Original Article

The fight against illicit finance: A critical review of the Labour government's policy

Nicholas Ryder
is a Reader in Law at the University of the West of England. He is Head of the Commercial Law Research Unit and specialises in financial crime, financial regulation and consumer law.

Correspondence: Nicholas Ryder, Department of Law, Faculty of Business and Law, University of the West of England, Bristol BS16 1QY, UK

ABSTRACT The aim of this article is to identify and critically consider the effectiveness of the Labour government's policy towards financial crime. The article highlights the general threat posed by financial crime, yet concentrates on the government's policies towards money laundering, fraud and terrorist financing.
Journal of Banking Regulation (2011) **12,** 252–275. doi:10.1057/jbr.2011.1

Keywords: government policy; Labour policy; money laundering; fraud; terrorist financing; financial crime

INTRODUCTION

The importance of tackling financial crime was illustrated during the 1980s and 1990s by US-led 'war on drugs' and the 'financial war on terrorism' in 2001. We have witnessed significant instances of fraud involving multinational corporations resulting in the collapse of the Bank of Credit Commerce International, Barings Bank, Enron and WorldCom. More recent instances of fraud include Jerome Kerivel, who made illegal transactions that cost Société Générale £3.7 billion.[1] In 2009, Bernard Madoff was sentenced to 150 years imprisonment after being found guilty of architecting a pyramid fraud worth approximately £40 billion.[2] The impact and scale of these scandals have been overshadowed by a new threat to the financial markets in the United States and the United Kingdom – mortgage fraud. The Association of Chief Police Officers claim that the annual level of mortgage fraud in the United Kingdom is approximately £700 million per year.[3] However, in the United States, the Federal Bureau of Investigation, citing research by the Prieston Group, concluded that the annual level of mortgage fraud is between $4 to $6 billion.[4] Therefore, it is essential that the United Kingdom creates and implements a robust financial crime policy. But what is financial crime? According to the International Monetary Fund (IMF), 'there is no internationally accepted definition of financial crime'.[5] A useful point of reference is the Financial Services and Markets Act 2000 (FSMA 2000). According to s.6(3), financial crime is defined as 'any offence involving fraud or dishonesty; misconduct in, or misuse of information relating to, a financial market; or handling the proceeds of crime'.[6] However, this definition does not specifically refer to either money laundering or the financing of terrorism, both of which are associated with other types of financial crime including fraud (p. 8).[5] Financial crime is mistakenly referred to as a 'victimless crime', and in many instances it is impossible to identify who or what has suffered a financial loss. If this statement is to be believed, why do so many governments dedicate resources and time to limit the extent and impact of financial crime? The answer to this question could be found in the following quotation from the Financial Action Task Force (FATF), 'criminal proceeds have the power to corrupt and ultimately destabilise communities or whole national economies'.[7] Financial crime is attributed to organised criminals who seek to maximise their profits so that they can enjoy a so-called 'champagne lifestyle'.[8] Furthermore, financial crime can erode the integrity of a nation's financial institutions. The IMF stated that 'negative consequences for a country's macroeconomic performance, impose welfare losses, and may also have negative cross border negative externalities' (p. 8).[5] Vaithilingam and Nair stated that 'financial-related crimes have significant economic and social consequences for nations worldwide. It weakens the financial systems which are the main players for global financial transactions'.[9] It is also a threat to national security.[10] For example, terrorists need money and resources to carry out their activities. Although much of the finance for terrorism comes from legitimate sources, a large percentage will come from criminal activity; a good example of this is the terrorist attacks of September 2001 where some of the finances were obtained from credit card fraud and identity theft.[11] Since these terrorist attacks, there has been an increased focus on cutting off the financial resources of terrorism; however, this is proving extremely difficult and controversial. What is the cost of financial crime? According to the FATF:

> UK law enforcement estimates the economic and social costs of serious organised crime, including the costs of combating it, at upwards of £20 billion a year. It is estimated that the total quantified organised crime market in the UK is worth about £15 billion per year as follows: drugs (50 per cent); excise fraud (25 per cent); fraud (12 per cent); counterfeiting (7 per cent); organised immigration crime (6 per cent).[12]

HM Treasury noted that 'organised crime generates over £20 billion of social and economic harm in the UK each year' (p. 6).[13] The Home Office stated that organised crime 'reaches into every community, ruining lives, driving other crime and instilling fear'.[14] Furthermore, financial crime has an adverse impact on the economies of countries. For example, Scanlan noted the economic impact of terrorism and stated that 'the disruption to the transport system in London caused by the bomb attacks of 7 and 21 July 2005 alone have been estimated to have cost the nation in excess of £3 billion'.[15] Similarly, the Bishopsgate bombing in London in 1993 caused damage to property in excess of £1 billion.[16] Therefore, this article identifies and comments on the policies adopted towards money laundering, fraud and the financing of terrorism.

MONEY LAUNDERING

The UK's anti-money laundering (AML) policy has been led by HM Treasury, a point illustrated by the publication of its 'Anti-money laundering strategy'.[17] However, there are other actors who play an important role in the UK's AML policy including the Financial Services Authority (FSA), the Joint Money Laundering Steering Group (JMLSG) and the Serious Organised Crime Agency (SOCA). In its policy document, HM Treasury stated that its strategy was based on three objectives – effectiveness, proportionality and engagement (p. 12).[17] In terms of the first objective, HM Treasury took the view that the United Kingdom would continue to ensure that it preserves an effective AML scheme so that it achieves its international obligations (p. 7).[17] This is achieved by a series of domestic measures including the Proceeds of Crime Act 2002 (PCA 2002), the MLR 2007, professional guidance issues by the JMLSG and specific AML rules issued by the FSA. These measures also seek to achieve the international standards set by the 40 Recommendations of the FATF, the obligations imposed on the United Kingdom by the Third Money

Laundering Directive and those contained in the Vienna and Palermo Conventions. The second objective, proportionality, means that the government will continue to adopt a risk-based approach towards money laundering. This seeks to ensure that its AML measures are cost effective so that firms can adopt a flexible approach towards meeting their obligations.[18] The final objective, engagement, provides that the authorities will continue to work with firms to ensure that the consultation process is fully utilised and that the levels of feedback regarding the performance of the regulated sector is communicated to them (p. 7).[17] HM Treasury outlined how it aims to achieve these objectives 'the existing regime consists of measures ranging from provisions in the *criminal law* [authors emphasis] to punish money launderers and to deprive them of their proceeds, to the obligation on the *financial services industry* [authors emphasis] and certain other sectors and professions to identify their customers and to report *suspicious activities* [authors emphasis] when necessary' (HM Treasury,[17] p. 11).[19] Therefore, for the purpose of this article, the UK's AML policy can be divided into three parts – the criminalisation of money laundering; that regulated financial institutions are compelled to put in place systems to preclude and identify money laundering; and the use of reporting identifiable or suspected money laundering transactions to the relevant authorities.

The criminalisation of money laundering

The primary money laundering legislation is contained in Part 7 of the PCA 2002.[20] The Act applies 'where money laundering activities took place on or after 23 February 2003'.[21] The three principal money laundering offences created by the Act are concealing, disguising, converting, transferring or removing from the jurisdiction or criminal property[22]; entering into or becoming concerned in an arrangement knowing or suspecting it to facilitate the acquisition, retention, use and control of criminal property on behalf of another person[23]; and acquiring, using or possessing criminal property.[24] These offences may be committed by any person, irrespective of the fact they work within the 'regulated sector' or undertake a 'relevant business'.[25] Other offences created by the Act include failure to disclose by the regulated sector[26]; failure to disclose by nominated officers in the regulated sector[27]; and failure to disclose by other nominated officers,[28] tipping off,[29] and prejudicing an investigation.[30]

A person commits an offence under s. 327 if they conceal criminal property, disguise criminal property, convert criminal property, transfer criminal property or remove criminal property from England and Wales or from Scotland or from Northern Ireland.[31] All of these offences apply to property that is criminal property if '(a) it constitutes a person's benefit from criminal conduct or it represents such a benefit (in whole or part and whether directly or indirectly), and (b) the alleged offender knows or suspects that it constitutes or represents such a benefit'.[32] The scope of this offence is wide and it is possible for *any* person to have made a 'gain', not just the person who committed the offence. There are three important points to note: First, the Act goes as far as stating that it is of no consequence 'who carried out the conduct' or 'who benefited from it' or 'whether the conduct occurred before or after the passing of this Act'.[33] Second, the gain must 'flow from that criminal activity'; this does not necessarily mean a financial gain and it could include improvements in someone's standards of living or profits derived from the criminal activity.[34] Third, that it 'represents such a benefit' (p. 344).[34] A person breaches s. 327 if they know or suspect that it constitutes or represents such a benefit.[35] Section 340(3) of the PCA offers a definition of criminal property, which enables the prosecution to argue that the offender has committed an offence under s. 327. Criminal property is defined as: '(a) it constitutes a person's benefit from criminal conduct or it represents such a benefit (in whole or part and whether directly or indirectly), and (b) the alleged offender knows or suspects that it constitutes or represents such a benefit'.[36] It is a defence for a person to make an authorised disclosure via a suspicious activity report; this is referred to as an authorised disclosure.[37] A person does not commit an offence if he makes an authorised disclosure[38]; he has a reasonable excuse for not making a disclosure[39]; and the action he does is in accordance with undertaking a function that relates to the enforcement of a provision under the PCA 2002.[40]

The second criminal offence provides that a person commits an offence if they enter or become concerned in an arrangement that they know of suspects 'the acquisition, retention, use or control of criminal property by or on behalf of another person'.[41] To establish a conviction, the prosecution must prove that a person became concerned with an arrangement that they knew or suspected would make it simpler for another person to acquire, retain, use or control criminal property. Furthermore, that the person concerned also knew or suspected that the property constituted or represented benefit from criminal conduct.[42] In order for a person to be guilty of the offence under this section, the definition of criminal property is again of central importance. The final offence provides that a person commits an offence if they acquire criminal property, use criminal property or have possession of criminal property.[43] This offence is not committed if a person makes an authorised disclosure,[44] planned to make such a disclosure but had a reasonable excuse for not doing so,[45] acquired or used or had possession of the property for adequate consideration,[46] undertook a function relating to the enforcement of any provision of the PCA or other relevant enactment,[47] that the conduct occurs overseas and is lawful in that particular jurisdiction,[48] and that the act is done by a deposit-taking body.[49] In order for a person to be convicted of an offence, it has to be proven that the property handled is 'criminal property' and that it comprises a benefit. Furthermore, it has to be proven that the defendant knows or suspects that the property is obtained from criminal conduct. It is important to note that terrorist property is not covered by the PCA 2002, but dealt with the Terrorism Act 2000.[50] The laundering of terrorist property is governed by Part III of the Terrorism Act 2000.

