firms) must have a person approved by the FCA to perform that function.

2.201 The money laundering reporting function is treated[110] as a 'significant influence function'. Persons who perform such significant influence functions will be subject to additional individual regulatory requirements as explained further below.

2.202 Under the FSMA 2000, ss 64A and 64B the FCA has issued the Statements of Principle and Code of Practice for Approved Persons. Statement of Principle 7 provides that 'An approved person performing an accountable significant influence function must take reasonable steps to ensure that the business of the firm for which he is responsible in his accountable function complies with the relevant requirements and standards of the regulatory system'.

FCA Financial Crime Guide

2.203 Following its 2011 consultation, the FSA published its regulatory guide on financial crime, called Financial Crime: a guide for firms, in December 2011. This has been routinely updated and was renamed under the FCA in 2018 as the 'Financial Crime Guide: A firm's guide to countering financial crime risks' (FCG) and 'The Financial Crime Guide: Financial Crime Thematic Reviews' (FCTR). The Guide aims to enhance understanding of financial crime expectations and

109 SYSC 6.3.10G.
110 FCA's Supervision Manual 10A.5.1

to help firms assess the adequacy of their financial crime systems and controls. The guide advocates risk-based and outcome-focused approaches to mitigating financial crime risk. The Guide now forms part of the FCA's Handbook. The Guide consolidates FCA Guidance on financial crime. It does not contain rules and its contents are not binding.

2.204 The FCA's guidance applies to all firms, although the extent to which it does apply will depend on the nature of the firm and its business. Each part of the guide contains sections on its application.

2.205 The introduction to the Guide states that the FCA will 'draw comfort' from seeing examples of firms implementing good practices as recommended by the guidance.

2.206 The Guide is broken into two parts, first of which contains both general and specific guidance on financial crime. In an effort to encourage firms to think carefully about their own specific risks, the guidance is made up of self-assessment questions and examples of good and poor practices with regard to financial crime systems and controls. Case studies are also included in the FCG, with references to sources of further information for firms. The FCG gives guidance on:

- financial crime systems and controls;
- money laundering and terrorist financing;
- fraud;
- data security;
- bribery and corruption;
- sanctions and asset freezes;
- insider dealing and market manipulation.

2.207 The FCTR of the guide summarises on a number of FCA/FSA thematic reviews which may be relevant to firms' procedures and controls. As in the FCG, examples of good and bad practices are provided. The FCTR considers:

- firms' high-level management of fraud risk;
- review of private banks' anti-money laundering (AML) systems and controls;
- automated AML transaction monitoring systems;
- review of firms' implementation of a risk-based approach to AML;
- data security in financial services;
- review of financial crime controls in offshore centres;
- financial services firms' approach to UK financial sanctions;

- anti-bribery and corruption in commercial insurance broking;
- the small firms' financial crime review;
- mortgage fraud against lenders;
- banks' management of high money-laundering risk situations;
- anti-bribery and corruption systems and controls in investment banks;
- banks' defences against investment fraud;
- banks' controls of financial crime risks in trade finance;
- how small banks manage money laundering and sanctions risk;
- managing bribery and corruption risk in commercial insurance brokering.

The JMLSG Guidance

2.208 The obligations in SYSC are 'backed up' by the Guidance Notes, which 'in effect, fleshes out the requirements of SYSC to give practical help to firms in assessing and mitigating their money laundering risk and putting in place an effective and efficient AML control environment'.[111]

2.209 The role of the Guidance is expressly recognised in SYSC, which provides at SYSC 6.3.5G that the FCA when considering whether a breach of its rules on systems and controls against money laundering has occurred, will have regard to whether a firm has followed relevant provisions in the Guidance. The Guidance makes clear, however, that they must not be applied 'unthinkingly' as a checklist of steps to take. Having said this, firms who depart from the Guidance need to exercise caution in doing so. A failure to comply with the Guidance is frequently relied on by the FCA in Final Notices against firms for money laundering breaches. The Guidance is considered more fully in Chapter 3.

Enforcement action

2.210 The FCA has various powers to bring enforcement action in relation to breaches of money laundering requirements. Such action may be taken either under a civil route (resulting, for example, in the imposition of a fine or censure) or under a criminal route resulting in a prosecution.

2.211 In taking enforcement action the FCA pursues a strategy of credible deterrence, which has recently resulted in favouring criminal prosecution over the administrative or civil sanctions, where appropriate. Criminal prosecutions have, however, tended to be used in the case of market related offences such as insider dealing.

