THE SOCIETY FOR ADVANCED LEGAL STUDIES

THE FUNDING OF TERROR
THE LEGAL IMPLICATIONS OF THE FINANCIAL WAR ON TERROR

THE INTERDICTION OF TERRORIST PROPERTY WORKING GROUP

JULY 2002

CONTENTS

PREFACE

'Terrorism is about gaining power through violence, and money is a means to that end.' These words of the Northern Ireland Affairs Committee of the House of Commons in their recent report, *The Financing of Terrorism in Northern Ireland*,[1] highlight that terrorism needs money and access to international payment systems. Unless it can acquire finance, and move the money around, a terrorist group cannot buy the weapons, communications systems and training necessary to conduct an effective campaign, especially over a sustained period. Disrupting, and if possible seizing, terrorist moneys are therefore central to any anti-terrorist strategy.

The terrible events of 11 September 2001 have brought these points home even more cogently. The international community has been galvanised into action. Acting under Chapter VII of the UN Charter, the Security Council decided that all states should criminalize the funding of terrorism and should 'freeze without delay funds and other financial assets or economic resources of terrorists, entities owned by terrorists and those acting for them'. (Resolution 1373 of 28 September 2001). National governments have been prompted to further action. For example, the UK government enacted the Anti-Terrorism, Crime and Security Act 2001, which amended in important respects the Terrorism Act 2000. As a result there is now an armoury of legal provisions obliging banks to disclose information to the authorities about suspected terrorists, prohibiting banks from making funds available to terrorists and freezing terrorist funds held by banks. But how effective are such provisions likely to be? One difference from money laundering is that terrorist funding typically involves much smaller sums, so detection problems are compounded. Another difference is that the sources of terrorist funding are often ostensibly legitimate – the al-Qaida network ran a range of businesses and financial support also came from a variety of charities. If the legal controls addressing money laundering have not always been a success, will those directed against terrorist funding be any more effective?

Late last year the Society of Advanced Legal Studies established an expert working group to get a handle on these issues and to come up with practical suggestions. The working group comprised four sub-groups: one to review international developments; the next to examine the impact of initiatives on financial institutions (compliance issues); another to look at the

[1] HC 978, 2002, Vol 1, p 9.

enforcement issues including international cooperation; and the final group to gauge the impact on other areas of the law. Here are their reports.

It may be useful to offer a bird's eye review of the report. Chapter 1, from sub-group 1, helpfully outlines international measures against terrorist financing, notably the UN International Convention for the Suppression of the Financing of Terrorism, now in force, together with the legislative measures taken in the United States. Of particular note is the UN assessment of how states have criminalized the financing of terrorism (para 1.6.7).

Chapter 2, from sub-group 2, offers an overview of the regulatory law. In addition, it summarizes the key rules of the Financial Services Authority and the guidance issued by the Joint Money Laundering Steering Group. The reporters consider whether the JMLSG is the most appropriate body to give detailed guidance to the financial sector on terrorist funding and conclude that it is (para 2.17.10). Also from sub-group 2, Chapter 3 places the law in context. Firstly, it considers the typologies of terrorist funding suggested by the Joint Money Laundering Steering Group and the Financial Action Task Force. The 11 September attack itself illustrated the difficulty in identifying terrorist financing, given the use of legitimate business fronts, charitable bodies and informal payment mechanisms. The indicia suggested by the Financial Crimes Enforcement Network may, however, provide assistance (para.3.3). There then follows an account of the various lists of persons suspected of terrorism or of supporting terrorism, issued by national bodies such as the Bank of England and the United States Office of Foreign Assets Control (OFAC), and the UN. The lists are numerous and not always consistent.

The next three chapters – chapters 4 to 6 – are from sub-group 5. They consider the interplay between provisions of the Terrorism Act 2000 and the Anti-terrorism, Crime and Security Act 2001 on the one hand, and various doctrines of English private law on the other. In Chapter 4 the reporters discuss the statutory disclosure duties by considering the nature and scope of a defendant's potential liability for breach of confidence, in the event that he or she discloses confidential information pursuant to statutory obligations under the Terrorism Act 2000, sections 19 and 20. The tension which exists at a theoretical level is brought out – between complying with the disclosure duties and the consequent exposure to action for breach of confidence. An amendment to existing legislation is proffered (para 4.7.3). Chapter 5 considers the disclosure provisions of the new Terrorism Act 2000, section 21A, and very helpfully discusses what is meant by a defendant's 'knowledge and suspicion' of terrorist activities, a question on which some light is thrown by various recent cases on the law of dishonest assistance in a breach of trust. The practical advice given (para 5.7.2) is for

institutions to implement clear and thorough 'know your customer' and reporting procedures, to follow the guidance issued by the relevant national and international agencies, and to ensure that staff are aware of the 'terrorist typologies' identified by bodies such as the Joint Money Laundering Steering Group and the Financial Action Task Force. Then Chapter 6 examines the private law tracing rules and the ways in which they might come into play when forfeiture orders are sought under the Anti-Terrorism, Crime and Security Act 2001, section 1. In particular, the reporters consider the position of third-party recipients of terrorist property caught by this section. While *bona fide* third party purchasers are protected, the legislation is not clear on what it intends with other innocent third parties who have earmarked property.

Finally, chapter 7 is from sub-group 4. It is a vitally important chapter, since however perfect the law in the books, without effective application it will be like something written in sand. The chapter first analyses the investigative and enforcement powers in UK legislation and gives it a clean bill of health. It then turns to implementation. The seizure of funds since 11 September is noted, but the caveat is entered that its impact is little understood, since we have no detailed knowledge of how these sums relate to actual and replenishable stock of funds available to terrorist groups. Of particular importance is the group's argument that it is not simply a matter of the human and other resources available for intelligence and enforcement, but the culture of the organization entrusted with the task. There are some pertinent comments about organisational change and also the need for states to encourage other jurisdictions to take action which they may find problematic at home (para 7.20.9).

I am immensely grateful to all who participated in the writing of this report. Those who had the burden of the actual preparation are named on the following page, but I know many others contributed to the final product, in discussions or by way of information and comment provided. Members of one sub-group will not always agree with what other sub-groups have said. Indeed, members of each sub-group will not necessarily endorse the final submission of their own sub-group. But overall, there is a great deal of meat in this report, and it is an immensely helpful contribution to the public debate.

Ross Cranston QC, MP

CHAPTER 1

International Legal Developments

1.1 Introduction

1.1.1 A new international regime for regulating terrorist financing has emerged for commercial and financial enterprises that operate in a transnational context, or conduct transactions involving foreign enterprises or individuals suspected of terrorist activity. Indeed, terrorist financing has become a major development in international financial regulation and poses an issue of regulatory concern for banks and financial institutions that operate on a transnational basis.

THE UNITED STATES RESPONSE

1.2 The aftermath of 11 September 2001 – Executive Order 13224

1.2.1 President Bush issued Executive Order 13224 entitled 'Blocking Property and Prohibiting Transactions with Persons who Commit, Threaten To Commit, Or Support Terrorism.' This Executive Order expanded the list of designated terrorist organisations to include over 30 individuals and organisations that have allegedly committed, or been involved in, acts of terrorism[2] All persons subject to US jurisdiction are required to block or freeze any assets being held on behalf of such persons and to notify OFAC accordingly. The Order also prohibits all foreign third parties from assisting or providing material support for, or associating with, designated terrorists. The Order observes that the global reach of terrorist financing made it necessary to impose extraterritorial financial sanctions against all 'foreign persons that support or otherwise associate with these foreign terrorists'.[3]

1.2.2 The Order provides a broad definition of terrorism that provides:

an activity that –

(i) involves a violent act or an act dangerous to human life, property, or infrastructure; and

---

[2] Some of the groups and individuals designated include the Al Qaida/Islamic Army organisation and Usama bin Laden: see Exec Order 13224 (24 Sept 2001), Annex.

[3] Exec. Order 13224, preamble (24 Sept 2001).

(ii) appears to be intended –

(A) to intimidate or coerce a civilian population ; or

(B) to influence the policy of a government by intimidation or coercion; or

(C) to affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking.

1.2.3 Such a broad definition of terrorism could reasonably be interpreted to apply to the activities of some states in recent years which have relied on 'violent acts' or 'acts dangerous to human life, property or infrastructure' to accomplish state objectives that necessarily involved the coercion of a civilian population or sought 'to influence the policy of a government by intimidation or coercion'.[4]

1.2.4 Section 1 of the Order blocks indefinitely any obligation to perform a contract entered into before the effective date of the Order with a designated terrorist entity or person listed in the Order, and requires all property or interests in property to be blocked of such designated persons that are located in the United States or that hereafter come within the US, or that come within the possession or control of a US person. The Secretary of the Treasury, in consultation with the Secretary of State and the Attorney General, has authority to determine which 'foreign persons' have committed or pose a significant threat of committing 'acts of terrorism that threaten the security of US nationals or the national security, foreign policy, or economy of the United States'.[5] Moreover, the Secretary of the Treasury may make determinations that certain foreign persons in third countries are 'owned or controlled by', or 'act for or on behalf of' foreign persons designated by the US to be terrorists.[6] Moreover, section 1 (d) of the Order expressly creates extraterritorial third party liability by authorising the Secretary of the Treasury, after consulting with other US government officials and with 'foreign authorities, if any,' to designate foreign persons who 'assist in, sponsor, or provide financial, material, or technological support for, or financial or other services to or in support of, such acts

[4] In the 1980s, the Nicaraguan government accused the United States of conduct that might reasonably fall within this definition of terrorism (*Nicaragua* v *United States*, I.C.J. Reports 1986, p 14). The ICJ decided, *inter alia*, 'that, by laying mines in the internal or territorial waters of the Republic of Nicaragua during the first months of 1984, the United States of America has acted, against the Republic of Nicaragua, in breach of its obligations under customary international law not to use force against another State, not to intervene in its affairs, not to violate its sovereignty and not to interrupt peaceful maritime commerce.' Ibid, para. 292 (6).

[5] s. 1 (b).

[6] s. 1 (c)

of terrorism or those persons listed' to be terrorists. All US trade, commerce or transactions with such third party persons would be prohibited unless a licence is obtained from OFAC, and they would be subject to civil and criminal sanctions under US law if they have a constitutional presence in the US.

1.2.5 The Order also prohibits any transaction or dealing by US persons, or by foreign persons within the US, in property or interests in property blocked pursuant to this Order, including but not limited to 'the making or receiving of any contribution of funds, goods, or services to or for the benefit of those persons listed' as terrorists in the Order.[7] This provision prohibits the right of US persons to make contributions of any type or to perform any type of service on behalf of a listed terrorist or a person or entity operating in a foreign country which the US has decreed to be owned or controlled by a listed terrorist. Moreover, any effort by a US person (or by a non-US person within the US) to undertake a transaction to restructure the ownership or control of property or a business entity in order to evade or avoid restrictions under the Order is prohibited and may attract both civil and criminal liability not only for financial institutions or companies holding property on behalf of listed terrorists but also for the professionals advising such transactions.[8] Moreover, any conspiracy formed to violate the Order is prohibited and has extraterritorial effect through the Federal Conspiracy statute.[9]

1.2.6 Section 6 states the importance of US cooperation with foreign governments in implementing the Order by providing that the Secretary of State and the Secretary of the Treasury and other government agencies 'shall make all relevant efforts to cooperate and coordinate with other countries' and may invoke existing bilateral and multilateral agreements and arrangements to achieve the objectives of the Order. This would include the prevention or suppression of acts of terrorism, and the denial of financing and financial services to terrorists and terrorist organizations, and the sharing of intelligence regarding funding activities in support of terrorist groups. It should be noted that the principle of 'cooperation and coordination' in section 6 appears to be mandatory only to the extent that US government officials may determine what efforts at cooperation and coordination are 'relevant efforts' to

---

[7] s. 2 (a).
[8] s. 2 (b).
[9] s. 1 (c). See *as amended* 18 USC § 371 (2000); see also *United States* v *Inco Bank & Trust Corpn.*, 845 F. 2d 919, 923-24 (11th Cir. 1988).

achieve the objectives of the Order. Essentially, the US government will not be precluded from acting unilaterally whenever it perceives that it is necessary to do so.

1.2.7 The Order departs slightly from other US sanctions programmes by defining the term 'United States person' to mean any US citizen, permanent resident alien, entity organised under the laws of the United States (including foreign branches), or any person in the United States. In an extraterritorial sense, this is a less sweeping definition than those adopted under the Cuban and North Korean Sanctions Programmes that define US person more broadly to include any foreign person deemed by the US government to be controlled by a US citizen, resident or US business entity. Under these programmes, a US person could be defined as a company incorporated under the laws of a foreign state whose shares are subject to significant US ownership or control.[10]

1.2.8 The Executive Order is a significant extension of extraterritorial third party liability for foreign banks, companies and individuals who conduct, facilitate or assist transactions involving US-designated terrorist organisations. OFAC is expected in the near future to issue regulations that describe in more detail how the Order will be applied and enforced.

1.3 The Patriot Act – International Money Laundering Abatement and Anti-terrorist Financing Act of 2001

1.3.1 Title III of the Patriot Act is entitled the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001. Title III contains the key provisions that apply to US and foreign banks and financial institutions. It amends, *inter alia*, certain provisions of the Bank Secrecy Act of 1970 and the Money Laundering Control Act of 1986. The Bank Secrecy Act has enhanced transparency for US financial institutions by preventing them from keeping opaque records and requiring them to maintain standardised transaction records and to report large currency transactions and suspicious transactions. Some of its provisions apply not only to financial institutions but also require any individual to report the movement of more than $10,000 in currency into and out of country. The Money Laundering Control Act creates the criminal offence of laundering the proceeds of crime and allows the criminal and civil forfeiture of the proceeds or property derived from crime.

[10] 31 CFR §515. 329 (a)-(d)(Cuban Asset Controls)(2000); 31 CFR §500.329(a)-(d) (2000).

Moreover, Title III contains, among other provisions, authority to take targeted action against countries, institutions, transactions, or types of accounts that the Secretary of the Treasury finds to be of prime money laundering concern. It also contains high standards of due diligence for correspondent accounts and inter-bank payable through accounts opened at US financial institutions by foreign offshore banks and banks in jurisdictions that have failed to comply with international anti-money laundering standards.