Regulated financial institutions

The second part of the UK's AML policy is reliant on the regulations imposed by the FSA, which has extensive rule-making powers to impose regulations on the regulated sector.[51] Until 2006, the obligations imposed were contained in Money Laundering Sourcebook (ML).[52] In January 2006, the FSA announced that it was streamlining ML,[52] and it became obsolete in August 2006. ML was replaced with a principles-based approach in the Senior Management Arrangements, Systems and Controls, or SYSC part of the Handbook. Part 3 provides that firms must have in place systems and controls that are appropriate for the firm to conduct its business.[53] In particular, a firm is required to 'take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime' (SYSC 3.2.6 R).[53] Therefore, firms are required to carry out regular assessments of the adequacy of the AML systems they have in place to prevent themselves from being used to further financial crime,[54] allocate a director or senior manager with overall responsibility for establishing and maintaining the AML system and to appoint a money laundering reporting officer.[55] The FSA has extensive investigative and enforcement powers. For example, it has the ability to require information from firms,[56] to appoint investigators,[57] to obtain the assistance of overseas financial regulators[58] and provide appointed investigators with additional powers.[59] Furthermore, it has become a prosecuting authority for certain money laundering offences.[60] The FSA also has the power to impose a financial penalty where it establishes that there has been a contravention by an authorised person of its rules.[61] The FSA has imposed a series of fines on firms that have breached ML even where there was no evidence of money laundering.[62] More recently, it has fined a firm's money laundering reporting officer.[63,64] The FSA also implements the 2007 MLR, the purpose of which is to prevent businesses based in the United Kingdom from being abused by criminals and terrorists for the purposes of money laundering.[65]

Financial intelligence

The final part is the use of SARs to gather financial intelligence, which are to be found in the PCA 2002 and the MLR 2007.[66] The PCA 2002 provides that SARs should be submitted if they 'suspect'[67] or have 'reasonable grounds for suspecting' that an offence has been committed.[68] Brown and Evans concluded that 'it is worthy of note that the test to be applied where the section refers to 'suspect' is a subjective test, whereas where there is reference to 'reasonable grounds to suspect', an objective test should be applied with the result under the objective test that a defendant's 'neglect' to properly comply with the obligations in POCA could result in a criminal conviction'.[69] If a firm has 'reasonable suspicion'[70] or any possibility provided that it is more than 'fanciful' that it is being used for the purposes of money laundering, it is required to notify its money laundering reporting officer who will complete an SAR and send it to SOCA, who will then determine whether further action is to be taken.[71] Wadsley contended that disclosure is required 'not just in clear-cut cases where there is knowledge of money laundering, but also where there is merely suspicion'.[72] The interpretation of the term 'suspicion' has been contemplated by courts in England and Wales on many occasions, and is seen by many commentators as limiting the effectiveness of money laundering reporting requirements.[73] Longmore LJ in *R* v. *Da Silva* took the view that:

> It seems to us that the essential element of the word suspect and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice.[74]

The Court of Appeal added:

> 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 fanciful, that the relevant facts exist. A vague feeling of unease would not suffice. But the statute does not require the suspicion to be 'clear' or 'firmly grounded and targeted on specific facts', or based upon 'reasonable grounds'.[74]

According to the Court of Appeal in *K* v. *National Westminster Bank, HMRC, SOCA*,[75] the interpretation of 'suspicion' is the same in civil law as it is in criminal law.[76] Brown and Evans took the view that 'in most cases, the statement by those making an SAR that they have a suspicion will be enough. It will be exceptional for the courts to require those that report a suspicion to provide justification for having a suspicion. In reality, it will be for those challenging the making of a SAR to prove that no suspicion existed'.[77] However, it is important to consider the decision of the Court of Appeal in *Shah* v. *HSBC Private Bank (UK) Ltd*.[78] Here, Longmore LJ took the view that 'I cannot see why, rather than submit to summary judgment dismissing the claim, Mr Shah cannot require the bank to prove its case that it had the relevant suspicion and be entitled to pursue the case to trial so that the bank can make good its contention in this respect' (p. 22).[78] As a result of the Court of Appeal's decision, Stanton took the view that 'a simple assertion that a professional person suspected the client to be money laundering does not suffice: evidence needs to be produced to prove the existence of the suspicion'.[79]

The overall effectiveness of the SARs regime has been questioned.[80–82] A common criticism of the reporting requirements is that they have created a 'fear factor' that has resulted in a significant increase in the number of SARs submitted.[83] The number of SARs submitted between 1995 and 2002 increased from 5000 to 60 000.[84] SOCA reported that it had received 228 834 SARs between October 2008 and September 2009.[85] This represents an increase of approximately 200 000 reports during a period of 13 years. The increase is associated with the threat of sanctions by the FSA, and it has led to the regulated sector adopting a tactic that has been referred to as 'defensive' or 'preventative' reporting.[86] The banking sector has raised concerns about the SAR's regime,[87] and it has been suggested that the requirements should be abandoned and that the resources should be redirected elsewhere.

FRAUD

The UK fraud policy can also be divided into three parts – the criminalisation of fraudulent activities; regulatory agencies and anti-fraud reporting requirements. Fraud has been propelled from its traditional tertiary position, behind money laundering and terrorist financing, to the top of the government's financial crime agenda. This is due to the publication of the Fraud Review (the Review) and the introduction of the Fraud Act 2006.[88] Sarker takes the view that 'a fresh crop of anti-fraud initiatives, reviews and legislation has sprung up, ostensibly demonstrating how fighting fraud is a top priority in the UK'.[89] However, this is not a view shared by all commentators and it has been argued that 'little has changed to reverse the perception of fraud as a low priority'.[89] The Review was commissioned by the Attorney General 'to recommend ways of reducing fraud and the harm it does to the economy and society'.[90] It considered three questions:

1. What is the level of fraud?
2. What is the appropriate role of the government in dealing with fraud?
3. How could government resources be spent to maximise value for money? (pp. 4-5)[90]

The Review was unable to accurately outline the extent of fraud. In relation to its second task, it concluded that the government has two functions – to protect public money from fraudsters and to protect consumers and businesses against fraud. The Review recommended that the government should adopt a holistic approach towards fraud and develop a national strategy. Furthermore, it recommended the creation of the National Fraud Authority to develop and implement the strategy. It also suggested that a National Fraud Reporting Centre should be created so that businesses and individuals could report fraud. The NFRC has been operating since October 2009,[91] as actionfraud.org. The National Fraud Intelligence Bureau is the agency dedicated to analyse and assess fraud, employing analysts from both law enforcement and private sector. Fourth, the Review suggested that a national lead police should be established based on the City of London Police Force.[92]

Criminalisation

Before 2006, the law relating to fraud comprised eight statutory deception offences in the Theft Act (1968 and 1978) and the common law offence of conspiracy to defraud.[93] The offences created by Theft Act were difficult to enforce.[94] Therefore, it led to the introduction of the Theft Act 1978, which did little to rectify the problems.[95] The Home Office noted that it 'is not always clear which offence should be charged, and defendants have successfully argued that the consequences of their particular deceptive behaviour did not fit the definition of the offence with which they have been charged'.[96] In 1998, the then Home Secretary Jack Straw MP asked the Law Commission to examine the law on fraud.[97] In 1999, it published a Consultation Paper that distinguished between two types of fraudulent offences – dishonesty and deception.[98] The Law Commission concluded that although the concerns expressed about the existing law were valid they could be met by extending the existing offences in preference to creating a single offence of fraud.[99] The Law Commission published its final report in 2002 with the Fraud Bill.[100] The Fraud Act came into force on 15 January 2007[101]; it overhauls and widens the criminal offences available with respect to fraudulent and deceptive behaviour.[102] The new offence, punishable by imprisonment of up to 10 years and/or an unlimited fine, can be committed in three different ways – fraud by false representation,[103] fraud by failing to disclose information[104] and fraud by abuse of position.[105] Dennis argued that the Act 'represents the culmination of a law reform debate that can be traced back more than 30 years'.[106] Scanlan takes the view that the Fraud Act 2006 'provides prosecutors with a broad range offence of fraud'.[107] This clearly represents a significant improvement on the statutory offences of the Theft Acts and the common law offences of conspiracy to defraud.

Regulatory authorities

There are a broad range of regulatory agencies that attempt to combat fraud.[108] The most prominent agency is the Serious Fraud Office (SFO), which was established following the 'era of financial deregulation' in 1980s, an era that resulted in London attracting 'foreign criminals, including "mademen" from the US Mafia, the "Cosa Nostra", who were now in London taking advantage of the new climate of enterprise, offering securities scams, commodity futures trading frauds and other forms of investment rip-offs'.[109] Bosworth-Davies noted that 'almost overnight, London became the fraud capital of Europe and every con-man, snake-oil, salesman, grafter and hustler turned up'.[109] To tackle these problems, the SFO was created with both investigative and prosecutorial powers.[110] The impetus for introducing the Criminal Justice Act 1987 and creating the SFO was the Fraud Trials Committee Report, or 'Roskill Report'. The Roskill Committee considered the introduction of more effective means of fighting fraud through changes to the law and criminal proceedings.[111] The Committee criticised the staffing levels of the agencies policing fraud, and that there was a great deal of overlap between them. Roskill concluded that 'co-operation between different investigating bodies in the UK was inefficient, and the interchange of information or assistance between our law enforcement authorities was unsatisfactory' (p. 8).[111] The Roskill Committee made 112 recommendations, of which all but two were implemented.[112] Its main recommendation was the creation of a new unified organisation responsible for the detection, investigation and prosecution of serious fraud cases. The result was the SFO, which has jurisdiction in England, Wales and Northern Ireland, but not Scotland.[113] It is headed by a director, who is appointed and accountable to the Attorney General. Under the Act, the SFO has the ability to search property and compel persons to answer questions and produce documents, provided they have reasonable grounds to do so.[114] The SFO has a budget of £44.6 million per year; it employees 303 staff and has 86 active cases.[115]

The SFO determines whether or not to investigate the matter if the allegation meets the following criteria:

1. Does the value of the alleged fraud exceed £1 million?
2. Is there an international element to the fraud?
3. Is it likely to cause widespread public concern?
4. Does the case require specialised knowledge?
5. Does the SFO need to use its investigative powers?