111 See the FSA Review of firms' implementation of risk-based approach to anti-money laundering (March 2008).

2.212 The FCA has powers under the FSMA 2000, ss 401 and 402 to prosecute certain specified criminal offences in England, Wales and Northern Ireland. Under the FSMA 2000, s 402(1) the FCA has the power to prosecute breaches of the MLR 2017 and offences under the CTA 2008, Sch 7. The FCA's Enforcement Guide states that when considering whether to prosecute a breach of the MLR 2017, the FCA will also have regard to whether the person concerned has followed the JMLSG's Guidance.

2.213 The Enforcement Guide also states that the FCA may prosecute criminal offences for which it is not the statutory prosecutor, but where the offences form part of the same criminality as the offences it is prosecuting under the FSMA 2000. The FCA's ability to bring prosecutions on this basis was challenged in the cases of *R v Rollins* and *R v McInerney*.[112] These cases concerned allegations of insider dealing contrary to the Criminal Justice Act 1993 and the conduct of a 'boiler room' business in contravention of the FSMA 2000, s 23. In both cases, the defendants were charged with breaches of POCA 2002, ss 327 and 328 in addition to the offences under the Criminal Justice Act 1993 and FSMA 2000. Pursuant to the FSMA 2000, s 402, the FSA was the statutory prosecutor for the purposes of the Criminal Justice Act 1993, Part V and the FSMA 2000, but had no express statutory power to prosecute contraventions of POCA 2002. The defendants challenged the charges under POCA 2002 on the basis that the FSA had no power to bring such charges. However, the Court of Appeal found in each case that the FSA had the power to bring such charges on the basis that it enjoyed a right to bring private prosecutions in relation to offences not specified under the FSMA 2000.

2.214 The FSA brought a number of civil enforcement cases against firms and individuals relating to breaches of the FSA's Rules and requirements relating to AML systems and controls requirements.

2.215 The FCA continues to bring enforcement action against individuals and firms for money laundering related failings. Fines have been imposed on Coutts & Co (£8.75 million), Habib Bank (£525,000), Turkish Bank UK (£294,000) and EFG Private Bank (£4.2 million). Each of the above cases was brought for a breach of Principle 3 of the FSA's Principles for Businesses (Management and Control), with the exception of Turkish Bank that was fined by the FSA under the Money Laundering Regulations 2007, reg 42, which conferred on the FCA the power to impose a civil penalty. More recently, the FCA has fined the following firms for systemic money laundering breaches, Standard Bank Plc (£7.740 million), Bank of Beirut (£2.1 million), Barclays Bank Plc UK (£72,069,400), Sonali Bank (£3,250,600 million) and Deutsche Bank (£163,076,224). These enforcement cases have highlighted a number of issues, particularly with regard to higher risk customers. These include the following:

112 [2010] UKSC 39.

Proper identification and management of money laundering risk

2.216 Certain of the criticisms made by the FCA concern the failure of firms to properly identify money laundering risks. The Turkish Bank case, for example, concerned correspondent banking services provided to respondents in Turkey and Northern Cyprus. The bank was criticised for failing to have sufficient regard to the higher risk posed by relationships with institutions in non-EEA jurisdictions. The lack of equivalence of Turkey, for example, had been identified in a FATF national evaluation report. A further aspect concerning the management of risk arose in the EFG Private Bank case. In this case, concerns relating to certain clients were identified in the course of performing due diligence. The FSA found that the bank had proceeded with the client relationship without properly documenting the reasons for continuing the relationship in spite of the adverse information obtained by the firm.

Performing proper customer due diligence

2.217 In some cases the FCA has found that firms have not performed basic due diligence checks properly. In particular, firms continue not to understand ownership structures properly. A failure to obtain details of beneficial ownership will mean that the firm will also not be in a position to identify PEPs related to the customer or to carry out proper sanctions screening. The FCA also stressed the need for firms to challenge information provided. For example, to question complex or opaque ownership structures such as the use of bearer shares. Where foreign language documents are used to identify or verify the identity of clients, firms should ensure that they are in a position to properly understand and evaluate these.

Performing proper enhanced due diligence

2.218 Firms must ensure that they have proper procedures around enhanced due diligence and that procedures and manuals make clear what additional steps need to be taken beyond prescribed standard due diligence. It is not enough to say that higher risk clients will be subject to enhanced due diligence if procedures do not state what additional steps need to be taken. Recent cases have identified failings by firms in not properly establishing source of wealth or source of funds. For example, in relation to source of funds where a prospective client's wealth is said to derive from a business, the beneficial ownership of that business should be verified.