Statutory provisions

1.3.2 Section 311 adds a new section 5318A to the Bank Secrecy Act to give the Treasury Secretary discretionary authority to impose one or more of five new 'special measures against foreign jurisdictions', foreign financial institutions, transactions involving such jurisdictions or institutions, or one or more types of accounts (including foreign accounts), that the Secretary determines to pose a 'primary money laundering concern' to the United States. The special measures include: (1) requiring additional record-keeping or reporting for particular transactions; (2) requiring identification of the foreign beneficial owners of accounts at US financial institutions; (3) requiring foreign banks to identify any of its customers who use (ie transfer of funds) an inter-bank payable through account opened by that foreign bank at a US bank; (4) requiring foreign banks to identify any of its customers who use an interbank correspondent account opened by that foreign bank at a US bank; and (5) after consultation with the Federal Reserve Board, the Secretary of State and Attorney General, to restrict or prohibit the opening or maintaining of certain interbank correspondent or payable-through accounts. The Treasury Department has already issued some regulations regarding recordkeeping and the level of disclosure, and will issue further regulations in the coming months.

1.3.3 Although foreign banks will not have to disclose such information directly to US authorities, US financial institutions will be required to collect this information from foreign banks and if necessary to report this information to US regulatory authorities. The objective of these measures is to establish enhanced due diligence and record-keeping requirements for foreign banks that hold private banking accounts with US financial institutions. The effect of the legislation will be to require foreign persons (business entities and individuals) who are the owners or beneficial owners of private banking accounts with a foreign bank that also maintains certain accounts with a US

bank to disclose the nature of its wealth or commercial affairs with its foreign banker. The US bank will then collect this material and make it available for inspection by US authorities. These requirements will apply only to foreign banks operating under a licence from either an offshore jurisdiction that has not complied with recognised international standards or any other jurisdiction designated by the Financial Action Task Force as having failed to comply with its minimum international standards.

1.3.4 If a foreign bank decides that it wants to opt out of these US regulatory controls, it must terminate all its correspondent, interbank and other accounts with US financial institutions. However, this will be a difficult option for many foreign banks that derive a significant amount of their business from transfers and transactions involving the US interbank payment system. Indeed, the international reach of the US banking system is demonstrated in part by the need of most non-US financial institutions to have access to US currency via a US bank in order to participate in the foreign exchange market. This type of link to the US euro-dollar market will attract extraterritorial jurisdiction for a foreign bank under the Patriot Act. It remains to be seen whether the benefits for a foreign bank of maintaining interbank payment links with US financial institutions exceeds the costs (including lost business) of complying with the new legislation.

Interbank correspondent accounts

1.3.5 The legislation recognises that transactions involving offshore jurisdictions make it difficult for US authorities to follow the money earned by organised crime groups and global terrorists organisations. One way in which money is laundered is through correspondent banking and payment facilities, which are often manipulated by foreign banks to permit the laundering of funds by hiding the true identities of the parties involved in the transactions. To this end, section 312 creates special disclosure requirements for foreign banks that maintain correspondent accounts[11] and other private banking accounts at US financial institutions by adding a new subsection (i) to the Bank Secrecy Act[12] which requires US financial institutions to establish 'appropriate', and, if necessary, enhanced due diligence procedures to

[11] Section 311 defines 'correspondent account' with respect to banking institutions as an account 'established to receive deposits from, make payments on behalf of a foreign financial institution, or handle other financial transactions related to such institution. This amends 31 U.S.C. §5318A (e)(1)(B).
[12] See 31 U.S.C. §5318 (i)(as amended).

detect and report instances of money laundering. New and enhanced due diligence standards are required for US financial institutions that enter into correspondent banking relationships with foreign banks that operate under *either* an offshore banking licence,[13] or a banking licence issued by states that have been (1) designated as non-cooperative with international anti-money laundering standards issued by an international body (ie. FATF) with the concurrence of the US representative to that body, or (2) subject to special measures set forth under section 311 (see above). Moreover, section 312 creates new minimum due diligence standards for maintenance of private banking accounts by US financial institutions. These new standards will become effective 270 days after the date of enactment (around 1 August 2002), and the Treasury Secretary is required to issue regulations, in consultation with the relevant federal functional regulators, within 180 days of enactment (around 1 May 2001) that further specify the requirements of this subsection. The statute, however, shall take effect regardless of whether or not such regulations have been issued, and will be enforceable by the relevant officials.[14]

1.3.6 Foreign banks that maintain correspondent accounts with US banks are required to appoint agents within the United States territory for service of process. The Attorney General and the Secretary of the Treasury can issue summons or subpoena records or documents, wherever located, relating to such correspondent accounts.

1.3.7 Section 313(a) prohibits certain covered financial institutions[15] from establishing, maintaining, administering or managing correspondent accounts with 'shell banks', which are defined as a foreign bank that has no physical presence in any jurisdiction.[16] This provision also requires covered financial institutions to take 'reasonable steps' to ensure that correspondent accounts provided to foreign banks are not being used indirectly to provide financial services to foreign shell banks. In addition, section 319 (b) requires that covered financial institutions which provide

---

[13] An offshore banking licence is defined as a licence to conduct banking business, where a condition of the licence is that the bank may not offer banking services to citizens of, or in the local currency of, the jurisdiction issuing the licence. See Supervisory Letter SR 01-29, Board of Governors of the Federal Reserve System. (26 Nov 2001).

[14] The provision of the subsection goes on to state that the 'failure to issue final regulations shall in no way affect the enforceability of s 5318 (i).

[15] 31 U.S.C. §5318(j) defines 'covered financial institution' as (1) any insured bank (as defined in s. 3(h) of the Federal Deposit Insurance Act (12 U.S.C. §1813(h)); (2) a commercial bank or trust company; (3) private banker; (4) an agency or branch of a foreign bank; (5) a credit union: (6) a broker or dealer registerd with the Securities and Exchange Commission under the Securities and Exchange Act of 1934 (15 U.S.C. §78a *et seq*).

[16] Section 313(a) *codified at* 31 U.S.C. §5318(j)(effective date 25 Dec. 2001). A physical presence is a place of business that is maintained by a foreign bank and is located at a fixed address, other than solely an electronic address, in a country in which the foreign bank is authorised to conduct banking activities. Ibid.

correspondent accounts to a foreign bank to maintain records of the owners of the foreign bank and the designated agent in the United States to accept service of legal process.

1.3.8 An exception exists, however, to permit a covered financial institution to maintain correspondent accounts with foreign shell banks that are affiliated with a depository institution, credit union, or foreign bank that maintains a physical presence in the US or in another jurisdiction, and the shell bank must be subject to supervision by the banking authority that regulates the affiliated entity.[17] The broad definition of 'covered financial institution' means that non-bank institutions, such as brokers and dealers in securities that operate in the United States, will be prohibited from establishing, maintaining, administering or managing an account for a foreign shell bank that is not a regulated affiliated.[18] To qualify as a regulated affiliate, the affiliated depository institution must demonstrate that it is regulated by a financial authority whose standards comply with generally accepted international norms as set forth by international bodies (ie, the Financial Action Task Force).[19]

Interbank payable-through accounts

1.3.9 Section 311 (e) defines a 'payable-through account' as 'an account, including a transaction account, . . . opened at a depository institution by a foreign financial institution by means of which the foreign financial institution permits its customers to engage, either directly or through a subaccount, in banking activities usual in connection with the business of banking in the United States. Section 319 of the Act amends the US Asset Confiscation and Forfeiture statute[20] to treat money deposited into an account of a foreign bank which has an interbank payable-through account with a US bank as having been deposited in the United States for purposes of the forfeiture rules. Enforcement of this provision would work by allowing any restraining order, seizure warrant, or arrest warrant *in rem* regarding the funds to be served on the US bank, and the amount of the funds restrained or seized at the US bank can cover a value up to the value of the funds deposited into the account at the

[17] The Act defines 'affiliate' as a foreign bank that is controlled by or under common control with another institution.
[18] Section 313(a) *codified and amended* at 31 U.S.C. §5318 (j).
[19] This section took effect 60 days from the date of enactment (around 1 Jan 2002).
[20] 18 U.S.C. § 981 (2000).

foreign bank.[21] The US government is not required to establish a direct link, or that the funds are directly traceable, to the funds that were deposited by the foreign defendant into the foreign bank.[22]

1.3.10 The Act also imposes a new reporting duty on securities brokers and dealers for which the regime is similar to the one in place for banks and on 'underground banking systems' and licensed senders of money by requiring them to file suspicious activity reports (SARs).[23] A safe harbour is created for any financial institution that discloses a possible violation of law through a SAR.[24] The Act also requires federal regulators to propose enhanced disclosure regulations and reporting and record-keeping requirements for investment companies (eg. pension fund and portfolio management firms). Civil and criminal liability may be imposed for trustees and investment managers in this regard.

1.3.11 The Secretary of Treasury is required to issue regulations[25] to foster cooperation amongst financial institutions, regulators and law enforcement agencies by permitting the sharing of information between regulators and law enforcement authorities regarding the activities of persons suspected, based on credible evidence, of engaging in money laundering activity or terrorist acts.[26] This section also allows banks to share information with other banks, without violating confidentiality laws, regarding suspicious accounts or transactions involving possible terrorist or money laundering activity. It also requires the Treasury Secretary to publish a semi-annual report with a detailed analysis of patterns of suspicious activity and other investigative insights gathered from investigations and bank reporting.

1.3.12 Under section 315, bribery and other foreign corruption offences become 'specified unlawful activities' for purposes of the crime of money laundering. The section also makes several other existing federal crimes serve as predicate offences for the crime of money laundering, including certain export control violations,[27] firearms violations, and certain computer fraud offences, and felony offences under the

---

[21] Section 319 (a) (1) (A).
[22] Section 319 (a) (2).
[23] Section 359.
[24] Section 351.
[25] Section 314 requires to be issued within 120 days of enactment.
[26] Ibid.
[27] These violations fall under both Arms Export Control Act's Munitions List (22 U.S.C. §2778), and the Export Administration Act's Regulations (15 CFR parts 730-744) regarding export controls of goods and services that may be re-exported or re-sold from a third country to a targeted country or terrorist group or criminal organisation.

Foreign Agents Registration Act of 1938. US courts are granted 'long-arm jurisdiction' over foreign persons who commit money laundering offences under US law.[28] This extraterritorial jurisdiction also applies to foreign banks opening US bank accounts, and to foreign persons who convert assets ordered confiscated by a US court. A federal court will have the authority to issue *ex parte* pre-trial restraining orders or to take other necessary action to preserve property in the United States to satisfy a possible future judgment. A federal court may appoint a receiver to collect and take custody of a defendant's assets to satisfy a criminal or civil money laundering or forfeiture judgment.[29] Also, the maximum civil and criminal penalties for violating US international counter-money laundering laws have been increased from $100,000 to $1 million per violation.[30]

1.3.13 The definition of 'financial institution' for purposes of sections 1956 and 1957 of the 1986 Money Laundering Control Act is expanded to include foreign banks or other financial institutions operating outside the United States. Financial institutions subject to anti-money laundering laws will be determined according to regulations issued by the Department of Treasury and will apply to foreign banks as defined under US law.[31] Moreover, concentration accounts at financial institutions will be more heavily regulated, as the Secretary of Treasury will be authorised to issue regulations concerning the maintenance of concentration accounts by US depository institutions in order to prevent an institution's customers from anonymously directing funds into or through such accounts.[32] This is designed to prevent the blocking of the identification of a customer with the movement of funds of which the customer is the direct or beneficial owner. The provision also prohibits financial institutions and their employees from informing customers of the existence of, or the means of identifying, concentration accounts at the institution. Regarding identity verification, section 326 requires the Treasury Secretary to issue regulations (jointly with each US functional regulator) that prescribe minimum standards for financial institutions and their customers regarding the identity of the customers that shall apply as part of the application to open a bank account. These minimum standards shall require financial institutions to implement, and customers who have received

[28] Section. 317.
[29] Ibid.
[30] Section 363.
[31] Section 1 of the International Banking Act of 1978 (12 USC 3101(7)).
[32] Section 326 (amending 31 U.S.C. § 5318(h).

adequate notice to comply with procedures concerning verification of customer identity, maintenance of records of identity verification, and consultation at account opening of lists of known or suspected terrorists provided to the financial institution by the US government.

1.3.14 Section 316 sets forth the procedural defences that a financial institution may take to defend against an government action to confiscate or forfeit property allegedly derived from terrorist activity or money laundering. Any owner of property that is confiscated under any provision of law relating to the confiscation of assets belonging to suspected international terrorists may contest that confiscation by following the established procedures set forth in the Federal Rules of Civil Procedure[33] and by asserting an affirmative defence based on one of the following: (a) that the property is not subject to confiscation under such provision of law; or (b) that the owner complies with the 'innocent owners defense' under federal law.[34] A owner of property will also have the right to contest the confiscation of assets of suspected international terrorists under the US Constitution and relevant provisions of the Administrative Procedure Act. Moreover, a US federal court may suspend the federal rules of evidence in certain circumstances where a party to the proceedings seeks to admit evidence that would otherwise be inadmissible under the federal rules, but the court must make a finding that the evidence is reliable and that complying with the federal rules of evidence will jeopardise the national security interests of the United States.[35] Many US judges are often reluctant to deny a US government motion to suspend the federal rules of evidence on the grounds of national security if the government can provide a reasonable explanation for why disclosure of an evidentiary source might jeopardise national security.