The SFO also considers the seriousness of the case and its complexity, and will investigate investment fraud, bribery and corruption, corporate fraud and public sector fraud. The effectiveness of the SFO has been questioned following a number of high-profile prosecutions that have failed. Mahendra describes the notorious failures of the SFO as reminiscent of 'watching the England cricket team – a victory being so rare and unexpected that it was a cause of national rejoicing'.[116] Indeed, Wright notes that 'because the SFO operates in the spotlight, the beam falls on the unsuccessful as well as the victorious. Indeed it shines with blinding brightness on the ones that get away'.[117] The prosecutorial inadequacies of the SFO were highlighted by the 'Review of the Serious Fraud Office'.[118] The Review compared the performance of the SFO with the US Attorney's Office for the Southern District of New York and the Manhattan District Attorney's Office and concluded that 'the discrepancies in conviction rates are striking' (pp. 3-4).[118] The Review noted that between 2003 and 2007, the SFO's average conviction rate was 61 per cent, whereas the conviction rates in the two aforementioned cases studies were 91 and 97 per cent, respectively.[119] In September 2007, the Crown Prosecution Service announced the creation of the Fraud Prosecution Unit, now referred to as the Fraud Prosecution Division,[120] which was established following the collapse of the Jubilee Line fraud trial.[121] The Unit will limit its involvement to suspected instances of fraud exceeding £750 000, cases involving the corruption of public officials, fraud on government departments, fraud on overseas governments, complicated money laundering cases and any other matter that it feels is within its remit.[121] In October 2008, HM Crown Prosecution Service Inspectorate concluded that there 'has been a positive direction of travel in terms of successful outcomes (convictions), which stood at a creditable 85 per cent of the defendants proceeded against in 2007–2008; underlying casework quality, which is characterised by strong legal decision-making and active case progression; and the development of management systems and leadership profile'.[122] Bosworth-Davies took the view that 'it [the Serious Fraud Office] was not the great success that Roskill envisaged, and its activities were marked out by 20 years of professional jealousy and internal squabbling among its component teams'.[123] On the contrary, the performance of the SFO is hampered by the complexity of the crimes it investigates.[117] Raphael noted that the SFO is 'always kept short of resources and instead of being a unified fraud office, was just another, more sophisticated, prosecution agency'.[117]

The FSA's fraud policy can be divided into four parts – a direct approach,[124] increased supervisory activity,[125] promoting a more joined-up approach[126] and Handbook modifications.[127] The FSA requires senior management to take responsibility for managing the risk of fraud and that firms are required to have in place effective controls and instruments that are proportionate to the risk the firm faces.[128] The FSA encourages firms to maintain their systems and controls, thematic work, improving the whistle-blowing arrangement, amending the financial crime material in the FSA Handbook and ensuring that the financial services sector, trade associations and the government continue to communicate the risk of fraud to customers.[128] To implement this policy, the FSA has been given an extensive array of enforcement powers, some of which it has utilised to combat fraud. It is a prosecuting authority for both money laundering and certain fraud-related offences,[129] and has the power to impose a financial penalty where it establishes that there has been a contravention by an authorised person of any requirement.[61] The FSA fined Capita Financial Administration Limited £300 000 for poor anti-fraud controls,[130] and in May 2007 fined BNP Paribas Private Bank £350 000 for weaknesses in its systems and controls that allowed a senior employee to fraudulently transfer £1.4 million out of the firm's clients' accounts without permission.[131] Furthermore, it has fined the Nationwide Building Society £980 000 for 'failing to have effective systems and controls to manage its information security risks',[132] and Norwich Union Life, £1.26 million for not 'having effective systems and controls in place to protect customers' confidential information and manage its financial crime risks'.[133] The FSA also has the power to ban authorised persons and firms from undertaking any regulated activity.[134] In 2008, the FSA had fined and/or banned 12 mortgage brokers for submitting false mortgage applications. In 2007, the FSA only imposed five bans were handed down. In 2008, the FSA prohibited 24 separate brokers and issued fines in excess of £500 000. In the first half of 2009, the level of fines imposed by the FSA had already exceeded this figure. In addition to imposing sanctions on fraudsters, the FSA has also enabled victims of fraud to recover losses suffered at the hands of companies involved in share fraud activity.[135]

The most recent agency created to tackle fraud is the NFA.[136] The objectives of the NFA include creating a criminal justice system that is sympathetic to the needs of victims of fraud by ensuring that the system operates more effectively and efficiently,[137] to discourage organised criminals from committing fraud in the United Kingdom and to increase the public's confidence in the response to fraud. Rider stated that the NFA

> has an impressive list of strategic aims: tackling the key threats of fraud that pose the greatest harm to the United Kingdom; the pursuit of fraudsters effectively, holding them to account and improving victim support; the reduction of the UKs exposure to fraud by building, sharing and acting on knowledge; and securing the international collaboration necessary to protect the UK from fraud.[138]

The NFA's Interim Chief Executive Sandra Quinn boldly claimed that 'we can respond quickly and effectively to the fraud threat'.[136] This level of optimism was not shared by Bosworth-Davies who stated that the NFA 'will last about as long as the unlamented Asset Recovery Agency'.[139] An important measure introduced by the NFA was the publication of the National Fraud Strategy, which is an integral part of the government's fraud policy,[140] under which the NFA is required to:

1. tackle the threats presented by fraud;
2. act effectively to pursue fraudsters and hold them to account;
3. improve the support available to victims;
4. reduce the UK's exposure to fraud by building the nation's capability to prevent it; and
5. target action against fraud more effectively by building, sharing and acting on knowledge and securing the international collaboration necessary to protect the United Kingdom from fraud.[140]

Despite the fanfare announcement by the government that it had created the NFA, one fundamental question that must be asked is whether it will actually make any difference towards the overall effectiveness of the UKs fraud policy. If we are to believe that the extent of fraud in the United Kingdom is somewhere between £14 billion and £30 billion, how is it possible for an agency to make any valuable dent in this statistic if it only has a budget of £29 million over a 3-year period?

The Office of Fair Trading (OFT) 'is chiefly concerned with the protection of consumers. It also regulates competition amongst businesses but this is approached from a consumer protection perspective'.[141] The OFT has three regulatory objectives – investigation of whether markets are working well for consumers, enforcement of competition laws and enforcement of consumer protection laws. It is important to note that the OFT has its own fraud policy.[142] The objectives of the OFT are similar to the TFC, in that it seeks to inform and protect consumers from fraudulent scams.[143] Furthermore, the OFT works and cooperates with other agencies such as the SFO,[144] and it also liaises with overseas agencies.[145] Finally, HM Revenue and Customs deals with issues such as VAT fraud, alcohol fraud[146] and oil fraud.[147]

The effectiveness of these anti-fraud agencies must be questioned. There is a considerable degree of overlap among the SFO and FSA; both have extensive investigative and prosecutorial powers that seek to achieve the same objective. The failures of the SFO are well documented; however, the FSA's effectiveness must be questioned because of its obsession with combating money laundering. It is recommended that a single financial crime agency should be established to coordinate the UKs fraud policy with extensive investigative and prosecutorial powers. Such an idea was first mooted by Fisher who recommended the creation of a 'single "Financial Crimes Enforcement Agency" to tackle serious fraud, corruption and financial market crimes'.[148] This recommendation has been supported by the Conservative party that would establish an Economic Crime Agency that would do the work of the SFO, the Fraud Prosecution Service and the OFT. The then Shadow Chancellor George Osborne MP stated that 'we are very, very bad at prosecuting white-collar crime. We have six different government departments, eight different agencies and the result is that these crimes go unpunished'.[149] Following the 2010 general election, the coalition government outlined its desire to create a single agency to tackle financial crime. The government stated:

> we take white collar crime as seriously as other crime, so we will create a single agency to take on the work of tackling serious economic crime that is currently done by, among others, the Serious Fraud Office, Financial Services Authority and Office of Fair Trading.[150]

However, it is likely that the 'financial crisis' could scupper the government's plans to create such an agency.[151] The Fraud Advisory Panel writing in March 2010 took the view that because of the current climate the time is not right for an economic crime agency.[152]

Reporting obligations

The Fraud Review noted that 'fraud is massively underreported. Fraud is not a police priority, so even when reports are taken little is done with them. Many victims therefore, don't report at all. So the official crime statistics display just the tip of the iceberg and developing a strategic law enforcement response is impossible because the information to target investigations does not exist'.[153] If a suspected fraud is committed against a bank, it is reported to its Money Laundering Reporting Officer (MLRO). Successful frauds are reported to SOCA. On the contrary, it is the decision for individual banks to determine whether or not to report the fraud to the police. In 2007, the Home Office announced that victims of credit card, cheque and online banking fraud are to report the matter to banks and financial institutions.[154] However, the obligation to report allegations of fraud is not as straightforward, but nonetheless still important. The primary statutory obligation for reported instances of fraud is contained under the PCA 2002.[26] It is a criminal offence under the 2002 Act to fail to disclose via an SAR where there is knowledge, suspicion or reasonable grounds to know or suspect, that a person is laundering the proceeds of criminal conduct. Successful fraud is defined as money laundering for the purpose of this Act.[155] Furthermore, the Act specifies that members of the regulated sector are required to report their suspicions 'as soon as reasonable practical' to SOCA via their MLRO. There is no legal obligation to report unsuccessful or attempted frauds to the authorities because any attempted frauds will not give rise to any legal criminal proceedings that are available for money laundering, and fall outside the scope of the mandatory reporting obligations under the PCA 2002. Ultimately, the decision lies with the police about whether or not an investigation will be conducted. The Home Office has advised that the police should only investigate where there are good grounds that they believe a criminal offence has been committed.[156]

Furthermore, members of the regulated sector are obliged to report fraud to the FSA in the following circumstances:

1. it becomes aware that an employee may have committed a fraud against one of its customers; or

2. it becomes aware that a person, whether or not employed by it, may have committed a fraud against it; or
3. it considers that any person, whether or not employed by it, is acting with intent to commit a fraud against it; or
4. it identifies irregularities in its accounting or other records, whether or not there is evidence of fraud; or
5. it suspects that one of its employees may be guilty of serious misconduct concerning his honesty or integrity and which is connected with the firm's regulated activities or ancillary activities.[157]

In determining whether or not the matter is significant, the firm must consider:

1. the size of any monetary loss or potential monetary loss to itself or its customers (either in terms of a single incident or group of similar or related incidents);
2. the risk of reputational loss to the firm; and
3. whether the incident or a pattern of incidents reflects weaknesses in the firm's internal controls (SUP 15.3.18G).[157]

The FSA Handbook also provides that the FSA 'the notifications under SUP 15.3.17 R are required as the FSA needs to be aware of the types of fraudulent and irregular activity which are being attempted or undertaken, and to act, if necessary, to prevent effects on consumers or other firms'.[158] Therefore, 'a notification under SUP 15.7.3 G should provide all relevant and significant details of the incident or suspected incident of which the firm is aware'.[158] Furthermore, 'if the firm may have suffered significant financial losses as a result of the incident, or may suffer reputational loss, and the FSA will wish to consider this and whether the incident suggests weaknesses in the firm's internal controls'.[159] If the institution has suffered a significant financial loss, or may suffer reputational loss as a result of the fraudulent activity, the FSA will take into account whether the incident suggests weaknesses in the institution's internal controls. If the fraud is committed by representatives and other Approved Persons, the FSA has the power to withdraw its authorisation and the possibility of prosecution.

The UKs policy towards fraud has gained momentum under the previous government, a willingness shared by the new coalition administration. However, there is still scope for improvement in the initiatives that have been introduced to tackle fraud. For example, the effectiveness of the criminalisation of fraud has been limited by the inadequacies of the Theft Acts and the common law offences, a position that has improved by the introduction of the Fraud Act. However, concerns still remain about the enforcement of these offences by the SFO and the CPS following the collapse of several high-profile instances of fraud. It is simply too early to determine whether the Fraud Act has made any difference to the prosecution of fraudsters. The coalition government must be commended for recognising the need to create single economic crime agency. The reporting of instances of suspicious fraudulent activities is fragmented with a number of different reporting mechanisms available. This causes confusion and delay.