Carrying out PEP screening

2.219 The FCA identified that certain firms have failed to carry out proper PEP screening. There are various reasons for this. As already indicated, where a firm has carried out inadequate CDD, the firm may not have identified beneficial owners or related persons and may not have understood the client's control

structure, so that the firm will lack the underlying information required to screen against. In other cases, front office staff have been responsible for screening and have not done this properly.

Incentives and providing challenge

2.220 The FCA had observed that in some firms front office staff's remuneration is based at least in part on the number of new accounts opened. Such practices incentivise the opening of new accounts so that robust controls should be in place to mitigate risks arising from this. Firms should consider the structure of remuneration for the front office and ensure that the number of new accounts opened does not feature disproportionately as a criterion. The FCA also noted that AML teams have failed to provide the appropriate level of challenge to the front office. Ultimately, this is an issue stemming from the culture of the firm and management backing to the control functions in the firm.

Governance and assurance processes

2.221 Firms take different approaches to the structuring of their AML compliance. In some cases due diligence is carried out by the front office, whereas in other cases it is performed by an on-boarding team or the compliance team. Firms should recognise the potential conflict of interest created by front office staff completing the due diligence and ensure that if this approach is adopted appropriate control and quality assurance processes are put in place. As well as covering the adequacy of the due diligence and on-boarding process, this should cover compliance with controls or restrictions imposed on the operation of customer accounts. In certain cases the FCA identified basic failings such as the failure to obtain completed AML questionnaires or the removal of controls without justification which could have been identified through proper assurance and monitoring processes. Firms also need to ensure that systems are in place for the gathering and monitoring of management information relating to these matters.

2.222 It is important to note that the enforcement action that the FCA has taken against regulated firms and their employees or officers relate in most cases to systems and controls breaches, where no money laundering in fact took place. Firms must therefore ensure that they have adequate systems and controls in place to address financial crime risks.

CIVIL LIABILITY

2.223 It is important to appreciate the limitations of civil liability in connection with money laundering. The primary purpose of civil remedies is to provide recompense to victims that have suffered loss as a result of wrongdoing. Different policy considerations have informed the criminal law; providing recompense for victims for losses resulting from wrongdoing is not considered a priority of the

criminal justice system generally or of legislation in particular. Some activities proscribed under the criminal law, such as laundering drugs money, involve no immediately identifiable victim or loss. Therefore, such activities of themselves cannot found a civil claim.

2.224 But in some cases, there will be identifiable victims. Indeed, a third party may notify the intermediary that the funds have been misappropriated by the customer. The dilemma will then be whether the intermediary should comply with the customer's instruction and risk a claim by the third party against the intermediary, or whether the intermediary should keep the account frozen until the dispute has been resolved and risk a claim by its customer for breach of mandate.

2.225 If the firm receives consent to proceed with the transaction (or the moratorium periods expire), the firm is then able to comply with the customer's instruction without infringing the provisions in POCA 2002, Part 7. However, if new information then comes to light that gives rise to a further suspicion which is more than fanciful, the firm must make a further disclosure to NCA and will be subject to the rigours of POCA 2002, Part 7.

2.226 Even if the NCA's consent to proceed with the transaction has been granted and there are no new grounds of suspicion, the firm may still retain a suspicion that the customer does *not* have a valid title to the funds in his account. In such a case, the firm may have genuine concerns about the risk of civil liability towards third party victims.

2.227 There have been relatively few civil claims and it is important not to exaggerate the position. In some cases may be because the possibility of civil proceedings is overlooked by victims. However, it is important for intermediaries to be aware of their exposure to such claims. Such proceedings were brought against intermediaries involved after the Brinks Mat gold bullion robbery at Heathrow airport in 1983, the fraud against Grupo Torras owned by the Kuwait Investment Office and the Federal Republic of Nigeria in relation to corruption of General Sani Abacha.[113] These claims were for very substantial amounts and enabled the victims to obtain substantial recompense.