1.3.15 US regulators are now given broader powers to collect information from US financial institutions regarding interbank accounts (correspondent and payable-through) by requiring them to produce requested information within 120 hours within receipt of a request.[36] US financial institutions will be required to sever their relationships with the foreign bank if it *either* fails to comply with the summons or

---

[33] In circumstances where the confiscated property is on board a maritime vessel or in customs house, the Supplemental Rules for Certain Admiralty and Maritime Claims must be followed.
[34] Section 316 (a) (1) & (2).
[35] Section 316 (b).
[36] Section 319 (b)(1)(B)(2).

subpoena *or* fails to contest the action in the relevant US court within 120 hours of it being served.[37]

1.3.16 Requiring the identification of the 'foreign beneficial owners' of interbank accounts with US financial institutions may create a disclosure obligation for many companies and trusts who are organised in foreign jurisdictions that might conflict with secrecy requirements under local law. Moreover, some jurisdictions make it a criminal offence to disclose information that identifies beneficial owners of shares in certain companies or the beneficiaries under certain trust arrangements. Section 319 takes account of this by vesting authority in the Attorney General to suspend or terminate a forfeiture under this section if the Attorney General determines that a direct conflict of laws exists between the laws of the jurisdiction in which the foreign bank is located and the laws of the United States with respect to liabilities arising from the restraint, seizure, or arrest of such funds, and that such suspension or termination 'would be in the interest of justice and would not harm the national interests of the United States.'[38]

1.3.17 The sweeping extraterritorial provisions discussed above may also work in favour of foreign regulators if they are seeking to obtain property located in the United States but which is derived from crimes committed in their countries. Section 320 permits the US government to institute forfeiture proceedings against the real or personal property found in the US that constitutes, or is derived from, an offence against a foreign nation, if (a) the offence involves the manufacture, distribution or sale of a controlled substance[39], or (b) would be punishable within the jurisdiction of the foreign nation by death or imprisonment for a term exceeding one year, *and* would be punishable under US law by imprisonment for a term exceeding one year, if the act or activity constituting the offence had occurred within the United States. Moreover, section 323 allows the US government to seek a restraining order to preserve the availability of property subject to a foreign forfeiture order or confiscation judgment.

1.3.18 Prior to the Patriot Act, US banking law provided a narrow definition for the term 'financial institution' for purposes of the Bank Secrecy Act that excluded many financial firms from the requirements of reporting suspicious transactions. Section

[37] Section 319 (b)(3)(A).
[38] Section 319 (a)(1)(B).
[39] See definition of controlled substance under section 413 of the Controlled Substances Act and any other conduct described in section 18 USC §1956 (c)(7)(B).

321 amends this omission by defining the term 'financial institution' broadly to include credit unions, futures commission merchants, commodity trading advisers, securities brokers/dealers and commodity pool operators, who are now obligated to comply with the reporting requirements of the Bank Secrecy Act.[40] Moreover, the Act pierces the veil of corporate personality by prohibiting any corporation (US or foreign) that seeks to maintain a forfeiture action in a US court from doing so if a controlling shareholder, or any person bringing the claim on behalf of the corporation, is a fugitive under US law.[41] This provision would also apply to restrict – and in some cases prohibit – a claim instituted by such a corporation to challenge a civil forfeiture action taken by the US government.

Applications for bank mergers and acquisitions

1.3.19 Under the Act, the Federal Reserve Board and the Federal Deposit Insurance Corporation are required to take account of the anti-money laundering records of any US or foreign bank or bank holding company that seeks to merge with, or acquire, a banking institution or bank holding company within the jurisdiction of these respective agencies. As part of such a review, the US regulators may request the records of all foreign branches or agencies of an applicant bank, or, in the case of a bank holding company, the records of its foreign subsidiaries.[42]

Efforts at cooperation and coordination with foreign regulators

1.3.20 The Act requires the Treasury Secretary, the Secretary of State, and the Attorney General to undertake 'reasonable steps' to encourage foreign governments to require the disclosure to US authorities of the names of a party who is the originator of wire transfer instructions sent to the United States, and to report annually to the relevant US congressional committees regarding any progress made with foreign regulators to accomplish this objective.[43] Moreover, Title III requires the President to direct these executive officials to coordinate their efforts with the Federal Reserve Board in negotiating with foreign supervisory authorities or foreign officials to ensure that non-US financial institutions maintain adequate records that relate to the accounts or

[40] Section 321 (a)-(c).
[41] Section 322.
[42] Section 327 (amends s 3 (c) of the Bank Holding Company Act of 1956, and s 18 (c) of the Federal Deposit Insurance Corporation Act of 1991). The regulators subject to this would be the Federal Reserve Board and the Federal Deposit Insurance Corporation.
[43] Section 328.

transactions involving alleged terrorist organisations, or any person engaged in money laundering or other financial crimes.[44] US authorities should seek to obtain such records from foreign financial supervisors, and to make the records available to US law enforcement authorities and financial regulators where appropriate. [45] Congress has also stated an overall policy objective of encouraging US banking and securities regulators to institute negotiations with foreign supervisory authorities for the purpose of developing international norms and rules that would require national authorities to enhance regulatory disclosure standards and to coordinate with foreign authorities in the investigation of terrorist financing and money laundering.[46] The regulations that implement these statutory provisions are likely to grant authority to US financial regulators to negotiate bilateral agreements and other understandings with foreign regulators in order to facilitate the enforcement of financial sanctions on a transnational basis.

1.3.21 The mandatory language of the USA Patriot Act indicates that US regulators will take a more assertive negotiating posture with other members of international bodies in order to achieve more precise and effective international standards and rules for the supervision and regulation of financial institutions with respect to financial crime and terrorist financing. Since the attacks of September 11, the US Congress and the relevant US financial regulators have expanded the extraterritorial scope of US economic sanctions policy and have engaged foreign regulators to adopt more effective measures to identify the sources of suspicious financial transactions and to interdict terrorists financing.

Compliance implications for banks

1.3.22 Title III of the Patriot Act and the OFAC terrorist sanctions regulations together are a comprehensive anti-terrorist programme to attack the financing of international terrorism and to enhance existing anti-money laundering and bank secrecy laws so that foreign banks that do business with the United States, and in particular utilise the US banking system and US currency, will be subject to high standards of due diligence and transparency. In particular, foreign banks must now identify the foreign beneficial owners of certain accounts at US financial institutions. The US

[44] Section 330.
[45] Ibid.
[46] Ibid.

Treasury Secretary will issue further regulations in the coming months to clarify these tough new restrictions on US and foreign banks. These extraterritorial provisions are likely to impose heavy compliance costs on foreign banks that have private banking relationships with US banks. Although this may lead some foreign banks to terminate their relationships with US financial institutions, most sophisticated banking companies need to maintain account relationships with US banks so that they may use the US inter-bank payment system, and therefore will have to comply with these stricter regulatory requirements. The congressional intent behind Title III is to prevent economic criminals and terrorists from using the US financial system to support their illicit activities.

1.3.23 The US Treasury Department's office of Foreign Assets Control (OFAC) blocked on 7 November 2001 the assets of the Al-Barakaat corporate group, a global network of money remitting companies, that were held by US-persons or US-controlled persons throughout the world. The grounds for the US freeze order was that Al-Barakaat was controlled by Usama bin Laden to support terrorist activities. Although the operations of Al-Barakaat in the US relied on traditional banking systems, it operated at the international level as a *hawala* network that allowed funds to be channelled into Somalia through Dubai. According to OFAC, this *hawala* network was used not only to fund al-Qaida and other bin Laden organizations, but also provided logistical support for his network.[47] The OFAC claims that its freeze and blocking orders have put Al-Barakaat out of business, and therefore it can no longer serve as a global money transmission network for terrorist groups. Other experts assert however that money transmission by al-Qaida and other terrorist groups takes place through other alternative remittance systems, and these systems (including *hawala*) completely circumvent existing strategies used by financial regulators at present to curtail terrorist financing.

1.3.24 Despite success in some areas, US and other regulatory authorities have not been able to penetrate and monitor many non-traditional remittance systems, such as *hawala.* In an effort to broaden its understanding of alternative remittance systems, the US Treasury's FinCen has formed an Alternative Remittance Branch that is responsible for the analysis of bank data and other information to identify mechanisms and systems used by criminal organizations to transfer funds in support

[47] It should be noted that Al-Barakaat denies any involvement with bin Laden or with any other terrorist groups. See E. Alden & M. Turner, 'Assets Frozen as US Targets al-Qaida Financing', *Financial. Times*, 7 Nov 2001.

of domestic and international terrorism. This regulatory approach intends to focus on *Informal Value Transfer Systems* (IVTS), such as *hawala, hundi*, and other Asian and South American systems as an important but inadequately understood methodology for fund movement. Regulators should also direct attention to developing key indicators of IVTS use by criminal and terrorist enterprises that would support law enforcement initiatives to combat terrorist activities. This would also involve identifying the policy implications for law enforcement and regulators should they acquire the knowledge and capability to monitor and interdict terrorist financing in informal value transfer systems. The development of an effective international regulatory regime to restrict terrorist financing will fail if its primary focus remains on the formal financial sector. Successful interdiction requires a comprehensive approach that operates on the assumption that most terrorist financing is facilitated through *hawala*-type networks and other informal value transfer systems. To date, international organisations and leading states (ie US) have not succeeded in developing adequate regulatory approaches in this area. Success in the war against international terrorism requires it.

INTERNATIONAL AND MULTILATERAL EFFORTS

1.4 Introduction

1.4.1 The efforts of international organizations, multilateral bodies, and the European Union to regulate and interdict the financing of terrorist activity have had an important impact in developing public international law in this area. Indeed, the United Nations and the Financial Action Task Force have taken the lead at the international level in setting international standards that require states to enhance their supervision and regulatory controls over banking and financial institutions in order to interdict the financing of terrorist activities. In addition, the European Union adopted a Regulation on 27 December 2001 that expands the list of designated terrorist groups and requires EU member states to prohibit commercial or financial transactions with persons or entities that provide support for, or are involved with, designated terrorist groups. These international and regional efforts have facilitated a great deal of bilateral and multilateral cooperation amongst countries that has resulted in a more effective global approach for the freezing of terrorist assets that are located in the formal banking and financial sectors of multiple jurisdictions.

Although international standard setting in this area is an essential component in devising an effective international regime to interdict terrorist financing, this paper suggests that a more comprehensive regulatory approach is needed to address the problem of terrorist financing in the underground financial sector.[48]

1.5 The United Nations

1.5.1 The lack of an international consensus concerning the definition of terrorism has served to hinder international organizations and multilateral bodies from actually defining what terrorism is, as opposed to criminalizing the acts that often constitute terrorism. The United Nations General Assembly has played an important role in addressing some of the more specific manifestations of international terrorism, such as airline hijackings, unlawful seizure of aircraft or hostage taking, by adopting resolutions and conventions that require states to criminalise these acts. It was not until the 1990s, however, that the General Assembly began to address the ancillary activities that support international terrorism. In 1994, the General Assembly passed Resolution 49/60, which reaffirmed existing UN 'condemnation of all acts, methods, practices of terrorism as criminal and unjustifiable'[49] The resolution also encourages states to undertake urgent review of the scope of existing international legal provisions on the prevention and repression of terrorism in all its forms to ensure that all aspects of terrorism are prohibited. To this end, General Assembly Resolution 51/210 recognises the threat posed by so-called charitable and cultural organisations serving as fronts for terrorist fundraising and training, and calls upon all states to take domestic measures to prevent and counteract the financing of terrorists and terrorists organisations.[50] Although these General Assembly resolutions were not legally binding on UN member states as a matter of international law, they recognised the global dimension of terrorist networks and the necessity for state legal and regulatory measures to restrict and terminate the direct and indirect sources of terrorist financing.

1.5.2 The first major multilateral convention adopted with the express objective of requiring states to suppress the financing of terrorism was the International

---

[48] This paper contains excerpts that appeared in the May 2002 issue of the Butterworths *Journal of International Banking and Financial Law*. Other portions of this paper will appear in K Alexander, *American Unilateralism and Extraterritorial Economic Sanctions* (Butterworths, 2002).

[49] See GA Res. 49/60 (9 Dec 1994) and Annex on the Declaration on Measures to Eliminate Terrorism.

[50] GA Res. 51/210 (17 Dec 1996), paras. 3(a)-(f).

Convention for the Suppression of the Financing of Terrorism. The Convention, opened for signature on 9 December 1999,[51] covers the offence of direct involvement or complicity in the financing or collection of funds for terrorist activity. The Convention recognises that the financing of terrorism is a matter of grave concern to the international community and requires states to adopt regulatory measures to prevent the flow of funds intended for terrorist purposes. Specifically, Article 2(1) requires states to create an offence when a 'person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they should be used' to commit an act that constitutes a terrorist offence. Article 2 also defines an act as constituting a specific terrorist offence if it either (1) constitutes a specific offence within the scope of one of the nine UN Conventions listed in the Treaty Annex that address various types of terrorism, or (2) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not actively taking part in hostilities involving armed conflict, when the purpose of such act was to intimidate a population, or to compel a government or international organisation to do or abstain from doing an act. It should be emphasized that the definition of terrorist offence in Article 2 is narrower than the definition adopted by President Bush in Executive Order 12344 issued on 24 September 2001 in the immediate aftermath of the 11 September attacks. The broader definition of the term terrorist offence adopted by the US government will likely create conflicts with US allies and other countries in prosecuting the war against international terrorism.

1.5.3 In addition, Article 8 requires each signatory state to take appropriate measures, according to local law, for the detection and freezing, seizure or forfeiture of any funds used or allocated for the purposes of the offences prescribed in section 2. Article 11 requires signatories to make offences prescribed in the Convention extraditable and to take jurisdiction over such offences by making them punishable with appropriate penalties. Under Article 18(1) national regulators of signatories are required to subject financial institutions and other professionals to 'know thy customer' requirements that involve the identification and filing of suspicious transaction reports. Article 18(2) requires signatories to cooperate in preventing the financing of terrorism in the areas of licensing money servicing businesses, and

[51] GA Res. 54/109, 4th Sess. (9 Dec 1999).

measures to detect or monitor cross-border transactions. Article 18(3) requires signatories to cooperate through exchanging information with respect to terrorist financing.