TERRORIST FINANCING

In 2002, HM Treasury published a report that outlined the important contribution made by the government towards targeting the sources of terrorist financing.[160] In 2007, the government launched 'The financial challenge to crime and terrorism', which 'sets out for the first time how the public and private sector would come together to deter terrorists from using the financial system, detect them when they did, and use financial tools to disrupt them'.[13] In 2010, HM Treasury stated that 'the government's aim is to deprive terrorists and violent extremists of the financial resources and systems needed for terrorist-related activity, including radicalisation' (p. 5).[160] What can be deduced from these policy documents is that the UK's terrorist financing policy can be divided into three parts – the criminalisation of terrorist financing, the freezing of terrorist assets and the use of SARs.

Criminalisation of terrorist financing

The Prevention of Terrorism (Temporary Provisions) Act 1989 criminalised terrorist financing and allowed the government to seek the forfeiture of any money or other property that, at the time of the offence, he had in his possession or under his control.[161] The United Kingdom has achieved some success in Northern Ireland against the Irish Republican Army by virtue of offences created by this Act.[162] However, the effectiveness of the Act was questioned and it resulted in a review of the UK's terrorist policy.[50] The consultation paper concluded that the terrorist financing provisions contained several weaknesses including the fact that there were only four terrorist financing convictions between 1978 and 1989 (paragraph 6.14).[162] Bell argues that 'there have been no successful prosecutions for terrorist funding offences in Northern Ireland over the last 30 years and the forfeiture provisions under the Prevention of Terrorism (Temporary Provisions) Act 1989 have never been utilised'.[163] The Home Office recommended that the scope of the terrorist financing provisions should be extended to fund-raising for all terrorist purposes.[164] The provisions were amended by the Terrorism Act 2000, which created five offences. Section 15 makes it a criminal offence for a person to solicit,[165] or to receive,[166] or provide money or property on behalf of terrorists if the person knows or has reasonable cause to suspect that such money may be used for the purpose of terrorism.[167] By virtue of Section 16, a person commits an offence if he uses money or other property for terrorist purposes.[168] Furthermore, the person commits an offence if he possesses money or other property and he intends that it should be used, or has reasonable cause to suspect that it will be used, for the purposes of terrorism.[169] Section 17 states that a person commits an offence if he enters into or becomes concerned in an arrangement in which money[170] or property is made available to another and the person knows or has cause to suspect that it may be used for terrorism.[171] A person breaches Section 18 if he enters into or becomes concerned in an arrangement that facilitates the retention or control by or on behalf of another person of terrorist property by concealment,[172] by removal from the jurisdiction,[173] by transfer to nominees[174] or in any other way.[175] It is a defence for a person charged under Section 19 to prove that they either did not know, or had reasonable cause to suspect that the arrangement was associated to terrorist property.[176] The Terrorism Act 2000 has had a limited impact. Bell noted that 'the primary difficulty for the prosecution in terrorist finance cases, however, is to prove beyond a reasonable doubt that the property is terrorist property'.[177]

Between 2001 and 2008, a total of 34 people have been charged with the fund-raising offences under Sections 15–19 of the Terrorism Act 2000.[178] Yet only a total of 10 people have been convicted of fund-raising offences under the 2000 Act during the same time period (Home Office[178], p. 73).[179] However, Lord Carlile did note that 'there are some charges pending, and statistics to appear during 2009 are likely to demonstrate a high degree of vigilance by the authorities against the possession, potential transfer and use of terrorist funds'.[180] Bell realistically concluded 'a strategy against terrorist funding, this option is the most difficult from an investigative and prosecutorial perspective. Experience suggests, therefore, that only rarely will it be possible to prove terrorist finance charges, for example, where an exact tracing exercise has been carried out showing a financial trail between money in a particular account and arms purchases on behalf of a terrorist organisation'.[177]

The Terrorism Act 2000 grants law enforcement agencies additional investigative powers including financial information and account monitoring orders.[181] These have been described as 'an essential part of the legislation'.[182]

The purpose of an account monitoring order is to permit law enforcement agencies to discover and recognise relevant bank accounts while undertaking a terrorist investigation. In order to obtain an account monitoring order, an application must be made by a police officer, at least at the rank of superintendent,[183] before a circuit judge,[184] who must be satisfied that '(a) the order is sought for the purposes of a terrorist investigation, (b) the tracing of terrorist property is desirable for the purposes of the investigation, and (c) the order will enhance the effectiveness of the investigation'.[185] Once an order has been granted, it will enable the police to require a financial institution … to provide customer information for the purposes of the investigation'.[186] Schedule 6 defines 'customer information' as including information about whether or not a business relationship exists or existed between a financial institution and a customer, the customer's account details, name, address and date of birth.[187] Peddie, citing Lord Carlile's 2005 report on the performance of the Terrorism Act 2000, stated 'Lord Carlile opined that the financial information order system worked well and that there was a good level of co-operation between the police and financial institutions'.[188] The Terrorism Act 2000 states that if a person is convicted of an offence under Part III,[189] any property connected with the offence could be the subject of a forfeiture order.[190] This is referred to as criminal forfeiture.[191] The person subject to the order, once granted by a court, is required to give to a police officer as designated any property specified in the order.[192] The Terrorism Act 2000 also allows for Orders in Council to be made to permit foreign forfeiture orders to be recognised in England.[193]

The Anti-terrorism, Crime and Security Act 2001 amended the provisions for account monitoring orders, financial information orders and disclosure information orders. Under the 2001 Act, an account monitoring order may be granted by a Crown Court Judge provided that the court is satisfied that the order is sought for the purposes of a terrorist investigation, the tracing of terrorist property is desirable for the purposes of the investigation, and the order will enhance the effectiveness of the investigation.[194] Billings took the view that 'the effect of an account monitoring order is that the financial institution served with it must provide information of the description specified, for the period of the order and in accordance with it as to the time and place of the provision of information'.[195] The Anti-terrorism, Crime and Security Act 2001 states that a court can grant a Financial Information Order that compels a financial institution to disclose certain types of customer information for a terrorist investigation. A disclosure of information order allows for the disclosure of certain types of information and are very wide ranging. For example, they apply to any of the provisions listed in Schedule 4 of the Anti-terrorism, Crime and Security Act 2001.

Furthermore, the Counter-Terrorism Act (2008) contained a number of provisions that the Government state are designed to enhance counter-terrorism powers. Under the Act, HM Treasury gained additional powers to direct financial institutions to carry out a graduated range of financial restrictions on business connected with jurisdictions of concern regarding money laundering and terrorist financing.[196] Part 1 of Schedule 7 outlines the conditions for giving a direction. HM Treasury liaises with the FATF who can dictate when appropriate action needs to be taken about a particular country because of the inherent risks of money laundering or terrorist financing.[197] These powers were used in 2008 after the FATF stated that it 'remains particularly concerned about Iran's failure to address the risk of terrorist financing and the serious threat this poses to the integrity of the international financial system'.[198] In response, HM Treasury issued a notice based on the advice of the FATF.[199] In addition, if HM Treasury is of the opinion that a country poses a considerable threat to the UK's national interests because of an increased threat of money laundering of terrorist financing, it is permitted to issue a direction. Part 2 of the Schedule outlines the persons to whom a direction may be given. This includes, for example, people operating within the financial services sector.[200] The third part of Schedule 7 outlines the requirements that can be imposed by a direction. This includes, for example, imposing certain conditions on financial transactions or business relationships. The direction could also require an improved level of due diligence and that new transaction should not be entered into. Part 6 of Schedule 7 provides for the use of civil sanctions by the relevant enforcement authority. A civil sanction can be imposed if a person fails to comply with the obligation imposed by the direction. The Schedule 7 powers were used by HM Treasury in 2009 when it issued 'Direction to the UK financial sector to cease all business relationships and transactions with Bank Mellat and Islamic Republic of Iran Shipping Lines'.[201] Goldby notes that 'the Order was made on the basis' that 'the Treasury believe that activity in Iran that facilitates the development or production of nuclear weapons poses a significant risk to the national interests of the United Kingdom'.[201] The Order was imposed because of the perceived increased threat posed by Iran.[201] The Order provides that the financial sector cease any business relationships with Bank Mellat and IRISL. This means that Bank Mellat are not allowed to conduct any financial transactions in the United Kingdom.[202] In 2009, Bank Mellat have challenged the direction by HM Treasury.[203]

Asset freezing

The Anti-terrorism Crime and Security Act 2001 authorises the seizure of terrorist cash anywhere in the United Kingdom,[204] the freezing of funds at the start of an investigation,[205] the monitoring of suspected accounts,[206] the imposition of requirements on people working within financial institutions to report where there are reasonable grounds to suspect that funds are destined for terrorism and to permit HM Treasury to freeze assets of foreign individuals and groups. Part II of the Act permits HM Treasury to freeze the assets of overseas governments or residents who have taken, or are likely to take, action to the detriment of the UK's economy or action constituting a threat to the life or property of a national or resident of the United Kingdom.[207] HM Treasury is allowed to make a freezing order if two statutory requirements are met. First, they must reasonably believe that action threatening the UK's economy or the life or property of UK nationals or residents has taken place or is likely to take place.[208] Second, the persons involved in the action must be resident outside the United Kingdom or be an overseas government.[209] The freezing order prevents all persons in the United Kingdom from making funds available to, or for the benefit of, a person or persons specified in the order.[210] HM Treasury is also required to keep the freezing order under review and to determine whether it should continually be enforced over a period of 2 years.[211] HM Treasury has frozen the assets of individuals and organisations that were suspected of financing terrorism.[212] The government regularly updates a list of organisations and individuals whose accounts have been frozen.[213] Before 2001, HM Treasury froze £90 million of terrorist assets, which is attributed towards the fall of the Taliban in Afghanistan in 2002.[214] After this initial success, HM Treasury has only been able to freeze a further £10 million.[215] It has been suggested that this success can be measured in the actual amount of money frozen 'and though the headline figure thus generated is doubtless politically satisfying to some, it is not a measure of effectiveness'.[216] In July 2009, Lord Myners reported that 'as of the end of June 2009, a total of 237 accounts containing £607 661 of suspected terrorist funds were frozen in the UK'.[217] In October 2007, HM Treasury's Asset Freezing Unit was created. Until this date, the Bank of England had its own Financial Sanctions Unit, and this was transferred under the ambit of HM Treasury. The Asset Freezing Unit is responsible for legislation on financial sanctions, the implementation and administration of domestic financial sanctions; the designation of terrorist organisations, the implementation and administration of international financial sanctions in the United Kingdom, liaising with the Foreign and Commonwealth Office and collaborating with international partners to develop the international frameworks for asset freezing. The FATF concluded that 'the UK has established a terrorist asset freezing regime which works well in practice. It has an effective domestic designation process which appears rapid, easy and efficient. The system can operate independently of the UN and EU listing mechanisms, where necessary'.[218] Therefore, the United Kingdom was fully compliant with the international standards and this resulted in the government stating that the United Kingdom was 'the first country to be awarded the fully compliant rating' in relation to asset freezing.[219]

The United Kingdom has implemented the Terrorism (United Nations Measures) Order to give legal effect to Security Council Resolution 1373.[220] The Order also gives effect for the enforcement of EC Regulation 2580/2001, which permits for the designation of people within this regulation for such measures that relate to, *inter alia*, the freezing of funds, financial assets and economic resources.[221] HM Treasury took the view that the aim of the Order 'was enhanced to provide further restrictions on making funds, economic resources and financial services available to anyone who has been designated in the UK by the Treasury as a person suspected of committing, attempting to commit, participating in or facilitating acts of terrorism'.[222] By virtue of Article 4 of the Order, HM Treasury has been given the power to designate a person if four conditions are met. HM Treasury has reasonable grounds to suspect that a person is or may be (a) a person who commits, attempts to commit, participates in or facilitates the commission of acts of terrorism; (b) a person named in the Council Decision; (c) a person owned or controlled, directly or indirectly, by a designated person; or (d) a person acting on behalf of or at the direction of a designated person. Under Article 5 of the Order, HM Treasury is required to undertake appropriate measures to publicise the direction or to notify specific people and to inform the person identified in the direction. Furthermore, under Article 7 of the 2006 Order, a person is prohibited from 'dealing with funds, financial assets and economic resources of anyone who commits, attempts to commit, participates in or facilitates the commission of acts of terrorism; designated persons; anyone owned or controlled by them or anyone acting on their behalf of or at their direction'. The article makes it a criminal offence to contravene this prohibition. Article 8 of the Order prohibits making funds, financial assets, economic resources or financial services available to anyone in respect of whom Article 7 applies. The article makes it a criminal offence to contravene this prohibition.