2.228 There is no single straightforward civil remedy that enables a victim to recover the proceeds of wrongdoing. There are a range of possible remedies including the common law remedy of monies had and received, tracing and constructive trusteeship.[114] This is not the place to consider the elements of each of these claims in detail. Liability for knowing assistance (sometimes referred to as dishonest assistance) is a type of constructive trusteeship. It probably

113 See para 2.5 above.

114 There is a concept of constructive trust in Scots law but the situations in which it arises are limited to either: (a) where a person in a fiduciary position gains a benefit by virtue of that position (*Magistrates of Aberdeen v University of Aberdeen* (1877) 4 R 48, HL); or (b) where there is an existing trust, and a stranger to that trust is, to his knowledge, in possession of property belonging to the trust (*Soar v Ashwell* [1893] 2 QB 390).

presents the greatest risk to intermediaries and other third parties and is therefore dealt with in outline in this chapter. The elements of civil liability for knowing assistance are similar as follows.

2.229 First, there must be a fiduciary relationship between the wrongdoer and the victim. Such fiduciary relationships have been found to exist in a wide variety of situations, usually far removed from orthodox trusts involving a settlor and beneficiaries. For example, fiduciary relationships have been found to arise in the following situations: director/company, employee/employer, civil servants/state and government minister/state relationships.

2.230 The second element is breach of fiduciary obligations. Many predicate activities are likely to constitute wrongdoing for these purposes, though it seems that there is no need for the trustee to have acted dishonestly or fraudulently.

2.231 Thirdly, the intermediary must provide the wrongdoer with assistance. Assistance has its usual meaning and could therefore include a wide range of activities such as banking or professional services including providing banking facilities, company incorporation and administration services and professional advice. Such activities could come also within the ambit of the money laundering offences described above.

2.232 Fourthly, the intermediary must have acted with conscious impropriety or dishonestly. This will be the key to establishing civil liability. There is some debate over the standard of knowledge and the law is not entirely clear. Many regard the decision of Lord Nicholls in a Privy Council case of *Royal Brunei Airlines Sdn Bhd v Tan*[115] to be a seminal authority on this point. There has since been much debate about the appropriate test for dishonesty and, in particular, whether it should be subjective or objective. Hopefully, that debate has been settled by the decision in *Twinsectra Ltd v Yardley*[116] which favoured a combined test, which means that the conduct in question must be dishonest by the ordinary standards of reasonable and honest people and that the defendant realised that by those standards his conduct was dishonest. Similarly in *Barlow Clowes International Ltd (in liquidation) v Eurotrust International Ltd*[117] the Privy Council held that it is unnecessary to show subjective dishonesty in the sense of consciousness that the transaction is dishonest. It is sufficient if the defendant knows of the elements of the transaction which make it dishonest according to normally accepted standards of behaviour.

2.233 When the elements of dishonest assistance are established, the defendant is personally liable to account by reason of its involvement in the wrongdoing. This liability does not depend on the defendant continuing to hold the proceeds of the wrongdoing. If the wrongdoing involves a substantial fraud, this liability could be very substantial.

115 [1995] 2 AC 378, PC.
116 [2002] UKHL 12, [2002] 2 All ER 377.
117 [2006] 1 All ER 333.

2.234 To reduce the potential exposure to third parties, there are a number of options open to an intermediary. Generally it is for the third party to apply for a freezing order in such a case, just as it is for the NCA to apply for a restraint order if its investigations reveal that the account contains the proceeds of criminal conduct. If, for whatever reason, the third party refuses to apply for such an order and the intermediary has real concerns, the intermediary may want to consider:

- asking for evidence from the third party to substantiate the allegations;
- making enquiries of the customer about the source of the funds (subject to any concerns that it may have about tipping off the customer (see para 2.89);
- if still in doubt, the intermediary could give the third party a maximum period of time within which to apply for a freezing order;
- interpleading between the third party and the customer;[118]
- seek directions from the court.[119]

118 The intermediary may make an application for relief by way of interpleader, in the absence of any proceedings, provided that it expects to be sued by two or more persons in relation to the account. See the case of *Crellin v Leyland* [1842] 6 Jur 733 where a bank did just this. The intermediary can make an application for relief by way of interpleader by issuing a claim form, containing the required information, which attaches evidence in the form of an affidavit by the applicant. If the application for relief from interpleader is successful the intermediary is likely to have to pay the disputed sum into court having deducted its assessed costs to date. The application is made under Civil Procedure Rules ('CPR') Sch 1, RSC Order 17, Interpleader.

119 For example, it could seek directions from the court or a declaration as to what to do under CPR 40.10. In following this course, it seems unlikely that the intermediary would be found to have acted dishonestly for the purposes of a dishonest assistance claim – see the dicta of Colman J in *Tayeb v HSBC Bank Plc* [2004] EWHC 1529 at [75].