1.5.4 The Convention entered into force on 10 April 2002 after the required 21 states of the 129 signatories had deposited their instruments of ratification with the United Nations. The UK adopted secondary legislation (SI No. 3365) to implement the Convention that prohibits any person from making 'any funds or financial (or related) services available directly or indirectly to or for the benefit of' a listed terrorist or organisation or company owned or controlled by a terrorist.[52] Similarly, the United States Congress, as part of the Patriot legislation, ratified the Convention, which has now been implemented into US law.[53]

1.6 Security Council Resolution to Combat Terrorist Financing

1.6.1 Before the events of 11 September, the Security Council had adopted several resolutions that addressed the problem of international terrorism and the role of states in supporting it. Specifically, Resolution 1214 of 8 December 1998 recalled that the Security Council was deeply disturbed that Afghan territory was being used to shelter and train terrorists and to plan terrorist acts, and reiterated how important the suppression of international terrorism is for international peace and security. Resolution 1267 of 15 October 1999 stated that the failure of Taliban authorities to comply with Resolution 1214 was unacceptable and that the Security Council was authorized, under Chapter VII of the UN Charter, to take all measures necessary to secure Taliban compliance with the resolution and to ensure that Usama bin Laden was handed over to any national authority which had indicted him (namely the US). Resolution 1269 of 19 October 1999 encouraged states to cooperate in identified ways to 'prevent and fight the threat to international peace and security as a result of terrorist activities.' Resolution 1333 authorised further economic sanctions against

[52] SI No 3365 (Mar. 2001). UK law imposes further restrictions on terrorist financing in the Anti-Terrorism, Crime and Security Act 2001, amending the Terrorism Act 2000: see Chapter 2 of this Report.

[53] See Title III of the US Patriot Act, 'International Anti-Money Laundering Abatement and Anti-Terrorist Financing Act of 2001'. See discussion in K. Alexander, 'United States Financial Sanctions and International Terrorism', *Journal of International Banking and Financial Law,* Butterworths, February 2002.

the Taliban and was the first Security Council resolution to require states to impose asset freezes without delay on the funds and assets of bin Laden and his associates.[54]

1.6.2 The attacks on the United States of 11 September led the UN Security Council to take further steps against international terrorism by adopting two resolutions that require states to cooperate and participate in a global anti-terrorism regime by taking active measures to implement counter-terrorism and financial controls. The two resolutions are Resolutions 1368, adopted on 12 September, and Resolution 1373, adopted on 28 September 2002. Resolution 1368 condemned the attacks and called upon all states 'to work together urgently to bring justice to the perpetrators, organizers and sponsors of these terrorist attacks and stresses that those responsible for aiding, supporting, or harboring the perpetrators, organizers and sponsors of these will be held accountable.'[55] The Resolution calls on all states to increase their efforts 'to prevent and suppress terrorist acts including by increased cooperation and full implementation of the relevant international anti-terrorist conventions and Security Council resolutions, especially resolution 1269 (1999)[56]. The Resolution also expresses the resolve of the international community to take 'all necessary steps to respond to the terrorist attacks of September 2001,' and to combat all forms of terrorism, as provided under the UN Charter.

1.6.3 Security Council Resolution 1373 requires all UN member states to prevent and suppress the financing of terrorists acts and to refrain from providing any type of support, active or passive, for terrorists and to deny safe haven to those who finance, plan or participate in terrorist acts.[57] Resolution 1373 emphasises the importance of freezing the assets of companies and entities owned or controlled by listed terrorist groups. Specifically, Article 1(b) requires states to create an offence for persons who wilfully provide or collect, by any means, directly or indirectly, funds with the knowledge that such funds be used to carry out terrorist acts. Article 1(c) requires states to freeze without delay funds, financial assets, or other economic resources belonging to, or controlled by, persons who commit, or attempt, to commit terrorist acts. Article 1(d) addresses the issue of third party financing by requiring states to prohibit 'nationals or any persons and entities within their territories from making

[54] It should also be noted that Resolution 1363 of 30 July 2001 reaffirmed resolutions 1267 and 1333 by urging all states to uphold these resolutions on the grounds that the situation in Afghanistan constituted a 'threat to international peace and security'.
[55] Resolution 1368.
[56] Resolution 1269 (19 Oct 1999).
[57] Article 2(c).

any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts'.

1.6.4 In addition, Resolution 1373 is significant because it establishes a mechanism to monitor implementation and requires UN member states to share information regarding activities and enforcement matters. The resolution expressly incorporates existing commitments made by UN members in previous international conventions, declarations and resolutions with respect to terrorism and makes them legally binding by invoking Chapter VII of the UN Charter, which authorizes the Security Council to take all necessary action, including imposing economic sanctions and the use of force, to ensure that the objectives of the resolution are achieved.

1.6.5 Resolution 1373 addresses the important issue of implementation by establishing a Counter-Terrorism Committee of the Security Council,[58] consisting of all the members of the Security Council, to monitor implementation of the resolution. The Committee requires all UN members to report according to a timetable on the steps they have taken to implement the resolution. The Committee has the authority to set forth compliance procedures for states to adhere in ensuring that the resolution is implemented. The Resolution authorizes the creation of a trust fund administered by the UN Secretariat and financed by member states to ensure that the Committee's monitoring function is effectively carried out. The Committee's overall mandate is to require UN members to take counter-terrorism measures that they may not otherwise take without treaty or statutory obligations. During the first ninety days following adoption of Resolution 1373, the Committee issued guidance to states on procedures for submitting compliance reports and also suggested areas where states could improve their capacity in adopting legislative and executive measures to combat terrorism. Further, the Committee published a directory of contact points to promote global cooperation and selected a group of independent experts to advise the Committee.[59]

1.6.6 States are required to submit reports regarding the legal, regulatory and enforcement measures they have taken to criminalize terrorist activity and to interdict terrorist

---

[58] The Committee is known as the United Nations Counter-Terrorism Committee. The chair of the committee is the United Kingdom's Ambassador to the United Nations, Sir Jeremy Greenstock. See 'Security Council Hears Report by Chair of UN Counter-Terrorism Committee',*UN Press Release* (18 Jan 2002).

[59] The Committee emphasizes transparency in its work and has made it documents public and accessible via the internet. See http://www.un.org

financing. The Committee will appoint experts to assess individual country reports and to set criteria for determining overall compliance with the requirements of Resolution 1373.[60] The Committee issued a compliance report on 5 April 2002 stating that 143 states had submitted reports and that the Committee had reviewed and sent comments to 62 of those states, while 50 states still had not yet submitted reports.

1.6.7 Many states have reported that the requirement in paragraph 1(b) that each state criminalize the financing of terrorism has already been covered by existing national anti-money laundering legislation and other criminal statutes.[61] The Committee has taken the view that, while money laundering and the financing of terrorism are often inter-related, these crimes are not identical. This is because money laundering can be defined broadly to mean 'the processing of criminal proceeds to disguise their illegal origin.' By contrast, the financing of terrorism often involves moneys that are not necessarily derived from illegal sources, but which are nevertheless used to fund terrorist activities. For instance, assets and profits acquired by legitimate means, and even declared to tax authorities, can be used to finance terrorist acts. Moreover, as discussed above, these proceeds can be generated not only by legitimate businesses but also by donations to charitable, social or cultural organizations, and then diverted from its intended or stated purpose to fund terrorist acts.

1.6.8 Based on the information provided in the Reports, the Committee therefore seeks to address three questions: (1) ascertain exactly what measures states have adopted thus far in criminalizing terrorist financing as required by sub-paragraph 1(b) of the Resolution; (2) what measures states have taken to freeze funds, financial or other assets of persons or entities suspected of terrorist activities as distinct from freezing funds or financial assets of persons involved in money laundering; and (3) what preventive controls or surveillance procedures states are using to ensure that funds intended for the financing of terrorism are not transferred through charitable, religious or cultural organizations.

1.6.9 It should be recognized, however, that disparities between countries in the sophistication of their legal systems and in administrative and technical skills will make the objective of accomplishing more uniform standards difficult, if not

[60] The experts are expected to have expertise in the areas of finance, national legislation, and law enforcement. The UN Secretariat will continue to identify experts for the Committee's ongoing work: see United Nations Press Conference, 'CTC 1373', (10 Jan 2002)(http://www.un.org/Docs/sc/committees/1373/10/jansum.htm).
[61] See Walter Gehr, 'Recurrent Issues, (Briefing for Member States)', (4 Apr 2002).

impractical, for many countries. Indeed, by merely adopting more uniform legal principles and enforcement procedures, especially with respect to the issues of extraterritorial jurisdiction, third party liability, and the precise definition of the offence of financing terrorism, a more uniform and efficient international enforcement regime will likely not emerge because of the lack of uniform national implementation due to disparities in administrative expertise, technical skills, and legal infrastructure. Notwithstanding these obstacles, there is an emerging consensus if the United Nations and other international organizations provide assistance in administrative and technical support for developing and emerging economies so that they can implement the necessary economic controls that the adoption of more harmonized legal principles and enforcement procedures will lead to a more effective international sanctions regime.

1.6.10 The objective of accomplishing more harmonisation in legal principles has been addressed by the experts committee and by the states in their country reports. In many state reports, a major issue of concern has arisen with respect to the precise definition of the financing of terrorism. Some states report that third party criminal liability for the crime of financing terrorism is already covered by the criminal law on *aiding and abetting*. Other state reports explain that the offence of conspiracy covers the offence of financing terrorism. The Security Council experts committee has rejected most of these explanations and in particular has stated that the auxiliary offence of *aiding and abetting* will not without more properly implement sub-paragraph 1 (b) of the Resolution, which requires each state to criminalize direct or indirect support for the financing of terrorism. The experts committee takes the view that Security Council Resolution 1373's requirement that each state become a party to the 1999 Terrorist Financing Convention obliges each state to adopt specific criminal offences that prohibit direct and indirect commercial or financial support for terrorist activity.

1.6.11 Some of the limitations of the Committee include that it will not intrude on the competence of other agencies in the UN system, and it will not seek to provide a legal definition of terrorism, although members will be encouraged to do so. Moreover, the Committee will not be authorized to designate terrorists or terrorist organizations and has no competence to resolve disputes between states over the

designation of terrorists. All such disputes will be referred to the Security Council.[62] Some observers have commented that the Committee's work is rapidly emerging into 'minimum international standards for counter-terrorism law.'[63] This may have implications for development of customary international law in the area of international terrorist controls.

1.7 Jurisdictional conflicts in defining terrorism and in enforcing Resolution 1373

1.7.1 Although the Counter-terrorism Committee's coordination of the implementation of international sanctions has had significant impact in exposing and restricting various aspects of terrorist financing and has fostered a degree of cooperation amongst states in addressing terrorism, the ultimate effectiveness of such sanctions will depend on the ability and willingness of national authorities to enforce them. Indeed, national authorities must ensure that economic sanctions are not evaded by multi-national holding companies composed of shell corporations and other sophisticated financial entities. Moreover, although each member state is permitted to implement and enforce sanctions according to its own legal principles, there should be a fair degree of commonality in how authorities define civil and criminal liability for breaching sanctions laws. Targeted entities should have basic protections against having their assets frozen or confiscated without due process of law. When one country's legal authorities violate such protections, other national authorities often become reluctant to coordinate transnational enforcement efforts. Indeed, the methods to implement the war against terrorism may clash with basic international human rights. Moreover, issues of extraterritorial jurisdiction and third party liability may take on different dimensions in different legal systems, thus thwarting the efficient implementation of international sanctions.

1.7.2 As discussed above, Resolution 1373 requires UN member states to freeze all the assets of designated terrorist groups and entities supporting such terrorists within the jurisdiction of each member state and according to its legal principles. Because the method of designating terrorist groups varies by state and the legal principles by which financial sanctions are imposed varies by state, serious disparities arise concerning the extent that financial sanctions will apply and the legal protections, if

---

[62] See note 58 above.

[63] See B. Zagaris, 'The Merging of International Terrorist and Money Laundering Policy,' *International Enforcement Law Reporter*, Apr 2002, p 39.

any, of those who are accused of supporting – either directly or indirectly – designated terrorists. Moreover, the system of designating terrorists and terrorist support groups varies between countries and is often based on intelligence derived from covert operations, which ordinarily cannot be divulged in judicial or tribunal proceedings. As in previous UN sanctions programmes, the Committee on Counter-Terrorism has failed to apply uniform standards in these areas, and because it has required member states to recognize the freeze orders of other member states directed at particular individuals or groups accused of terrorism without providing any international standards to guarantee that such sanctions are not being imposed in an arbitrary and capricious manner, much dispute has arisen amongst major states with respect to whether such orders should be given mutual respect if issued without adherence to basic human rights.

1.7.3 The Swedish and French governments raised these issues with the Security Council in January of 2002 in a case involving whether they were obliged to recognise certain freeze orders of the US government's Office of Foreign Assets Control (OFAC) with respect to three Somali-born Swedish citizens whom the US had designated as terrorists in the aftermath of the11 September attacks. The Swedish and French governments sought to highlight the issue of the rule of law and the protections, if any, which individuals or businesses were entitled to when confronted with asset freeze orders issued by foreign governments that were acting within the legal framework of the UN sanctions committee. The US had transmitted its terrorists list to the Security Council's Counter-terrorism Committee, and the Security Council had required that member states freeze the assets of the alleged terrorists.

1.7.4 The Swedish government froze the accounts of Abdirisak Aden, Abdulaziz Abdi, and Yusaf Ahmed Ali, on the grounds that US intelligence claimed they had provided financial support to al-Qaida. The alleged terrorists contended that they had only transferred money to their families in Somalia. The Swedish government requested information from the US government in order to determine whether the alleged terrorists were actually involved in terrorist financing. The French government also intervened by urging the Security Council to review its sanctions list and to establish some basic rules for enforcing anti-terrorist financial sanctions that would include specific criteria to impose sanctions, such as a direct link with al-Qaida or the Taliban, and a procedure for regularly reviewing the list. The US government has opposed the Swedish request and the French government proposal

because divulging such information might threaten national security by endangering the ability to gather intelligence.[64]

1.7.5 The three defendants have complained that their assets have been frozen without opportunity to contest the charges. The financial sanctions imposed by the Swedish government are abroad in that they even restrict cash payments by the defendants for legal fees and prohibit Swedes from contributing to their legal defence. Their case has become a *cause celebre* with a prominent Swedish lawyer, Leif Silbersky, taking on their defence. The Swedish ambassador to the United Nations has asked the Counter-Terrorism Committee of the Security Council to review the defendant's inclusion on the sanctions list. The Swedish government has raised these concerns because the freeze order emanates from the US Treasury Department whose authority to designate terrorists and to freeze their assets derives from a presidential order that is based on authority found in the International Emergency Economic Powers Acts of 1977. US courts have ruled that executive orders to impose financial sanctions are subject only to the most limited judicial review. Foreign governments should therefore be concerned about the legitimacy and factual accuracy of US terrorist designations and freeze orders.