The legality of the Terrorism (United Nations Measures) Order 2006 was challenged in *A* v. *HM Treasury*.[223] Here, the appellants required orders from the court to quash the freezing of their assets under the 2006 Terrorism (United Nations) Order.[224] Collins J decided that the orders granted should be set aside against five applicants on three grounds. First, that parliamentary approval should have been sought and that they should not have been made by Order in Council. Second, the court decided that it was impossible to determine how the test adopted by HM Treasury, that it had reasonable grounds for suspecting the applicants was of could be committing terrorists acts, could represent a necessary means of applying the relevant United Nations Resolution. Third, that the 2006 Order created criminal offences that contravened the principle of legal certainty. The interpretation of the phrase 'economic resources' was crucial, and the court decided that the definition of this phrase meant that the family members of the applicants did not know whether they were breaching the Order or whether they needed a licence from HM Treasury.[225] HM Treasury petitioned the Court of Appeal,[226] who considered four issues. First, was the 2006 Terrorism

Order unlawful and should it be quashed? Second, what was impact of the lack of procedural safeguards in the 2006 Order? Third, whether the offences created under Articles 7 and 8 of the Order satisfied the principles of legal certainty and proportionality? Finally, whether the Al-Qaeda and Taliban (United Nations Measures) 2006 was unlawful because a person placed on the United Nations Sanctions Committee list has no appeal mechanism against that decision. The Court of Appeal held that the reasonable ground test adopted by HM Treasury did not go beyond the ambit of Resolution 1373, but the requirement in the 2006 Order of 'or may be' did go further than the Resolution. Therefore, it determined that the directions granted by HM Treasury were quashed. Second, the Court of Appeal stated that the courts must be relied on to guarantee that satisfactory procedural protection is upheld for applicants under the Order.[227] Third, the provisions of the licensing system under the Order were proportionate and legally certain. Finally, the Al-Qaeda and Taliban (United Nations Measures) 2006 was lawful.

In response, the government has introduced the Terrorism (United Nations Measures) Order,[228] which provides that a direction will cease to have effect 12 months after it is made, but HM Treasury has the ability to renew a direction.[229] The Order revises the prohibition on making funds, economic resources and financial services available for the benefit of a designation person so that they only apply if the designated person obtains, or is able to obtain, a significant financial benefit. Furthermore, the ban on making funds, economic resources and financial available directly to a designated person, as outlined above, are unaltered. Furthermore, the 2009 Order changes the prohibition on making economic resources available to a designated person by providing a defence to that person if they did not know and had no reasonable cause to suspect that economic resources that they provided to a designated person would be likely to be exchanged or used in exchange for funds, goods or services. The Financial Services Secretary to the Treasury, Lord Myners, took the view that 'overall, these changes will improve the operation of the asset-freezing regime, ensure that it remains fair and proportionate and help facilitate effective compliance by ensuring that prohibitions are more tailored and clearer in how they apply'.[217] The matter finally came before the Supreme Court who also considered the legitimacy of the Terrorism (United Nations Measures) Order and the Al-Qaeda and Taliban (United Nations Measures) Order 2006. The Supreme Court determined that both of the Orders were *ultra vires* and HM Treasury swiftly responded by publishing the Draft Terrorist Asset Freezing Bill (2010) and implementing the Terrorist Asset-Freezing (Temporary Provisions) Act 2010. Johnston and Nanopoulos took the view that the Act 'deems all of the impugned Orders in Council under the 1946 Act to have been validly adopted and thus retains in force all directions made under those Orders; the Act will expire on 31 December 2010'.[230]

Reporting requirements

Schedule 2 Part III to the Anti-terrorism, Crime and Security Act 2001 inserted s. 21A into the Terrorism Act 2000 and created the offence of failure to disclose for the regulated sector. A person commits an offence under this section if three conditions are met. The first condition is that the accused knows or suspects, or has reasonable grounds for knowing or suspecting that a person has committed an offence under Sections 15–18 of the Terrorism Act 2000.[231] The second condition is that the information or other matter upon which the accused has based his knowledge or suspicion, or which gives reasonable grounds for such knowledge of suspicion, came to him in the course of a business that operates within the regulated sector.[232] The third condition is that the accused does not disclose the information or other matter to a constable or nominated officer, normally a money laundering reporting officer as soon as practicable after he received the information.[233] Lord Carlile took the view that these reporting obligations are 'still under-publicised duty, to which the only major statutory exception is genuine legal professional privilege'.[182] Since the introduction of the new section 21A, there have been no trials in which this new section have been tested (p. 18).[233] First, that the defendant knows or suspects, or has reasonable grounds for knowing or suspecting that another person has committed an offence under Sections 15–18 of the Terrorism Act 2000.[234] The second condition is that the information or other matter on which his knowledge or suspicion is based, or which gives reasonable grounds for such knowledge or suspicion, came to him in the course of a business in the regulated sector.[234] The final condition is that he does not disclose the information or other matter to a constable or a nominated officer as soon as is practicable after it comes to him.[235] A person does not commit an offence if they had a reasonable excuse for not disclosing the information or other matter or he is a professional legal adviser and the information or other matter came to him in privileged circumstances.[235] Lord Carlile took the view that 'this is a wide and still under-publicised duty, to which the only major statutory exception is genuine legal professional privilege'.[236] The Anti-terrorism, Crime and Security Act 2001 amended the Terrorism Act 2000 and inserted a defence of protected disclosures.[237] In order for this defence to be utilised, three conditions must be met. The first condition is that the information or other matter disclosed came to the person making the disclosure (the discloser) in the course of a business in the regulated sector.[238] The second condition is that the information or other matter causes the discloser to know or suspect, or gives him reasonable grounds for knowing or suspecting that a person has committed an offence as outlined above under Sections 15–18 of the Terrorism Act 2000.[239] The third and final condition is that the disclosure is made to a constable or a nominated officer as soon as is practicable after the information or other matter comes to the discloser.[240] A new S. 21ZA was inserted into the Terrorism Act in December 2007.[241] This amendment allows people to undertake unlawful acts provided there is consent by an authorised officer and its aim is to facilitate the discovery of offences. The amendments also aim to protect disclosures after disclosures are made after entering into such arrangements. Section 21ZC also provides a defence of reasonable excuse for not disclosing. An individual or organisation who suspects that an offence has been committed under the Terrorism Act 2000 required to complete an SAR, which is then sent to SOCA for processing. Lord Carlile, in his annual report on the operation of the TA 2000, commented that 'there are concerns in the business sector about difficulties of compliance and the serious consequences that may flow from this'.[242] In 2005, the Lander Review noted that 'in 2005, just under 2100 of the total SARs (1 per cent) were judged by the FIU terrorism team to be of potential interest in a terrorist context, of which about 650 were passed on to the NTFIU for more detailed investigation. There was a slight peak of reports of interest following the events of 7 and 21 July 2005'.[243] The number of terrorist-related SARs submitted between 2007 and 2008 was 956,[244] whereas the number between 2008 and 2009 was 703.[245] The usefulness of SARs in relation to terrorist financing was highlighted by SOCA who took the view that 'although the numbers continue to be small in proportion to the total numbers of SARs, their value can be significant, as has been demonstrated in previous years in which major terrorist incidents have taken place. All UK counter-terrorism investigations have a financial aspect to them, and the UKFIU Terrorist Finance Team has continued to provide support to these over the year' (p. 17).[245]

CONCLUSIONS

Money laundering

The United Kingdom has fully complied with its international obligations under the Vienna and Palermo Conventions and its requirements under the Money Laundering Directives. In fact, the UK's measures go beyond its international obligations. The criminalisation of money laundering occurred in 1986, since when the legislative frameworks have been updated and codified by the PCA 2002. The involvement of the FSA is an innovative attempt to reduce the impact of money laundering. It is the first time that a financial regulatory body in the United Kingdom has been given such a specific role, a position that can be contrasted with the United States. The FSA has implemented a costly and at times unnecessarily complicated regime, yet they have at least attempted to lessen the AML obligations by implementing SYSC. The scheme introduced by the FSA will, in the main, do little to discourage well-organised criminals from laundering money in the United Kingdom. The SARs reporting requirements have imposed significant administrative burdens on financial institutions. They have led to an increased level of record-keeping, report filing and internal policing requirements. The imposition of even more mandatory reporting requirements was inevitable given the government's tough stance towards money laundering. It is questionable, however, whether the filing of an SAR will make any difference given the difficulties in securing prosecutions in money laundering offences. It is also possible to argue that the reporting requirements have created a 'needle-in-the-haystack' problem, especially given the large number of SARs annually submitted. In its 2004 policy document, HM Treasury referred to 2003 IMF review of the UK's AML legislative framework and policy. The review concluded that 'the UK has a comprehensive legal, institutional and supervisory regime for AML'.[17] However, the UK's AML approach can be criticised because of its ambit and burden imposed on the sectors that are forced to comply with it.[246] Maylam noted that despite the best efforts of the United Kingdom, the fight against money laundering 'can only be effective if conducted on a global basis with a spirit of co-operation and legal compatibility'.[247]

Fraud

The UK fraud policy has gathered pace following the publication of the Fraud Review in 2006, but is still in a state of flux. The policy adopted is very similar to that adopted in the United States, but the criminalisation of fraud can be contrasted with the approach in the United States. The United Kingdom has a single Fraud Act, which criminalises different types of fraudulent activities and provides prosecutors with new powers to tackle fraud. The second part of its anti-fraud policy concerns primary and secondary agencies, and it is this part that is need of fundamental reform. There is no single agency that takes a lead role in tackling fraud; there are simply too many agencies who performing the same function, a position that has deteriorated by the fact that not one government department performs a similar function to the Department of Justice. For example, HM Treasury has been charged with developing and implementing the UK's policies towards money laundering and terrorist financing, yet it has very little to do with the UK's fraud policy. Furthermore, the Home Office, who has been charged with tackling the problems associated with organised crime, does little to tackle fraud. Therefore, it is recommended that a single government department be given the task of tackling all types of financial crime, it seems logical that this task is given to HM Treasury, given its experience with money laundering and terrorist financing. Another example of the overlap between anti-fraud agencies relates to the fact that both the SFO and FSA have the ability to conduct investigations and initiate prosecutions. The NFA has been given a 3-year budget of £29 million to tackle an industry that is worth £30 billion. Therefore, it faces an improbable mission to reduce the extent of fraud with a very small budget. This makes little or no sense. The UK government should develop unitary financial crime agency that incorporates the functions of the agencies outlined above. It is possible to argue that this process has already started with the merger of several agencies including the

National Crime Squad, the National Criminal Intelligence Service and the Assets Recovery Agency into SOCA. The final part of the UK's policy can be contrasted with that of the United States. The primary legislation that imposes reporting obligations is the PCA 2002, under which fraud is reported to SOCA. However, in some circumstances allegations of fraud are reported to banks, the police and the regulated sector reports to the FSA. The system needs clarification and it has not been assisted by the creation of the NFRC. In the United States, allegations of fraud are reported to FinCEN, and it is suggested that the United Kingdom should adopt a similar reporting strategy, and that all suspicious transactions relating to fraud should be reported to SOCA.

The United Kingdom has had specific anti-terrorist financial legislation in place since 1989 and it has learnt a number of important lessons from the terrorist campaign conducted by the Irish Republican Army and other para-military organisations. The government has fully implemented UN Resolutions and it must be commended for going beyond the scope of its international obligations. The United Kingdom has adopted a similar approach towards the prevention of terrorist finance as that utilised by the United States. The Terrorism Act 2000 overhauled the terrorist financing offences that yielded a derisory four convictions over a 10-year period. This could be explained by the sheer number of sources of financing available to terrorist organisations. The ability to freeze the assets of suspected terrorist organisations has been available since 1964, yet it was not until the fall of the Taliban that HM Treasury froze assets over £80 million. The ability of the government to freeze the assets of terrorist organisations initially appeared to be an effective weapon against terrorist finance. Subsequently, HM Treasury has only frozen a further £10 million of suspected terrorist assets. However, the ability to freeze the assets of suspected terrorists has been limited to the decision in *A* v. *HM Treasury*. Therefore, this part of the policy must be criticised because, like the US stance, it is a short-term solution to a long-term problem. The effectiveness of the reporting requirements under the Terrorism Act 2000 and the Anti-terrorism Crime and Security Act 2001 must also be queried, owing to the extensive sources of funding options available to terrorists.

REFERENCES AND NOTES

1 Haines, J. (2009) The national fraud strategy: New rules to crackdown on fraud. *Company Lawyer* 30(7): 213.

2 BBC News. (2009) Fraudster Madoff gets 150 years. 29 June, http://news.bbc.co.uk/1/hi/business/8124838.stm, accessed 3 November 2010.

3 Association of Chief Police Officers. (2008) Police committed to tackling mortgage fraud. 5 March 2008, http://www.acpo.police.uk/pressrelease.asp?PR_GUID=%7B7F278B1E-CA47-4C00-AFD2-CC599E4BA786%7D, accessed 13 September 2009.

4 Chris Swecker, former FBI Assistant Director, Criminal Investigative Division, Introductory Statement: House Financial Services Subcommittee on Housing and Community Opportunity, 7 October 2004, as cited in Federal Bureau of Investigation. (2008) *2007 Mortgage Report*. Washington DC: Federal Bureau of Investigation.

5 International Monetary Fund. (2001) *Financial System Abuse, Financial Crime and Money Laundering – Background Paper*. Washington DC: International Monetary Fund, p. 5.

6 Financial Services and Markets Act 2000, s. 6(3).

7 Financial Action Task Force. (2004) *Report on Money Laundering and Terrorist Financing Typologies 2003–2004*. Paris: Financial Action Task Force.

8 National Audit Office. (2007) *The Assets Recovery Agency – Report by the Comptroller and Auditor General*. London: National Audit Office, p. 4.

9 Vaithilingam, S. and Nair, M. (2007) Factors affecting money laundering: Lesson for developing countries. *Journal of Money Laundering Control* 10(3): 352–366, at 353. Of the different types of financial crime discussed in this article it has been argued by several commentators that money laundering has greatest potential to affect a nation's economy and financial services system. See for example Paradise, T. (1998) Money laundering and international political economy. *Journal of Money Laundering Control* 1(3): 229–244 and Quirk, P. (1997) Money laundering: Muddying the macro economy. *Finance and Development* 34(1): 7–9.

10 For an excellent commentary on the effects of money laundering on economies see Unger, B. (2007) *The Scale and Impacts of Money Laundering*. Cheltenham, UK: Edwards Elgar, pp. 109–182.

11 The 9/11 Commission. (2004) *The 9/11 Commission Report – Final Report of the National Commission on Terrorist Attacks upon the United States*. London: Norton & Company, p. 170.

12 Financial Action Task Force. (2007) *Summary of Third Mutual Evaluation Report Anti-money Laundering and Combating the Financing of Terrorism – United Kingdom of Great Britain*

and Northern Ireland. Paris: Financial Action Task Force, pp. 1–2.

13 HM Treasury. (2007) *The Financial Challenge to Crime and Terrorism*. London: HM Treasury, p. 6.

14 Home Office. (2004) *One Step Ahead – A 21st Century Strategy to Defeat Organised Crime*. London: Home Office, p. 1.

15 Scanlan, G. (2006) The enterprise of crime and terror – The implications for good business. Looking to the future – Old and new threats. *Journal of Financial Crime* 13(2): 164–176, at 164.

16 HM Treasury. (2002) *Combating the Financing of Terrorism*. London: HM Treasury, p. 11.

17 HM Treasury. (2004) *Anti-money Laundering Strategy*. London: HM Treasury.

18 It is important to note that other countries within the European Union have adopted a risk-based approach towards money laundering regulation. See Geiger, H. and Wuensch, O. (2007) The fight against money laundering: An economic analysis of a cost-benefit paradoxon. *Journal of Money Laundering Control* 10(1): 91–105.

19 For a similar view see Leong, A. (2007) Chasing dirty money: domestic and international measures against money laundering. *Journal of Money Laundering Control* 10(2): 140–156, at 141–142.

20 It is important to note that drug money laundering was initially criminalised by the Drug Trafficking Offences Act 1986, while money laundering was criminalised by virtue of the Criminal Justice Act 1993.

21 Forston, R. (2008) Money laundering offences under POCA 2002. In: W. Blair and R. Brent (eds.) *Banks and Financial Crime – The International Law of Tainted Money*. Oxford, UK: Oxford University Press, pp. 155–202, at 157.

22 Proceeds of Crime Act 2002, s. 327.

23 Proceeds of Crime Act 2002, s. 328.

24 Proceeds of Crime Act 2002, s. 329.

25 For a definition of these terms see Forston[21] at pp. 160–161.

26 Proceeds of Crime Act 2002, s. 330.

27 Proceeds of Crime Act 2002, s. 331.

28 Proceeds of Crime Act 2002, s. 332.

29 Proceeds of Crime Act 2002, s. 333A.

30 Proceeds of Crime Act 2002, s. 342.

31 Proceeds of Crime Act 2002, s. 327(1). The interpretation of criminal property broad because it includes property anywhere in the world, Proceeds of Crime Act 2002, s. 340(9).

32 Proceeds of Crime Act 2002, s. 340(1). For a critical discussion of the interpretation of this phrase see Bentley, D. and Fisher, R. (2008) Criminal property under PCOA 2002 – Time to clean up the law? *Archbold News* 2: 7–9.

33 Proceeds of Crime Act 2002, s. 340(3)(a).

34 Hudson, A. (2009) *The Law of Finance*. London: Sweet and Maxwell, p. 345.

35 Proceeds of Crime Act 2002, s. 340(3)(b).

36 Proceeds of Crime Act 2002, s. 3403(a).

37 Proceeds of Crime Act 2002, s. 338.

38 Proceeds of Crime Act 2002, s. 338(1)(a).

39 Proceeds of Crime Act 2002, s. 338(1)(b).

40 Proceeds of Crime Act 2002, s. 327(2).

41 Proceeds of Crime Act 2002, s. 328(1).

42 This section amends and updates section 50 of the Drug Trafficking Act 1994 and section 93A of the Criminal Justice Act 1988, section 38 of the Criminal Law (Consolidation) (Scotland) Act 1995 and Article 46 of the Proceeds of Crime (Northern Ireland) Order 1996.

43 Proceeds of Crime Act 2002, s. 329(1).

44 Proceeds of Crime Act 2002, s. 329(1)(a).

45 Proceeds of Crime Act 2002, s, 329(1)(b).

46 Proceeds of Crime Act 2002, s, 329(1)(c).

47 Proceeds of Crime Act 2002, s, 329(1)(d).

48 Proceeds of Crime Act 2002, s, 329(2A), (2B).

49 Proceeds of Crime Act 2002, s, 329(2C).

50 The foundations of the offences created by the Terrorism Act 2000 are to be found in Home Office. (1998) *Legislation Against Terrorism – A Consultation Paper*. London: Home Office, For an interesting debate on the merger of the two offences of money laundering and terrorist laundering, see Alexander, R. (2009) Money laundering and terrorist financing: Time for a combined offence. *Company Lawyer* 30(7): 200–204.

51 Financial Services and Markets Act 2000, s. 146.

52 Financial Services Authority. (2006) *Money Laundering Handbook*. London: Financial Services Authority, The FSA adopted the MLR 1993 via the Financial Services and Markets Act 2000 Regulations (Relating to Money Laundering Regulations) 2001, S.I. 2001/1819.

53 Financial Services Authority. (2006) *FSA Handbook*. London: Financial Services Authority, at SYSC 3.1.1.

54 See Financial Services Authority[53], at SYSC 3.2.6 C.

55 See Financial Services Authority[53], at SYSC 3.2.6 H and I.

56 Financial Services and Markets Act 2000, ss. 165–166.

57 Financial Services and Markets Act 2000, ss. 167–168.

58 Financial Services and Markets Act 2000, s. 169.

59 Financial Services and Markets Act 2000, s. 172.

60 Financial Services and Markets Act 2000, s. 402 (1)(a). The scope of the FSA's prosecutorial powers were approved by the Supreme Court in *R* v. *Rollins* [2010] UKSC 39. See Ryder, N. (2010) The financial services authority and proceeds of crime act – too little too late? *Financial Regulation International*, September: 8–9.

61 Financial Services and Markets Act 2000, s. 206 (1).

62 See generally Ryder, N. (2008) The financial services authority and money laundering: A game of cat and mouse. *Cambridge Law Journal* 67(3): 635–653.

63 See for example Financial Services Authority. (2008) FSA fines firm and MLRO for money laundering controls failings. 29 October, http://www.fsa.gov.uk/pages/Library/Communication/PR/2008/125.shtml, accessed 29 October 2008.

64 Financial Services Authority. (2010) FSA fines Alpari and its former money laundering reporting officer, Sudipto Chattopadhyay for anti-money laundering failings. 5 May, http://www.fsa.gov.uk/pages/Library/Communication/PR/2010/077.shtml, accessed 6 May 2010.