1.8 Financial Action Task Force

1.8.1 The Financial Action Task Force (FATF) has also played a significant role in developing international standards to combat terrorist financing. FATF has emerged as a major player in setting international standards to combat financial crime.[65] FATF was established by the G7 Heads of State in 1989 at the G7 Summit. FATF is the only international body dedicated solely to fighting money laundering and other aspects of financial crime. The membership of FATF includes all the members of the Organisation for Economic Cooperation and Development (OECD).[66] In 1990, FATF issued a Forty Point list of Recommendations on money laundering countermeasures intended to constitute an international 'minimal standard in the

[64] S. Schmemann, 'Swedes Take Up the Cause of 3 on US Terror List', *New York Times*, 26 Jan 2002, p. A7, col. 1.

[65] See K. Alexander, 'Multi-national Efforts To Combat Financial Crime and the Role of the Financial Action Task Force', *Journal of International Financial Markets* (Oct 2000).

[66] The FATF Secretariat is located at the OECD.

fight against money laundering'.[67] The Forty Points prescribe a range of actions designed to improve national legal regimes, enhance the role of the financial system, and strengthen international cooperation against financial crime.

1.8.2 The Forty Recommendations are not legally binding under public international law. This is intended to give national authorities maximum flexibility and control in implementing international standards into national legal systems. The non-binding nature of FATF standards however has been called into question in recent years because FATF has on several occasions threatened to impose sanctions against states deemed by FATF as having failed to adopt national legislation to implement the Forty Recommendations.[68] FATF's threat to use sanctions has in most cases resulted in targeted states and jurisdictions adopting the necessary legal measures to implement FATF standards.

1.8.3 In response to the events of 11 September, the Financial Action Task Force convened an extraordinary plenary meeting in Washington DC on 29 and 30 October 2001 with the objective of expanding its mission beyond money laundering and financial crime to include the financing of international terrorist activity. At this meeting, the FATF President, Ms. Clair Lo, the Director of the Hong Kong Securities and Futures Authority, called on all countries in the world to adopt and implement newly-issued FATF 'Special Recommendations' intended to deny terrorists and their supporters access to the international financial system.[69] FATF members established 8 Special Recommendations on Terrorist Financing that have become the international standard for how countries can regulate their financial institutions in a way that reduces exposure to terrorist financing. FATF members take the view that the 'Special Recommendations' on terrorist financing, combined with the FATF Forty Recommendations on Money Laundering, establish the basic framework for detecting, preventing and suppressing the financing of terrorism and terrorist acts.

1.8.4 Special Recommendation I states that 'each country should take immediate steps to ratify and to implement' the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism and to implement immediately the UN

---

[67] See Directorate for Financial, Fiscal and Enterprise Affairs, Organization for Economic Cooperation and Development, FATF VII Report on Money Laundering Typologies 2-3 (1996). See also OECD website: www.oecd.org .

[68] Turkey in 1996 for failing to enact a law criminalizing money laundering and Austria in 2000 for failing to eliminate their anonymous numbered bank account system.

[69] See 'FATF Cracks Down on Terrorist Financing', 31 October 2001, http://www.oecd.org/o.../0,3371,EN-document (visited 27 Nov 2001).

resolutions relating to the prevention and suppression of the financing of terrorism, particularly the UN Security Council Resolution 1373 that was adopted on 28 September 2001. Special Recommendation II urges each country to criminalize the financing of terrorism and associated money laundering.

1.8.5 Equally important, Special Recommendation III requires each country to implement measures to freeze funds without delay or other terrorist assets, and those intermediaries or other third parties who finance terrorism or terrorist organisations should be defined as such in accordance with the United Nations Resolutions relating to the prevention and suppression of the financing of terrorist acts. In addition to freezing assets, Recommendation III urges countries to adopt and implement measures (including legislative ones) that authorises the competent national authorities to seize and confiscate property defined as the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations. This provision appears to allow each country to define what property is considered to be the proceeds of terrorist activity. More important, the FATF Recommendations omit any definition of terrorism and appear to allow member states to adopt a definition under their local law. Special Recommendation IV urges each country to adopt effective regulations that require financial institutions and other business entities subject to anti-money laundering obligations to report promptly to national authorities any suspicious transactions or accounts that may be related to terrorism.

1.8.6 In January 2002, a FATF Plenary Session in Hong Kong issued a statement that FATF would engage all countries, including non-FATF members, in a self-assessment process to ensure that FATF and non-FATF members adopt effective regulatory measures to reduce terrorist financing in their respective jurisdictions. FATF efforts in this area, along with the continued engagement by many national authorities with other international bodies and organisations, seeks to marginalise terrorist financiers by bringing the global financial system under surveillance. To this end, the 'Special Recommendations' supplement and reinforce the measures already adopted by the UN and create a more comprehensive international regime for interdicting the financing and commercial support of terrorists and terrorist activities.

1.8.7 Other international bodies involved in setting international standards to interdict terrorist financing include the G7, G8 and G20. On November 17, 2001, the G20 finance ministers and central bank governors met in Ottawa, Canada and agreed that

they would block terrorist assets in their respective jurisdictions. They also agreed to report publicly on precisely which terrorist groups each country has blocked and the amount of money blocked. This position was also taken by the Executive Board of the International Monetary Fund, which acted on November 18, 2001 to require its members which seek financial assistance to impose similar financial controls.

1.8.8 In February 2002, the G7 heads of state met in Ottawa and agreed an ambitious new programme that would involve the coordination of national computer and telecommunication systems in order to identify terrorists whose assets would be subject to freeze orders. This will involve closer cooperation and coordination between national authorities regarding the disclosure of certain types of information (some of which might be confidential under local law) and the procedures for sharing it, and maintaining it, if possible, in a confidential nature.

Financial Intelligence Units – the Egmont Group

1.8.9 As part of the fight against international money laundering, the OECD countries acting through the Financial Action Task Force created a Financial Intelligence Units (FIUs) network. The FIUs are specialised national agencies designed to attack financial crime in its various modes through the exchange of information, sharing of expertise, and other forms of cooperation. The annual meetings of FIUs began in 1995 at the Egmont-Arenberg Palace in Belgium and today are known as the Egmont Group.[70] The Egmont Group meets on a regular basis and has become a genuine international forum without any official status that has taken the lead in addressing major issues in both money laundering control and terrorist financing.

1.8.10 The global network of information exchange and cooperation established by the Egmont Group has been a valuable and responsive avenue through which to exchange terrorist-related information. Indeed, the US Financial Crimes Enforcement Network (FinCEN) hosted a special meeting of the Egmont Group on terrorist financing in October 2001 to explore ways to support multilateral efforts to combat terrorist financing. During the special meeting, the Egmont Group agreed to: (1) review existing national legislation to identify and eliminate existing impediments to exchanging information between FIUs, especially when such

[70] The Egmont Group seeks to establish for the private sector strategies of prevention in the area of money laundering by emphasising public-private cooperation.

information concerns terrorist activity; (2) encourage national governments to make terrorist financing a predicate offence to money laundering and to consider terrorist financing a form of suspicious activity for which financial institutions should be aware; (3) facilitate information requests from other FIUs and ensure that information passed in the FIU system does not leak to other government agencies; (4) and pool Egmont resources, where appropriate, to conduct joint strategic studies of money laundering vulnerabilities, including the *hawala* underground banking system.

1.9 European Union

1.9.1 The European Community has adopted two Regulations to comply with UN Security Council Resolutions requiring states to interdict the financing of terrorism. Regulation 467/2001 requires certain restrictive measures to be taken – including the freezing of assets – against the Taliban and Usama bin Laden and persons and entities associated with him, such as the al-Quaida organisation. This Regulation however does not expressly require states to take legal measures to restrict third parties from providing material support – either direct or indirect – to terrorists. To achieve this, the EC recently adopted on 27 December 2001 a Council Regulation entitled 'specific restrictive measures directed against certain persons and entities with a view to combating terrorism.' The Regulation expands the list of designated terrorists beyond those affiliated with bin Laden to include many European terrorist groups (Real IRA and the Basque ETA).

1.9.2 The Regulation's Common Position states in Article 3 that the European Community will act within its competence to adopt financial sanctions at the Community level that will ensure that funds, financial assets, economic resources or other related services will not be made available to designated terrorists. The Regulation expressly requires Member States to adopt broad principles of liability to be applied to natural or legal persons who assist in the funding of terrorism. Article 2 of the Regulation prohibits, except where a Member State grants a licence, any person or entity from providing 'financial services to, or for the benefit of, a natural or legal person, group or entity' that is designated as a terrorist. Article 3 prohibits the knowing or intentional participation in activities, which have the object or effect of circumventing the restrictions set forth in Article 2. Article 4 provides a list of disclosure obligations for banks and other financial institutions, including insurance

companies, regarding suspicious accounts and the amount held or controlled by suspect persons and to cooperate with other EC member authorities and the Commission in ensuring that these requirements are effectively enforced. Article 9 allows Member states to determine the precise scope of sanctions (civil and/or criminal) to be imposed where provisions of the Regulation are infringed. Sanctions must be 'effective, proportionate and dissuasive.'

CHAPTER 2

The Law: An Overview

INTRODUCTION

2.1 Remit

2.1.1 Chapters 1 and 2 set out to analyse the impact of the initiatives against terrorist property on banks and financial institutions by considering the principal pressure points that such institutions (referred to in this Introduction as 'institutions' for the sake of convenience) have felt to date under the new initiatives, and also by drawing upon their experience in attempting to comply with earlier (generally anti-money laundering) legislation and requirements.

2.1.2 Before turning to consideration of the practical issues in Chapter 3, this chapter summarises (1) the UK legislative initiatives, (2) the relevant FATF and FSA rules/guidance, (3) the US legislative initiatives and finally (4) the UN action regarding the financing of terrorism. For obvious reasons we have not attempted to deal with any further jurisdictions.

2.2 The practical issues

2.2.1 Significant practical issues facing institutions attempting to abide by the initiatives stem from the problems inherent in identifying terrorist money. Traditional anti-money laundering techniques rely partly at least upon the identification of suspicious transactions/patterns of transactions, and classically the handling of large amounts of cash, the presence of which cannot easily be explained given what is known about the relevant customer. 'Terrorist' money is often generated legitimately; in such cases it only becomes tainted when it is donated (or destined to be donated) to a terrorist organisation. 'Money intended for terrorism does not move around the financial system like dirty money; it does not need to make rapid movements between accounts, across borders, through a range of currencies, into and out of assets. It simply behaves like ordinary money doing ordinary things and so is almost impossible to identify. This means that the usual range of counter-money laundering techniques and tools are of very limited use. For example each act of terrorism may

require relatively small amounts of money – and so neither the cash transaction reporting measures nor suspicious transactions reporting systems are triggered.'[71]

2.2.2 Existing laws and systems are designed to focus on the origins of dirty money – they are not designed to try to second guess where it will be going in the future. They are not able to 'spot legitimate money passing through for illegitimate purposes in the future'.[72] Consequently it is often only if an account holder (or counter-party to transactions on an account) is known or suspected to be involved in terrorism that a bank can be said to have reason to be suspicious.

2.2.3 Accordingly, in attempting to implement the initiatives institutions are highly dependent upon information as to identity. On the assumption that their traditional 'know your customer' procedures give them knowledge of the identity of their clients, they have to try to establish whether any of those clients might be involved in or supporting terrorist activity. At present, there is a multiplicity of lists of 'suspicious' persons, published (often on the internet) by a large number of different bodies. Smaller institutions in particular may find it hard to cope (or to cope competently) with the position as it stands. We have thus addressed the possibility of the creation of a unified, authoritative list, presented in a format that makes it easy to cross check against existing databases.

2.2.4 For similar reasons, we have considered the desirability of creating a single reference point for institutions with queries to raise or with information to pass on, as at present responsibility is or appears to be divided (on no easily identifiable logical basis) between a number of different bodies. Two obvious candidates for such a role are the Treasury and the FSA; in either case it is likely that the added burden would necessitate the creation of a new department, but nevertheless these seem logical choices given the tasks undertaken by them at present.

2.2.5 The difficulties faced by institutions are rendered more acute by the aggravated reputational risk involved in potential breaches of the anti-terrorism initiatives. In the present climate any suspicion to the effect that an institution has somehow aided terrorists might well have a catastrophic effect on that institution; given that in significant respects the initiatives create 'strict liability offences' it will be easier to fall foul of them than is the case with traditional anti-money laundering rules, but the

---

[71] http://www.riskvalues.com

[72] Michael Peel and John Willman, 'The dirty money that is hardest to clean up', *Financial Times*, 20 November 2001.

subtleties of that distinction between the two regimes are likely to be lost on the public. It is of course hoped that the potential solutions mentioned in this paper will be doubly beneficial: they should minimise the risk to institutions of breaching the initiatives, and they should assist society's efforts to prevent terrorism in aiding (particularly smaller) institutions efficiently and effectively to apply the disciplines required by the initiatives.

2.2.6 In addition to the possible creation of a domestic single reference point, we have considered the desirability of creating a single, authoritative international reference point. By the same logic it seems to us desirable that institutions with business in more than one jurisdiction should be able to have reference to one source of information and guidance, confident that in so doing they are meeting the obligations imposed on them. The creation of such a body on the international stage (or endowing an existing body with the role) would be a much more ambitious and difficult task, but nevertheless in our view ought to be considered.

2.2.7 Suggestions similar to some of ours have already been promulgated by a group of large institutions under the rubric of the Wolfsberg principles, and so we have seen fit to include a section summarising the Wolfsberg Group's principles and recommendations (they can be viewed in more detail at www.wolfsberg-principles.com).