65 Money Laundering Regulations 2007, S.I. 2007/2157.

66 It is important to note that the reporting obligations imposed by the Proceeds of Crime Act 2002 have been severely criticised by the Court of Appeal in *UMBS Online Ltd* [2007] EWCA Civ 406.

67 Proceeds of Crime Act 2002, s. 328(1), s.330(2)(a) and s.331(2)(a).

68 Proceeds of Crime Act 2002, s. 330(2)(b) and s.331(2)(b).

69 Brown, G. and Evans, T. (2008) The impact: The breadth and depth of the anti-money laundering provisions requiring

reporting of suspicious activities. *Journal of International Banking Law and Regulation* 23(5): 274–277, at 276.

70 It is important to note that the Court of Appeal in *R* v. *Da Silva* [2006] EWCA Cro., 1654 rejected the argument by Da Silva that the court 'could not imply a word such as "reasonable" into the relevant statutory provision'. See Brown and Evans[69], p. 275.

71 *K Ltd* v. *National Westminster Bank plc* [2007] WLR 311.

72 Wadsley, J. (2008) Painful perceptions and fundamental rights – Anti-money laundering regulation and lawyers. *Company Lawyer* 29(3): 65–75, at 67.

73 Other guidance for the definition of suspicion is offered by Joint Money Laundering Steering Group. (2007) *Prevention of Money Laundering/Combating Terrorist Financing Guidance for the UK Financial Sector Part 1*. London: Joint Money Laundering Steering Group, Guidance 6.9.

74 [2006] EWCA Cro,. 1654. This case related to the interpretation of the phrase under the Criminal Justice Act 1988.

75 [2006] EWCA Civ 1039.

76 Forston[21], at p. 163.

77 Brown and Evans[69], at p. 275. For a more detailed discussion see *K Limited* v. *National Westminster Bank* [2006] EWCA Civ 1039.

78 [2010] EWCA Civ 31; [2010] Lloyd's Rep F.C. 276 (CA (Civ Div)). For an analysis of the impact of this case see Marshall, P. (2010) Does Shah v HSBC Private Bank Ltd make the anti-money laundering consent regime unworkable? *Butterworths Journal of International Banking & Financial Law* 25(5): 287–290.

79 Stanton, K. (2010) Money laundering: a limited remedy for clients. *Professional Negligence* 26(1): 56–59, at 58.

80 See for example KPMG. (2003) *Money Laundering: Review of the Reporting System*. London: KPMG.

81 Fleming, M. (2005) *UK Law Enforcement Agency Use and Management of Suspicious Activity Reports: Towards Determining the Value of the Regime*. London: University College London.

82 Serious Organised Crime Agency. (2006) *Review of the Suspicious Activity Reports Regime*. London: Serious Organised Crime Agency.

83 Sarker, R. (2006) Anti-money laundering requirements: Too much pain for too little gain. *Company Lawyer* 27(8): 250–251, at 251.

84 KPMG[80], at p. 14.

85 Serious Organised Crime Agency. (2009) *The Suspicious Activity Reports Regime Annual Report 2008*. London: Serious Organised Crime Agency, p. 14.

86 Leong[19], at p. 142.

87 Home Office. (2004) *Report on the Operation in 2004 of the Terrorism Act 2000*. London: Home Office, pp. 19–20.

88 The government announced that it intended to introduce a radical overhaul of the laws on fraud in its 2005 general election manifesto Labour Party. (2005) *Labour Party Manifesto – Britain Forward Not Back*. London: Labour Party.

89 Sarker, R. (2007) Fighting fraud – A missed opportunity? *Company Lawyer* 28(8): 243–244, at 243.

90 Attorney General's Office. (2006) *Fraud Review – Final Report*. London: Attorney General's Office, p. 4.

91 National Fraud Authority. (2009) National Fraud Reporting Centre's '0300' line launches in the West Midlands, http://www.attorneygeneral.gov.uk/nfa/WhatAreWeSaying/NewsRelease/Documents/NFRC%20launch%2026%20Oct%2009.pdf, accessed 3 March 2010.

92 Attorney General's Office[90], at p. 10. The effectiveness of this decision has been questioned. See for example Rider, B. (2009) A bold step? *Company Lawyer* 30(1): 1–2, at 1.

93 Other noteworthy attempts to tackle fraud before the Theft Act were the Prevention of Fraud (Investments) Act 1958 and the Financial Services Act 1986.

94 See generally Kiernan, P. and Scanlan, G. (2003) Fraud and the law commission: The future of dishonesty. *Journal of Financial Crime* 10(3): 199–208.

95 Wright, R. (2007) Developing effective tools to manage the risk of damage caused by economically motivated crime fraud. *Journal of Financial Crime* 14(1): 17–27, at 18.

96 For a more detailed illustration of this problem see generally *R* v. *Preddy* [1996] AC 815, 831.

97 Specifically the Law Commission were asked to 'to examine the law on fraud, and in particular to consider whether it: is readily comprehensible to juries; is adequate for effective prosecution; is fair to potential defendants; meets the need of developing technology including electronic means of transfer; and to make recommendations to improve the law in these respects with all due expedition. In making these recommendations to consider whether a general offence of fraud would improve the criminal law'. See HC Debates 7 April 1998 c.176-177WA.

98 The Law Commission. (1999) *Legislating the Criminal Code Fraud and Deception – Law Commission Consultation Paper no 155*. London: Law Commission.

99 The Law Commission also published an informal discussion paper in 2000. See Law Commission. (2000) *Informal Discussion Paper: Fraud and Deception – Further Proposals From the Criminal Law Team*. London: Law Commission.

100 For an analysis of the Law Commission's report see Kiernan and Scanlan[94].

101 The Fraud Act 2006 (Commencement) Order 2006, S.I. 2006/3500.

102 For a detailed commentary and analysis of the Fraud Act see Ormerod, D. (2007) The Fraud Act 2006 – Criminalising lying? *Criminal Law Review*, March: 193–219, However, it is important to note that not all of the offences under the Theft Act 1968 have been abolished. For example false accounting (Theft Act 1968, s. 17), the liability of company directors (Theft Act 1968, s. 18), false statements by company directors (Theft Act 1968, s. 19) and dishonest destruction of documents (Theft Act 1968, s. 20(1)).

103 Fraud Act 2006, s. 2.

104 Fraud Act 2006, s. 3.

105 Fraud Act 2006, s. 4.

106 Dennis, I. (2007) Fraud Act 2006. *Criminal Law Review*, January: 1–2, at 1.

107 Scanlan, G. (2008) Offences concerning directors and officers of a company: Fraud and corruption in the United Kingdom – The present and the future. *Journal of Financial Crime* 15(1): 22–37, at 25.

108 Wright stated that 'it is reassuring that the newly formed Serious Organised Crime Agency … will have non-fiscal fraud as one of its major priorities'. See Wright[95], at p. 14.

109 Bosworth-Davies, R. (2009) Investigating financial crime: The continuing evolution of the public fraud investigation

role – A personal perspective. *Company Lawyer* 30(7): 195–199, at 196.
110 See generally Wright, R. (2003) Fraud after Roskill: A view from the serious fraud office. *Journal of Financial Crime* 11(1): 10–16.
111 The Committee was asked to 'consider in what ways the conduct of criminal proceedings in England and Wales arising from fraud can be improved and to consider what changes in existing law and procedure would be desirable to secure the just, expeditious and economical disposal of such proceedings'. See Fraud Trials Committee Report (1986) HMSO.
112 For a detailed commentary of the Roskill Commission see Levi, M. (2003) The Roskill Fraud Commission revisited: An assessment. *Journal of Financial Crime* 11(1): 38–44.
113 Criminal Justice Act 1987, s. 1.
114 Criminal Justice Act 1987, s. 2. It is important to note that the SFO has other investigative and prosecutorial powers under the Fraud Act 2006, the Theft Act 1968, the Companies Act 2006, the Serious Crime Act 2007, the Serious Organised Crime and Police Act 2005, the Proceeds of Crime Act 2002 and the Regulation of Investigatory Powers Act 2000.
115 Serious Fraud Office. (2010) *Achievements 2009–2010*. London: Serious Fraud Office, p. 3.
116 Mahendra, B. (2002) Fighting serious fraud. *New Law Journal* 152(7020): 289.
117 Wright[110], at p. 10.
118 de Grazia, J. (2008) *Review of the Serious Fraud Office – Final Report*. London: Serious Fraud Office.
119 de Grazia[118], p. 129.
120 Crown Prosecution Service. (2009) DPP announces new head of Fraud Prosecution Division. 31 July, http://www.cps.gov.uk/news/press_releases/136_09/, accessed 22 January 2010.
121 Masters, J. (2008) Fraud and money laundering: The evolving criminalisation of corporate non-compliance. *Journal of Money Laundering Control* 11(2): 103–122, at 104.
122 HM Crown Prosecution Service Inspectorate. (2008) *Review of the Fraud Prosecution Service*. London: HM Crown Prosecution Service Inspectorate, p. 5.
123 Bosworth-Davies[109], at p. 198.
124 This would have seen the FSA focusing its efforts on specific types of fraud or dishonesty which constitute the greatest areas of concern, and where they can make a difference.
125 This would include, for example, considering the firms' systems and controls against fraud in more detail in our supervisory work, including how firms collect date on fraud and dishonesty.
126 The third approach would involve the FSA liaising closely with the financial sector and other interested parties in order to achieve a more effective approach towards fraud prevention in the financial services sector.
127 The final proposed method would include codification and clarification of the relevant fraud risk management provisions of the Handbook.
128 Robinson, P. (2004) The FSA's new approach to fraud – Fighting fraud in partnership. London, 26 October.
129 For example, in 2008 the FSA successfully prosecuted William Radclyffe for offences under the Theft Acts, the Financial Services Act 1986 and the Financial Services and Markets Act 2000. See Financial Services Authority. (2008) False stockbroker sentenced to 15 months. 13 February, http://www.fsa.gov.uk/pages/Library/Communication/PR/2008/011.shtmlm, accessed 28 March 2010.
130 Financial Services Authority. (2006) FSA fines Capita Financial Administrators Limited £300 000 in first anti-fraud controls case. 16 March, http://www.fsa.gov.uk/pages/Library/Communication/PR/2006/019.shtml, accessed 16 March 2006.
131 Financial Services Authority. (2008) *Financial Services Authority Annual Report 2007/2008*. London: Financial Services Authority, p. 23.
132 Financial Services Authority. (2007) FSA fines Nationwide £980 000 for information security lapses. 14 February, http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/021.shtml, accessed 14 February 2007.
133 Financial Services Authority. (2007) FSA fines Norwich Union Life £1.26 million. 4 November, http://www.fsa.gov.uk/pages/Library/Communication/PR/2007/130.shtml, accessed 8 October 2010.
134 Financial Services and Markets Act 2000, s. 56.
135 In February 2010 the FSA recovered £270 000 for defrauded investors who were advised to buy shares in Eduvest plc Financial Services Authority. (2010) FSA returns £270 000 to victims of share fraud. 23 February, http://www.fsa.gov.uk/pages/Library/Communication/PR/2010/032.shtml, accessed 21 March 2010.
136 National Fraud Authority. (2010) *The National Fraud Strategy – A New Approach to Combating Fraud*. London: National Fraud Authority, p. 10.
137 For a more detailed discussion of how this is to be achieved see The Attorney General's Office. (2008) *Extending the Powers of the Crown Court to Prevent Fraud and Compensate Victims: A Consultation*. London: Attorney General's Office.
138 Rider[92], at p. 1.
139 Bosworth-Davies[109], at p. 199.
140 National Fraud Authority[136], at p. 3.
141 Kiernan, P. (2003) The regulatory bodies fraud: Its enforcement in the twenty-first century. *Company Lawyer* 24(10): 293–299, at 295.
142 Office of Fair Trading. (n/d) *Prevention of Fraud Policy*. London: Office of Fair Trading.
143 See for example Office of Fair Trading. (2009) *Scamnesty 2010 Campaign Strategy*. London: Office of Fair Trading.
144 See for example Office of Fair Trading. (2003) *Memorandum of Understanding Between the Office of Fair Trading and the Director of the Serious Fraud Office*. London: Office of Fair Trading.
145 See for example Office of Fair Trading. (2005) OFT and Nigerian financial crime squad join forces to combat spam fraud. 4 November, http://www.oft.gov.uk/news-and-updates/press/2005/210-05, accessed 2 August 2005.
146 See for example HM Revenue and Customs. (2009) *Renewal of the 'Tackling Alcohol Fraud' Strategy*. London: HM Revenue and Customs.
147 See HM Customs and Excise. (2002) *Oils Fraud Strategy: Summary of Consultation Responses Regulatory Impact Assessment*. London: HM Customs and Excise.

148 Fisher, J. (2010) *Fighting Fraud and Financial Crime A New Architecture for the Investigation and Prosecution of Serious Fraud, Corruption and Financial Market Crimes*. London: Policy Exchange, p. 3.
149 Timesonline. (2010) Conservatives confirm plans for single Economic Crime Agency, http://timesonline.typepad.com/law/2010/04/conservatives-confirm-plans-for-single-economic-crime-agency.html, accessed 26 April.
150 HM Government. (2010) *The Coalition: Our Programme for Government*. London: HM Government, p. 9.
151 Leigh, D. and Evans, R. (2010) Cost of new economic crime agency could prove prohibitive. *The Guardian*, 2 June, http://www.guardian.co.uk/business/2010/jun/02/economic-crime-agency-scheme-cost, accessed 12 July 2010.
152 See generally Fraud Advisory Panel. (2010) *Roskill Revisited: Is There a Case for a Unified Fraud Prosecution Office?*. London: Fraud.
153 Attorney General's Office[90], at p. 7.
154 Home Office. (n/d) Fraud, http://www.crimereduction.homeoffice.gov.uk/fraud/fraud17.htm, accessed 7 December 2009.
155 It is important to note that the Proceeds of Crime Act 2002 applies to serious crime, which includes fraud.
156 Home Office. (2004) *Home Office Circular 47/2004 Priorities for the Investigation of Fraud Cases*. London: Home Office.
157 Financial Services Authority. (2008) *FSA Handbook – SUP (Supervision)*. London: Financial Services Authority, at SUP 15.3.17R.
158 Financial Services Authority[157], at SUP 15.3.19G.
159 Financial Services Authority[157], at SUP 15.3.20G.
160 HM Treasury. (2002) *Combating the Financing of Terrorism – A Report on UK Action*. London: HM Treasury.
161 Prevention of Terrorism (Temporary Provisions) Act 1989, s. 13. Also see Levi, M. (2010) Combating the financing of terrorism: A history and assessment of the control of threat finance. *British Journal of Criminology* 50(4): 650–669, at 652.
162 For a more detailed discussion of terrorist funding in Northern Ireland see Tupman, W. (1998) Where has all the money gone? The IRA as a profit-making concern. *Journal of Money Laundering Control* 1(4): 303–311.
163 Bell, R. (2003) The confiscation, forfeiture and disruption of terrorist finances. *Journal of Money Laundering Control* 7(2): 105–125, 113.
164 Home Office[50], at paragraph 6.15.
165 Terrorism Act 2000, s. 15(1).
166 Terrorism Act 2000, s. 15(2).
167 Terrorism Act 2000, s. 15(3).
168 Terrorism Act 2000, s. 16(1).
169 Terrorism Act 2000, s. 16(2).
170 Terrorism Act 2000, s. 17(1).
171 Terrorism Act 2000, s. 17(2).
172 Terrorism Act 2000, s. 18(1)(a).
173 Terrorism Act 2000, s. 18(1)(b).
174 Terrorism Act 2000, s. 18(1)(c).
175 Terrorism Act 2000, s. 18(1)(d).
176 Terrorism Act 2000, s. 18(2).
177 Bell above, n 189 at p. 113.
178 Home Office. (2009) *Lord Carlile Report on the Operation in 2008 of the Terrorism Act 2000 and of Part 1 of the Terrorism Act 2006*. London: Home Office, p. 68.
179 Also see Financial Action Task Force. (2007) *Third Mutual Evaluation Report Anti-money Laundering and Combating the Financing of Terrorism – The United Kingdom and Northern Ireland*. Paris: Financial Action Task Force, p. 45.
180 Home Office[178], at p.18.
181 Terrorism Act 2000, schedule 6.
182 Home Office[178], at p. 23.
183 Terrorism Act 2000, schedule 6, paragraph 2(a).
184 Terrorism Act 2000, schedule 6, paragraph 2(b).
185 Terrorism Act 2000, schedule 6, paragraph 3.
186 Peddie, J. (2008) Anti-terrorism legislation and market regulation. In: W. Blair and R. Brent (eds.) *Banks and Financial Crime – The International Law of Tainted Money.* Oxford, UK: Oxford University Press, pp. 437–458, at 440.
187 Terrorism Act 2000, schedule 6, paragraph 7.
188 Peddie above, n 213 at p. 441.
189 Terrorism Act 2000, ss. 15–19.
190 Terrorism Act 2000, s. 23.
191 Terrorism Act 2000, s. 28.
192 Terrorism Act 2000, schedule 4.
193 Peddie[186], at p. 443.
194 Terrorism Act 2000, s. 38A.
195 Binning, P. (2002) In safe hands? Striking the balance between privacy and security – Anti-terrorist finance measures. *European Human Rights Law Review* 6: 737–749, at 747.
196 Counter-Terrorism Act 2008, schedule 7.
197 Counter-Terrorism Act 2008, schedule 7, part 1.
198 Financial Action Task Force. (2009) FATF Statement. 25 February, http://www.fatf-gafi.org/dataoecd/18/28/42242615.pdf, accessed 3 August 2010.
199 HM Treasury. (2009) HM Treasury warns businesses of serious threats posed to the international financial system. 11 March, http://webarchive.nationalarchives.gov.uk/+/http://www.hm-treasury.gov.uk/press_26_09.htm, accessed 3 August 2010.
200 Counter-Terrorism Act 2008, Schedule 7, part 2 paragraph 3.
201 Goldby, M. (2010) The impact of Schedule 7 of the Counter-Terrorism Act 2008 on banks and their customers. *Journal of Money Laundering Control* 13(4): 351–371.
202 For a description of the losses suffered by Bank Mellat see *Bank Mellat* v. *HM Treasury* [2010] EWHC 1332 (QB), para 2 and *Bank Mellat* v. *HM Treasury* [2010] EWCA Civ 483, para 12.
203 See *Bank Mellat* v. *HM Treasury* [2010] EWHC 1332 (QB).
204 Anti-terrorism Crime and Security Act 2001, Schedule 1, Part 2.
205 Anti-terrorism Crime and Security Act 2001, ss. 4–16.
206 Anti-terrorism Crime and Security Act 2001, Schedule 1, Part 1.
207 This provision repealed the Emergency Laws (Re-enactments and Repeals) Act 1964, s. 2.
208 The Act provides that HM Treasury is not required to prove actual detriment to freeze the assets of a suspected terrorist, but that a threat is sufficient.
209 Terrorism Act 2000, s. 4(1)(a) and (b).
210 Terrorism Act 2000, s. 5.
211 Terrorism Act 2000, s. 7 and 9.
212 The freezing of assets is permitted by the Terrorism (United Nations Measures) Order 2006 (SI 2006/2657).

213 Terrorism Act 2000, Part II, Schedule 1.
214 Ryder, N. (2007) A false sense of security? An analysis of the legislative approaches towards the prevention of terrorist finance in the United States of and the United Kingdom. *Journal of Business Law*, September: 821–850, at 843.
215 HM Treasury[13], at p. 27.
216 Ryder[214], at p. 844.
217 15 July 2009: Column WS96.
218 Financial Action Task Force[179], at p. 76.
219 HM Treasury[16], at p. 11.
220 S.I 2006/2657.
221 27 December 2001, on specific restrictive measures directed against certain persons and entities with a view to combating terrorism.
222 HM Treasury[107], at pp. 25–26.
223 [2008] EWHC 869.
224 One of the applicants unsuccessfully argued that an order granted against himself by the Al-Qaeda and Taliban (United Nations Measures) Order 2006, S.I. 2006/2952 should be set aside.
225 For a more detailed discussion of this issue see *M* v. *HM Treasury* [2008] UKHL 26.
226 *A* v. *HM Treasury* [2008] EWCA Civ 1187.
227 The Court of Appeal stated that the method adopted should be comparable with that adopted in *Secretary of State for the Home Department* v. *MB* [2008] A.C. 440.
228 S.I. 2009/1747.
229 S.I. 2009/1747, article 5.
230 Johnston, A. and Nanopoulos, E. (2010) Case comment the new UK Supreme Court, the separation of powers and anti-terrorism measures. *Cambridge Law Journal* 69(2): 217–220, at 220.
231 Terrorism Act 2000, s. 21A(2).
232 Terrorism Act 2000, s. 21A(3).
233 Terrorism Act 2000, s. 21A(4).
234 Anti-terrorism, Crime and Security Act 2001, schedule 2 part 3.
235 Terrorism Act 2000, s. 21A.
236 Home Office[100], at p. 18.
237 Terrorism Act 2000, s. 21B.
238 Terrorism Act 2000, s. 21B(2).
239 Terrorism Act 2000, s. 21B(3).
240 Terrorism Act 2000, s. 21B(4).
241 Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007 SI 2007/3398.
242 Home Office[178], at pp. 19–20.
243 Serious Organised Crime Agency[82], at p. 13.
244 Serious Organised Crime Agency. (2008) *The Suspicious Activity Reports Regime Annual Report 2008*. London: Serious Organised Crime Agency, p. 42.
245 Serious Organised Crime Agency. (2010) *The Suspicious Activity Reports Regime Annual Report 2009*. London: Serious Organised Crime Agency, p. 11.
246 Rhodes, R. and Palastrand, S. (2004) A guide to money laundering legislation. *Journal of Money Laundering Control* 8(1): 9–18, at 17.
247 Maylam, S. (2002) Prosecution for money laundering in the UK. *Journal of Financial Crime* 10(2): 157–158, at 157–158.