2.2.8 This chapter also highlights a number of other discrete issues, including a possible conflict between the Data Protection Act 1998 and anti-money laundering legislation, which has been exacerbated by the recent legislative anti-terrorism initiatives. The conflict arises between rights to data access (possibly including the fact and contents of reports to NCIS) on the one hand, and 'tipping off' offences on the other, and ought in our view clearly to be addressed by a blanket exemption relating to (at least) terrorist related reports.

2.2.9 Given that many of the problems we have identified stem from the lack of any obvious 'terrorist account typology', we have addressed the available evidence as to typologies in paragraph 3.2 below. We have also considered the possibility of harnessing AI technology, in the form of customer relationship management software. Technical approaches to these problems are being developed by the software industry. To really 'know one's customer' an institution needs to have background information about the customer and additionally it needs to *'keep track of the banking services used by the client and any software needs to track the*

relationships between accounts and between clients in different areas of an institution.' [73] Of course, as regulatory processes are strengthened terrorists will probably seek to avoid them by diversifying their financial activities into multiple outlets to avoid the build up of useful informational connections that may trigger suspicious transaction reports — the new 'smurfing.'

2.2.10 Some software companies, eg Risk Values Ltd, are developing programmes which attempt to identify account holders who 'exhibit the characteristics which indicate that they would be willing to abuse the relationship with the financial institution and do it without reference to name, colour, race religion or transaction history.'[74] The system is said to employ standard personality analysis used in market research. It requires the institution to ask a series of questions. These answers are then compared to known data. The software providers claim that the techniques have been validated by cross- research in cultures ranging from Turkey, Taiwan, Yucatan, Honduras, India, United States, Canada, United Kingdom and Israel. However, whilst software may well become a useful tool in the future, our conclusion is that at present at least (particularly given the absence of any definitive statistical database identifying reliable distinctions in operation between terrorist and non-terrorist accounts) it does not provide a complete answer.

UK LEGISLATION

2.3 Introduction

2.3.1 The Terrorism Act 2000 ('Terrorism Act') and the Anti-Terrorism, Crime and Security Act 2001 ('Anti-Terrorism Act') provide for a comprehensive statutory scheme to deal with terrorist property and known or suspected terrorist activity. It is not easy to judge their likely effect on Banks and financial institutions, other than to say that relationships with both regulator and customer are likely to be seriously affected. It is appropriate to deal with the law under the following headings: (1) main offences, (2) duty to disclose information regarding the main offences, (3) obtaining information and evidence and (4) the control of terrorist cash.

---

[73] Tom Obermaier (head of risk management, Deutsche Bank Global Cash Services Division), from 'Anti-Terror Law Puts Banks into the Hot Seat.' http://www.banktech.com/story/amLaundering/BNK200011207S0002

[74] Risk Values Limited at www.riskvalues.com

2.4 Main Offences

2.4.1 The Terrorism Act provides for four main offences, which may potentially impact upon the financial sector. These are fundraising (s 15), use and possession (s 16), funding arrangements (s 17) and money laundering (s 18).

Fundraising

2.4.2 The offence of fund-raising may be committed in three ways: (1) Providing money or other property[75], (2) receiving money or other property[76], (3) or inviting another to provide money or other property[77], intending that it should be used or having reasonable cause to suspect that it will be used for the purposes of terrorism. Note that this offence may be committed by simply making funds available, 'whether or not for consideration'[78].

Use and possession

2.4.3 Section 16 provides that it is an offence to use or possess money or other property intending that it should be used or having reasonable cause to suspect that it will be used for the purposes of terrorism.

Funding arrangements

2.4.4 A funding arrangement is one which results in money or property being made available[79]. Where a person enters into such an arrangement knowing or having reasonable cause to suspect that it will or may be used for the purposes of terrorism, he commits an offence[80].

Money Laundering

2.4.5 The offence of money laundering (s 18) is committed where a person becomes (i) concerned in an arrangement which (ii) facilitates the retention or control by or on behalf of another person of terrorist property by concealment, removal from the jurisdiction, by transfer to nominees, or in any other way[81]. It will be a defence for a

---

[75] Section 15 (3) (a).
[76] Section 15 (2) (a).
[77] Section 15 (1) (a).
[78] Section 15 (4).
[79] Section 17 (a).
[80] Section 17 (b).
[81] Section 18 (1).

person charged under section 18 to prove that he did not know and had no reasonable cause to suspect that the arrangement related to terrorist property[82].

2.4.6 In respect of these main offences section 63 of the Terrorism Act provides for extra-territorial jurisdiction. A person is guilty of an offence under sections 15-18 if anything is done outside the United Kingdom, which would have constituted an offence under those sections if committed in the UK. The maximum sentence on indictment for an offence under sections 15-18 is 14 years, or a fine (present maximum £5000), or both[83].

2.4.7 The courts have the power to make a forfeiture order where a person is convicted of an offence under sections 15-18[84]. Schedule 4 of the Act makes detailed provision for the implementation and enforcement of forfeiture orders. The Schedule also gives courts the right to grant restraint orders where proceedings have been instituted under sections 15-18, but not concluded[85].

2.5 Defences: Disclosure

2.5.1 Where a person is acting with the express consent of a constable (police constable) he will not commit an offence under sections 15-18[86]. Nor will a person commit an offence under those sections if he discloses to a constable his suspicion or belief that money or other property may be terrorist property and he also discloses the information on which his suspicion or belief is based[87]. Any disclosure must be under the person's own initiative and must be made as soon as reasonably practicable[88]. It will be a defence for a person charged with an offence under sections 15-18 if that person intended to make a disclosure and there is a reasonable excuse for it not being made[89]. The provisions of section 21 apply where employers make provision for disclosures to be made to them as if the disclosures were made to constables[90].

---

[82] Section 18 (2).
[83] Section 22.
[84] Section 23 (1).
[85] Schedule 4, para 5.
[86] Section 21(1).
[87] Section 21(2). In practice disclosure is made to the National Criminal Intelligence Service (NCIS). See Goldspink and Cole, *International Criminal Fraud*, Sweet and Maxwell, Vol 1, at 3-62 for a discussion on disclosures to NCIS.
[88] Section 21(3).
[89] Section 21(5).
[90] Section 21(6).

DUTY TO DISCLOSE INFORMATION REGARDING THE MAIN OFFENCE

2.6 Introduction

2.6.1 The duty to disclose information regarding terrorist offences is nothing new, having previously been enforced by the Terrorism Act 2000, and before that the Prevention of Terrorism (Temporary Provisions) Act 1980. The principal difference in obligations between the regulated and non-regulated sectors amounts to this: unregulated persons are affected only by those relevant matters where they have an actual suspicion or belief. Regulated persons, however, must report all relevant matters they might reasonably be expected to know or suspect.

2.6.2 The practical effect of this distinction is, it is submitted, likely to be limited to whether the conduct of a defendant charged with one of the main offences is said to be judged according to a subjective or an objective standard. Given that consideration will inevitably have to be given to whether it was reasonable for a non-regulated defendant not to be put on his guard, the difference will be of little comfort to non-regulated persons[91].

2.7 General (s 19) non-regulated sector

2.7.1 Everyone who obtains information during the course of a trade, profession, business or employment is under a duty to disclose to a constable his belief or suspicion that another person has committed an offence under sections 15-18[92]. A person may disclose a suspicion or belief that any money or other property is terrorist property or derived from it and any matter on which the suspicion or belief is based. If the disclosure is not made as soon as is reasonably practicable an offence is committed[93], attracting a sentence of up to five years on indictment[94].

2.7.2 Section 19(7) again gives extra territorial effect to sections 15 – 18, this time from the point of view of the duty to report under section 19. The practical effect of this is that a suspicion or belief about an offence under section 15 – 18, wherever in the

---

[91] See Goldspink and Cole, *International Commercial Fraud* (Sweet and Maxwell) at 3-63 for a discussion of what constitutes lack of knowledge or suspicion under the 'all crimes' money laundering statute (Criminal Justice Act 1988). The same principles, it is submitted, apply here.
[92] Section 19 (1).
[93] Section 19 (2).
[94] Section 19 (8).

world the offence takes place, is discloseable, and non-disclosure is therefore likewise punishable.

2.7.3 It is a defence to show that there was a reasonable excuse for not making the disclosure[95]. Where a proper disclosure is made to an employer who has in place an established procedure for making such disclosures, a defence is provided[96]. Finally information obtained in privileged circumstances otherwise than with a view to furthering a criminal purpose is also covered by a defence[97].

2.8 Regulated sector (s 21A)

2.8.1 Those businesses in the regulated sector are defined by Schedule 3A of the Terrorism Act (inserted by s 3 of the Anti-Terrorism Act). This includes the following activities: accepting deposits by a person with permission to accept deposits, the business of the National Savings Bank, bureaux de change, credit unions and dealing, arranging, managing or advising on investments[98]. The financial institutions will be largely the same as those subject to the 1993 Money Laundering Regulations, with the exception that bureaux de change are now included.

2.8.2 Section 3 of the Anti-Terrorism Act also inserted sections 21A-21B into the Terrorism Act. Section 21A provides that a person commits an offence if he does not disclose information from which he knows or suspects or has reasonable grounds for knowing or suspecting that person has committed an offence under sections 15-18, to a constable or a nominated officer (this is a person who is nominated by the employer to receive such disclosures (s 21 (7)) as soon as practicable. Similar to section 19 there are defences for non-disclosure where there is a reasonable excuse and for information imparted in privileged circumstances[99]. The maximum sentence on indictment is again five years[100].

2.8.3 Section 21B provides for protection from a breach of any restriction on the disclosure of information where disclosures are made in the regulated sector.

---

[95] Section 19 (3).
[96] Section 19 (4).
[97] Section 19 (5).
[98] Schedule 3A, para 1.
[99] Section 21A(5).
[100] Section 21A(12).

OBTAINING INFORMATION AND EVIDENCE

2.9 Search and seizure

2.9.1 Schedule 5 of the Terrorism Act details the procedures required for searches to be made. Warrants may be granted on application to a Justice of the Peace to search premises and any person on them, and to seize and retain any relevant information that is found on the premises[101]. Information will be relevant if there are reasonable grounds to believe that it is likely to be of substantial value to a terrorist investigation and it must be seized in order to prevent it from being concealed, lost, damaged, altered or destroyed[102]. This does not apply to those objects that are the subject of legal privilege[103]. Warrants may only be granted for the purposes of a terrorist investigation and if there are reasonable grounds for believing that there is material on the premises of the nature specified[104]. It is an offence to wilfully obstruct a search[105].

2.10 Customer information orders

2.10.1 Schedule 6 of the Terrorism Act allows a court to grant orders, which require financial institutions (an authorised person who carries on the business of taking deposits, a building society, a credit union etc (see Sched 2 (6)) to provide in a specified manner customer information for the purposes of a terrorist investigation. Customer information includes the customer's account number, full name, date of birth, and address or former address[106]. It is an offence not to comply with any requirement in an order, punishable by fine[107]. A director, manager or secretary of the institution may also be liable under this section and if found guilty, may be liable to imprisonment for up to six months[108]. It will be a defence to show that the information required was not in the institution's possession or that it was not reasonably practicable for the institution to comply with the requirement[109]. The court must be satisfied that the order is sought for the purposes of a terrorist

[101] Paragraphs 1(1)-(2).
[102] Paragraph 1(3).
[103] Paragraph 1(4) (a).
[104] Paragraph 1(5).
[105] Paragraph 3(7).
[106] Paragraph 7.
[107] Paragraph 1 (3).
[108] Paragraphs 8(2)-(3).
[109] Paragraph 1(4).

investigation, the tracing of the property is desirable and the order will enhance the effectiveness of the investigation[110].

2.11 Account Monitoring Orders

2.11.1 Section 38A and Schedule 6A have been inserted into the Terrorism Act by the Anti-Terrorism Act, Schedule 2. Schedule 6A provides that an account monitoring order may be granted by a Circuit Judge. Such an order states that a particular financial institution must for a specified period, in the manner specified, at or by the time specified and at the places specified provide specified information to an appropriate officer (this will be a police officer)[111]. The court may grant an order if satisfied that the order is sought for a terrorist investigation, the tracing of terrorist property is desirable and that the order will enhance the effectiveness of the investigation[112]. The time period of the order must not exceed 90 days[113].

2.11.2 Where a person has information which he believes will assist in preventing the commission by another person of an act of terrorism or securing the apprehension, prosecution or conviction of another person for acts of terrorism there is a duty to disclose this as soon as is reasonably practicable (s 38B, inserted by the Anti-Terrorism Act, s 117). Disclosure of the information should be made to a constable[114]. It will be an offence not to make the disclosure without a reasonable excuse[115].

CONTROL OF TERRORIST CASH

2.12 Modes of control

The legislation provides for four modes of controlling cash used for terrorist purposes. These are seizure, forfeiture, freezing orders, and restraint orders.

Seizure

2.12.1 Schedule 1 of the Anti-Terrorism Act makes detailed provisions for the seizure and forfeiture of terrorist cash. Under Part 2 of the Schedule an 'authorised officer' (a

[110] Paragraph 5.
[111] Paragraph 2(4).
[112] Paragraph 2(1).
[113] Paragraph 2 (5).
[114] Section 38B(3)(a).
[115] Section 38B (4).

constable, customs officer or an immigration officer[116]) may seize any cash where he has reasonable grounds for suspecting that it is terrorist cash (cash intended to be used for the purposes of terrorism, consists of the resources of a proscribed organisation (those organisations listed in Sched 2 of the Terrorism Act), or represents property obtained through terrorism[117]) or part of it is terrorist cash (where it is not reasonably practicable to seize part of it[118])[119].

2.12.2 Cash seized under this Part may be detained for a period of 48 hours[120]. If an order is thereafter made by a magistrates' court, the cash may be further detained for up to 3 months[121]. Successive orders may be made up to a total period of two years[122]. Such an order will only be granted on one of the following conditions:

(i) there are reasonable grounds to suspect that the cash is intended to be used for the purposes of terrorism and that either the continued detention of the cash is justified while its intended use is further investigated or consideration is given to bringing proceedings against someone with which the cash is connected or proceedings against such a person have been started but not concluded.

(ii) there are reasonable grounds for suspecting that the cash consists of resources of a proscribed organisation and it is justified while an investigation is made etc.

(iii) there are reasonable grounds for suspecting that the cash is 'earmarked as terrorist property' and it is justified while an investigation is made etc[123].

2.12.3 Property earmarked as terrorist property is property which is obtained through terrorism[124]. Any cash that is detained for more than 48 hours must be held in an interest bearing account and any interest will be added on its release or forfeiture (this does not apply to cash which is required for evidence of an offence or evidence in proceedings)[125]. The person from whom cash was seized may apply to the court to

[116] Paragraph 19(1).
[117] Paragraph 1.
[118] Paragraph 2(2).
[119] Paragraph 2.
[120] Paragraph 3(1).
[121] Paragraph 3(2)(a).
[122] Paragraph 3(2)(b).
[123] Paragraph 3(6).
[124] Paragraph 11(1).
[125] Paragraph 4.

have the whole or part of the cash released, but this will not be allowed where proceedings for forfeiture have not been concluded or while any proceedings in the UK or elsewhere have in relation to the cash are yet to be concluded[126].

Forfeiture of detained cash

2.12.4 Where cash is detained under Part 2, an authorised officer, or the Commissioners of Customs and Excise may apply to court to have the whole or part of it forfeited (Pt 3). A forfeiture order will only be granted if the court is satisfied that the cash or part of it is terrorist cash[127]. Any party to forfeiture proceedings may make an appeal before the end of a 30-day period starting from the date on which the order was made[128]. After this period has elapsed or after an appeal is disposed of, the cash and any interest accrued must be placed in the Consolidated Fund[129].

2.12.5 A person from whom cash has been seized may apply to the court for it to be released if the property he was deprived of was not, immediately before it was seized property obtained by or in return for criminal conduct and nor did it represent such property (Pt 4). Where no forfeiture order is made the person may apply to the court for compensation[130].

Forfeiture

2.12.6 There is provision in the Terrorism Act for forfeiture orders to be made where a person is convicted of an offence under section 11 or 12 (membership or support of a proscribed organisation[131]). The order can apply to any money or other property which the person had in his possession or under his control at the time of the offence and has been used in connection with the activities of the specified organisation or the court believes that it may be so used[132].

Account freezing orders ('freezing orders'): Anti Terrorism Act, section 4

2.12.7 Orders made under these provisions should not be confused with the traditional civil litigation freezing order. They prohibit persons from making funds available to or

[126] Paragraph 5.
[127] Paragraph 6(2).
[128] Paragraph 7.
[129] Paragraph 8 (1)(a).
[130] Paragraph 10(1).
[131] Section 111(1).
[132] Section 111(2).

for the benefit of a person(s) specified in the order, and may be made by the Treasury by statutory instrument under the provisions of the Anti-Terrorism Act[133]. They cease to have effect after two years[134]. Under section 4 the Treasury must reasonably believe that action which is to the detriment of the UK's economy (or part of it) has been or is likely to be taken by a person or persons, or action constituting a threat to the life or property of one or more nationals/ residents of the UK has been or is likely to be taken, and (2) the person who is believed to have taken the action must be either the government of a country or territory outside the UK or resident of a country or territory outside the UK[135].

2.12.8 Schedule 3 makes further provision in relation to the detail of freezing orders and the disclosure of information. The order must include provision as to the meaning of 'making available to, or for the benefit of', such as allowing a person to withdraw from an account[136]. An order may require information or documents to be provided if reasonably needed for the purposes of ascertaining whether an offence has been committed[137]. For such a requirement to be in place the following conditions must be met[138]. Firstly, the person required to disclose must be specified in the order. Secondly, this person must know or suspect that the person specified in the order, as being the person for whose benefit the funds are not to be made available, is or has been a customer or a person with whom he has had dealings since the freezing order has been in place. Thirdly, the information on which the knowledge or suspicion is based has come to him in the course of the business sector. A person commits an offence if he fails to provide evidence or does so recklessly[139].

Restraint orders

This is one of the move traditional forms of attaching and preserving the (alleged) proceeds of criminal conduct. The Anti Terrorism Act strengthens and extends the powers of the High Court to make a restraint order under Schedule 4 of the Terrorism Act. Essentially the court need only be satisfied that a person is to be changed under sections 15-18 of the Terrorism Act, and that a forfeiture order has

[133] Anti-Terrorism Act, s 5(1).
[134] Section 8.
[135] Sections 4 (2)-(3).
[136] Paragraph 3.
[137] Paragraph 5(1).
[138] Paragraph 6.
[139] Paragraph 7(4).

been made, or may be made in any proceedings. (The old provision referred to 'those proceedings'[140])[141].

OVERVIEW OF FATF/FSA RULES ON TERRORIST FINANCING; DATA PROTECTION ACT; JMLSG GUIDANCE NOTES

2.13 Financial Action Task Force (FATF)

What is the FATF?

(Note: All passages in quotes below are sourced directly from the FATF website, http://www1.oecd.org/fatf/).

2.13.1 'The Financial Action Task Force on Money Laundering (FATF) is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering. The Task Force is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms to combat money laundering.

2.13.2 'The FATF monitors members' progress in implementing anti-money laundering measures, reviews money laundering techniques and counter-measures, and promotes the adoption and implementation of anti-money laundering measures globally. In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering.

2.13.3 'The FATF does not have a tightly defined constitution or an unlimited life span. The Task Force conducts regular reviews of its mission every five years. The FATF has been in existence since 1989, and it has been agreed that it should continue its work until 2004. It will only continue to exist and to perform its function after this date provided the member governments agree that this is necessary'.

History of the FATF

2.13.4 'In response to mounting concern over money laundering, the Financial Action Task Force on Money Laundering (FATF) was established by the G-7 Summit that was held in Paris in 1989. Recognising the threat posed to the banking system and to financial institutions, the G-7 Heads of State or Government and President of the

[140] Terrorism Act, Sched 4, para 5(2)(c).
[141] Anti-Terrorism Act, Sched 2, para 2(2)(c).

European Commission convened the Task Force from the G-7 member States, the European Commission, and eight other countries.

2.13.5 'The Task Force was given the responsibility of examining money laundering techniques and trends, reviewing the action which had already been taken at a national or international level, and setting out the measures that still needed to be taken to combat money laundering. In April 1990, less than one year after its creation, the FATF issued a report containing a set of Forty Recommendations, which provide a comprehensive blueprint of the action needed to fight against money laundering'.

The Forty Recommendations

2.13.6 These fall under the following headings:

- General framework;
- Role of national legal systems in combating money laundering (scope of the criminal offence of money laundering: provisional measures and confiscation);
- Role of the financial system in combating money laundering (customer identification and record keeping rules: Increased diligence of financial institutions: measures to cope with the problem of countries with no or insufficient anti-money laundering measures: Other measures to avoid money laundering: implementation and role of regulatory and other administrative authorities);
- Strengthening of international co-operation (administrative co-operation: other forms of co-operation).

2.13.7 'During 1991 and 1992, the FATF expanded its membership from the original total of 16 to 28 members. Since that early period, the FATF has continued to examine the methods used to launder criminal proceeds and has completed two rounds of mutual evaluations of its member countries and jurisdictions. FATF has updated the Forty Recommendations to reflect the changes which have occurred in money laundering and has sought to encourage other countries around the world to adopt anti-money laundering measures'.

Extraordinary plenary on terrorist financing

2.13.8 'At an extraordinary Plenary on the financing of terrorism held in Washington, DC on 29 and 30 October 2001, the FATF expanded its mission beyond money laundering. It will now also focus its energy and expertise on the world-wide effort to combat terrorist financing. During the extraordinary Plenary, the FATF agreed to and issued new international standards to combat terrorist financing, which it calls on all countries to adopt and implement. Implementing these Special Recommendations will deny terrorists and their supporters access to the international financial system. The agreement on the Special Recommendations commits members to:

- Take immediate steps to ratify and implement the relevant United Nations instruments.
- Criminalize the financing of terrorism, terrorist acts and terrorist organisations.
- Freeze and confiscate terrorist assets.
- Report suspicious transactions linked to terrorism.
- Provide the widest possible range of assistance to other countries' law enforcement and regulatory authorities for terrorist financing investigations.
- Impose anti-money laundering requirements on alternative remittance systems.
- Strengthen customer identification measures in international and domestic wire transfers.
- Ensure that entities, in particular non-profit organisations, cannot be misused to finance terrorism'

Plan of action

2.13.9 'In order to secure the swift and effective implementation of these new standards, FATF agreed to the following comprehensive plan of action:

- By 31 December 2001, self-assessment by all FATF members against the Special Recommendations. This will include a commitment to come into compliance with the Special Recommendations by June 2002 and action plans addressing the implementation of Recommendations not already in place. All countries around the world will be invited to participate on the same terms as FATF members.

- By February 2002, the development of additional guidance for financial institutions on the techniques and mechanisms used in the financing of terrorism. This additional guidance has now been published.
- In June 2002, the initiation of a process to identify jurisdictions that lack appropriate measures to combat terrorist financing and discussion of next steps, including the possibility of counter-measures, for jurisdictions that do not counter terrorist financing.
- Regular publication by its members of the amount of suspected terrorist assets frozen, in accordance with the appropriate United Nations Security Council Resolutions.
- The provision by FATF members of technical assistance to non-members, as necessary, to assist them in complying with the Special Recommendations'.

2.13.10 'In taking forward its plan of action against terrorist financing, the FATF will intensify its co-operation with the FATF-style regional bodies and international organisations and bodies, such as the United Nations, the Egmont Group of Financial Intelligence Units, the G-20, and International Financial Institutions, that support and contribute to the international effort against money laundering and terrorist financing.

2.13.11 'FATF also agreed to take into account the Special Recommendations as it revises the FATF Forty Recommendations on Money Laundering and to intensify its work with respect to corporate vehicles, correspondent banking, identification of beneficial owners of accounts, and regulation of non-bank financial institutions'.

2.14 Financial Services Authority - Money Laundering Sourcebook

What is the Financial Services Authority (FSA)?

2.14.1 The FSA is the single regulator of the Financial Services industry in the UK. It is a company limited by guarantee, which is accountable to HM Treasury for the performance of its functions. It was set up with four statutory objectives[142]:

- Market confidence
- Public awareness
- The protection of consumers

[142] Financial Services and Markets Act 2000 s 2(2).

- The reduction of financial crime

2.14.2 The reduction of financial crime objective is reducing the extent to which it is possible for a business carried out by a regulation person or in contravention of the general prohibition[143] to be used for a purpose connected with financial crime[144]. The FSA must have regard, in considering the reduction of financial crime objective, to the desirability of regulated persons being aware of the risk of their business being used in connection with the commission of financial crime, and of regulated persons taking appropriate measures (in terms of administration and employment practices, and their conduct of transactions) and devoting adequate resources to prevent financial crime, facilitate its detection, and monitor its incidence[145]. 'Financial crime' includes any offence involving fraud or dishonesty, misconduct in or misuse of information relating to a market, or handling the proceeds of crime[146].

2.14.3 Since 1 December 2001, the FSA has been a prosecuting authority (except in Scotland) in respect of money laundering[147]. This power applies whether or not the entity to be prosecuted is regulated by the FSA. In respect of the financial institutions the FSA does regulate, it has issued a Sourcebook setting out the Rules it has issued in relation to money laundering[148]. The Sourcebook[149] operates 'parallel to but separate from' the criminal law in the area of money laundering prevention.

Purpose of the Sourcebook

2.14.4 The purpose of the sourcebook is to require relevant firms to have effective anti-money laundering systems and controls, in order to reduce the opportunities for money laundering in relation to relevant firms. It is also to require relevant firms to ensure that approved persons exercise appropriate responsibilities in relation to these anti-money laundering systems and controls.

2.14.5 Section 2 of the Act (the FSA's general duties) sets out the regulatory objectives of promoting market confidence and public awareness, protecting consumers and reducing financial crime. The reduction of financial crime objective is the most

[143] Sections 19(1)-(2).
[144] Section 6(1).
[145] Section 6(2).
[146] Section 6(3).
[147] Section 402 (b).
[148] Pursuant to s 146 Financial Services and Markets Act 2000.
[149] See Appendix 3 for the full text of the FSA Money Laundering Sourcebook.

important to the sourcebook. One aspect of the reduction of financial crime objective is the risk of the businesses of relevant firms being used in connection with offences which involve handling the proceeds of crime. It follows that an effective and proportionate regulatory regime is important in reducing the extent to which it is possible for the businesses carried on by relevant firms to be used for money laundering. These rules and compliance with them will also help the FSA to meet the objective of maintaining market confidence, by reducing the risks posed to the financial community by money laundering. As to the public awareness objective, this sourcebook is designed to assist relevant firms and, through them, the public at large, to be better informed about the safeguards for the financial system provided by effective anti-money laundering systems and controls. Consumers are better protected if relevant firms are able to protect themselves against criminal activity and to record the steps they have taken for that purpose.

2.14.6 The sourcebook provides support, in relation to money laundering, for certain other parts of the Handbook, mainly:

(a) the Principles (PRIN), especially PRIN 3 (eg 'Management and Control – a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems');

(b) the Statements of Principles and Code of Practice for Approved Persons (APER), in particular Statements of Principle 2 ('Skill care and diligence – an approved person must act with due skill care and diligence in carrying out his controlled function') and Principle 7 ('Regulatory requirements – an approved person performing a significant influence function must take reasonable steps to ensure that the business of the firm for which he is responsible in his controlled function complies with the regulatory requirements imposed on that business');

(c) Senior Management Arrangements, Systems and Controls (SYSC), in particular SYSC3 ('a firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business'); and

(d) the Training and Competence sourcebook(TC).

2.14.7 The sourcebook relates to regulatory requirements, as opposed to requirements imposed by the criminal law. It is therefore not relevant regulatory or supervisory guidance for the purposes of regulation 5(3) of the Money Laundering Regulations.

Content of the Sourcebook

2.14.8 The Sourcebook is split into eight chapters headed *Application and Purpose, General Money Laundering Duties, Identification of the Client, Reporting, Using National and International Findings on Material Deficiencies, Awareness of and Training for Staff, The Money Laundering Reporting Officer (MLRO) and Other Arrangements, Sole Traders and Authorised Professional Firms.*

- Chapter 1 is covered in paragraphs 2.14.4 - 2.14.7 above on the purpose of the Sourcebook.
- Chapter 2 sets out the general duty to set up and operate arrangements to ensure that the firm and its representatives comply with the Rules.
- Chapter 3 defines specific terms, and sets out the duty on the firm to take reasonable steps to find out who its client is. This includes verifying the identity of the client and any agent of the client. To this end the FSA will have regard to compliance with the JMLSG Guidance Notes in assessing whether a breach of the Rules has occurred. The timing of the identification requirement, and exceptions to the Rules are also outlined. Additional guidance is given about the identification of financially excluded individuals.
- Chapter 4 covers internal reporting procedures (including disciplinary arrangements for staff who fail to report without a reasonable excuse), access to know your business information for the MLRO to investigate reports, and external reporting requirements.
- Chapter 5 requires firms to take reasonable steps to ensure it obtains and makes use of any government or FATF findings on material deficiencies in money laundering arrangements. This chapter is examined in more detail below.
- Chapter 6 sets out requirements for ensuring that staff are made aware of and are given regular training about what is expected of them in relation to money laundering prevention, and what the consequences for the firm and for them are if they fall short of those expectations.

- Chapter 7 highlights the role and responsibilities of the MLRO. It also covers a requirement for the MLRO to make an annual report on compliance with the Sourcebook to the firm's senior management, and record keeping arrangements.
- Chapter 8 specifies which chapters of the Sourcebook apply to Sole Traders and Authorised Professional Firms.

Focus on Chapter 5 of the Sourcebook

2.14.9 'The purpose of this chapter is to enable government and FATF findings of inadequacy, concerning the approach to money laundering of individual countries or jurisdictions, to be brought to bear on relevant firms' decisions and arrangements'.

2.14.10 A relevant firm must take reasonable steps to whenever this rule applies to ensure that it obtains and makes proper use of any government or FATF findings……'

2.14.11 'Proper use' includes applying the information on the introduction of a client for a one off transaction, or on the introduction by a client of a person on whose behalf he is acting. Also to applying the information whenever first obtained to know your business information, and disseminating the information in the course of dealing with staff awareness and training.

2.14.12 'Findings' are 'any published notices which are issued by the government of the UK, or any government department in the UK, or by the FATF, and which contain a finding or other conclusion on the part of the government or a government department or the FATF:

(a) that it has examined the arrangements for restraining money laundering in a particular state or jurisdiction other than the UK, and

(b) that it has found those arrangements to be materially deficient in comparison with one or more of the relevant internationally accepted standards, including any recommendations published by the FATF, required of or recommended to States and jurisdictions'.

2.14.13 The FSA has agreed to publish on its website from time to time any government, government department, or FATF findings in order to assist firms in monitoring current findings to which Chapter 5 relates. Any extracts in quotes are sourced directly from the FSA Money Laundering Sourcebook.

2.15 FSA Press releases post 11 September 2001

FSA press release 20 September 2001: 'FSA Statement: follow-up to events in the US.'

2.15.1 The FSA reminded the firms that it regulates they should check their records for names of alleged subjects under investigation by the FBI in connection with the World Trade Centre and Pentagon terrorist attacks (the FBI list of names is available on the FSA website at www.fsa.gov.uk). Firms were also reminded of their general legal obligations to report suspicious transactions.

2.15.2 Carol Sergeant, Managing Director of Regulatory Processes and Risk at the FSA, said:

> 'Many financial institutions have already checked their records for these names. This is, however, not just something that banks should be looking at – it is an issue for all financial institutions in the UK. Firms should review any dealings with these individuals, if they have not already done so, to ensure all necessary suspicious transaction reports have been made to the National Criminal Intelligence Service in the usual way. Firms should not of course confine themselves to these names. I want to remind them that they have a legal responsibility to report any suspicious transaction'.

NB: The FSA stated that it would be contacting firms it regulates to ensure that they are checking their records in line with this request. Separately, the Bank of England had also written to banks in the UK reminding them of the long-standing financial sanctions imposed by the United Nations against the Taliban, Usama bin Laden or anyone acting on their behalf.

2.15.3 The FSA continues to liaise closely with the National Criminal Intelligence Service, the Metropolitan Police and the Bank of England and all other relevant authorities both in the UK and elsewhere. The FSA encouraged firms to check their website on a regular basis for further updates.

FSA press release 25 September 2001: 'Assets Frozen in the United States'

2.15.4 The US President, George W Bush, issued an Order targeting terrorists and blocking the accounts of a number of organisations and individuals. A list of those identified

in the order, published by the US office of Foreign Assets Controls (OFAC) was attached.

2.15.5 The FSA reminded the firms it regulates to check their records for those named by OFAC. Carol Sergeant, Managing Director of Regulatory Processes and Risk at the FSA said:'As with the names of suspected terrorists published recently by the FBI, it is important that all firms should review any dealings with the individuals and entities named by OFAC, if they have not already done so. Under money laundering and anti-terrorism legislation, firms need to ensure all necessary suspicious transaction reports have been made to the National Criminal Intelligence Service in the usual way'.(The list published by OFAC can be located at the OFAC website at www.treas.gov/ofac)

NB: On 20 September 2001, the FSA circulated the FBI's list of subjects allegedly connected with the terrorist attacks in the US. They (the FSA) reminded regulated firms that they should check records for names of alleged subjects under investigation by the FBI and were also reminded of their general legal obligations to report suspicious transactions.

2.16 Data Protection Act 1998

2.16.1 Individuals are entitled to access to the personal data held about them by data controllers, including Financial Institutions. This right is enshrined in section 7 of the Data Protection Act 1998 ('The Act'). Under section 7, individuals are entitled to be told by data controllers whether or not the controller is processing their data. If their data is being processed, the data controller must give a description of the personal data, the purposes for which it is being processed, and the recipients to whom it is disclosed. The information must be disclosed in an intelligible form.

2.16.2 Data subjects wanting access to data held about them must apply to the data controller in writing. Generally, a fee will be required. Requests must be complied with within 40 days of receipt of a request. This deadline may be extended if receipt of the fee is delayed, if the data controller needs to satisfy him/herself as to the identity of the person making the request, or if it is difficult to locate the information requested by the data subject.

2.16.3 The Act applies to electronic and manually operated personal data records, under section 1(1) (c). An exemption to this right of access applies under section 29 where

the processing is required for, among other things, the prevention or detection of crime, or the apprehension or prosecution of offenders. However, guidance to the Act, at paragraph 5.3.4, suggests that such exemption will not act as a blanket, and all cases will be viewed on their merits as to whether the exemption applies.

2.17 Terrorist funding and the JMLSG December 2001 Guidance Notes

2.17.1 The overall effect of the changes made to the February 2001 version of the Money-Laundering Guidance Notes, as reflected in the December 2001 version, is to place more emphasis on the implications of the Terrorism Act 2000 and the Anti-Terrorism Crime and Security Act 2001 in relation to reporting obligations. Details of information which may be sought in respect of a terrorist investigation were already outlined in Section 7 (paragraphs 7.25 and 7.26) of the February 2001 Guidance Notes, and this guidance remains unchanged. Sections 2 and 5 contain new guidance on reporting obligations. Section 8 contains an outline of the Terrorism Act 2000 which replaces previous guidance on the Prevention of Terrorism (Temporary Provisions) Act 1989.

Section 2: What the UK Law & Financial Sector Regulations & Rules Require

2.17.2 Section 2.5 gives guidance on the obligation to report, and the implications of failing to report, terrorist funding or the suspicion of terrorist funding.

2.17.3 Section 2.6 notes the test of disclosure has been strengthened by the Anti-Terrorism Crime and Security Act from subjective to objective (making it an offence not to report if there is 'reasonable grounds' to suspect terrorist funding). This paragraph also notes that the court would consider whether a defendant had followed relevant approved guidance in this situation.

2.17.4 Several new paragraphs (2.32 - 2.36) reiterate the statutory obligation to report any suspicion of terrorist financing. These new paragraphs also describe the key differences between the use of terrorist and criminal funds which make it difficult to identify and track terrorist funds, and emphasize the importance of 'know your customer' procedures in reducing a firm's risk in this area.

Section 5: Recognition and Reporting Suspicious Transactions

2.17.5 Section 5.2 reiterates the mandatory obligations to report any suspicion of terrorist financing.

Section 8: Appendix C

2.17.6 This section gives a basic outline of the Terrorism Act 2000. This Act came into effect in February 2001 and replaces the Prevention of Terrorism (Temporary Provisions) Act 1989. The guidance states that the new Act provides:

- a new definition of terrorism
- a broader range of financial offences
- removal of jurisdictional boundaries
- wider powers to access information

and lists the sections of the Act which set out the duties of disclosure and offences under the Act.

2.17.7 The FSA has determined that it does not wish to issue regulatory guidance in support of the Regulations. The Bank of England Sanctions Unit has issued a letter to the BBA giving some guidance to Banks, but only a proportion of terrorist groups are subject to Bank of England sanctions.Given those facts, we have considered whether or not the JMLSG is the right body to give guidance on terrorist funding.

2.17.8 Practical guidance on terrorist financing is limited and the main outstanding issues are:

1. Industry best practice on terrorist financing is still developing and there needs to be a body that establishes standards and can make representations on behalf of financial sector firms.
2. There are practical difficulties associated with the volume of names published on the numerous lists and it is accepted that some lists are more important than others.
3. Where firms obtain a name match between a customer and one of the published names, further identifiers e.g. dates of birth and addresses are not always available to assist the firm determine whether the customer is the target of financial sanctions.
4. Firms should assess which countries carry the highest risks and should conduct careful scrutiny of transactions from countries known to be a source of terrorist financing. Firms could and should work together with Government on the risk assessment.

2.17.9 The major banks have made representations to the Bank of England because the information relating to financial sanctions (including the various lists of names of terrorist suspects) needed to be accessed via press releases. The Bank of England now has a consolidated list of names on the Bank's web site in a pdf file and has also made available on its web site a revised source document in an Excel spreadsheet. This should enable banks to import versions into their databases with advantages for searching databases.

2.17.10 It seems that the JMLSG is the correct body to give detailed guidance to the financial sector on terrorist financing for the following reasons:

1. The JMLSG has been producing Money Laundering Guidance Notes for the financial sector since 1990. The purpose of the JMLSG Guidance Notes is to indicate good generic industry practice and to give a practical interpretation of the Regulations.
2. Regulation 5(3) of the Money Laundering Regulations 1993 provides that in determining whether a person or institution has complied with any of the requirements of the Regulations, a court may take account of relevant guidance issued or approved by a supervisory or regulatory body, or in its absence, guidance provided by a trade association or other representative body. The FSA will take into account compliance with the JMLSG Guidance Notes when assessing firms.
3. The JMLSG comprises 15 member associations, giving wide scope within the financial sector. The Guidance Notes are applicable to the following;

    - all banks, building societies and other credit institutions;
    - all individuals and firms engaging in investment business within the meaning of the Financial Services and Markets Act 2000.
    - all insurance companies covered by the European Life Directives, including the life business of Lloyd's of London.
    - bureaux de change, cheque encashment centres and money transmission services etc; and

- all unregulated financial sector businesses including retail credit providers and asset finance providers,

to the extent that the relevant business for the purposes of the Regulations is within the jurisdiction of the United Kingdom courts.

4. The risk of terrorist funding entering the financial system can be reduced if firms apply satisfactory anti-money laundering strategies and particularly in respect of know your customer procedures.

5. The scope of the JMLSG Guidance Notes includes the legal requirements that apply where there is a suspicion that funds will be used for the purposes of terrorism. The Anti-Terrorism Crime and Security Act 2001 strengthens the test of disclosure in respect of terrorist funding from subjective to objective by making it an offence not to make a report wherever information received in the course of business in the regulated sector provides 'reasonable grounds' to suspect terrorist funding. In recognition of this stronger test the court will be asked to consider whether a defendant has followed relevant guidance approved by HM Treasury. Guidance on Terrorist Financing that is included in the JMLSG Guidance Notes has been drafted and approved by HM Treasury for this purpose.

2.17.11 A Money Laundering Advisory Committee is being established by HM Treasury in order to influence the development of anti money laundering strategies. The inaugural meeting took place during May 2002 and included representatives from the Treasury, Home Office, JMLSG, Financial Services Authority, National Criminal Intelligence Service and professional bodies such as the Law Society and the Consultative Committee of Accountancy Bodies. This further reinforces the semi-official position that the UK Government issues specific guidance to financial institutions through the JMLSG. In view of the above, we believe that the JMLSG remains the right body to give guidance on terrorist funding.

US ANTI-MONEY LAUNDERING REGULATION

2.18 Introduction

2.18.1 US anti-money laundering legislation is contained in 18 U.S.C. §§ 1956, 1957 (a criminal law statute), and the Bank Secrecy Act 1970 and its implementing regulations ('BSA'). On 26 October 2001, President Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the 'Patriot Act'). Title III of the Patriot Act, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 (the 'IMLA'), has amended the anti-money laundering provisions in 18 U.S.C. §§ 1956, 1957 and the BSA. A summary of the principal anti-money laundering provisions and the amendments introduced recently is set out below.

2.19 Section 1956

2.19.1 Title 18 U.S.C. § 1956 ('section 1956') prohibits any person from conducting or attempting to conduct a *financial transaction* while knowing or being wilfully blind to the fact that the property involved in the financial transaction represents the proceeds of some form of unlawful activity.

2.19.2 The requirement of a financial transaction is broadly defined. It includes any purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition and with respect to a financial institution includes a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument, use of a safe deposit box, or any other payment, transfer, or delivery through or to a financial institution. As indicated below, the IMLA has broadened the definition of a financial institution to include foreign banks.

2.19.3 The financial transaction must in fact involve the proceeds of specified unlawful activity. The phrase specified unlawful activity is also broadly defined in section 1956 and covers over 170 activities, including mail fraud, wire fraud, RICO offences, securities fraud, as well as other federal criminal offences. In addition, to come within the scope of section 1956 the relevant transaction must be intended to promote the carrying on of a specified unlawful activity, to effect tax fraud or evasion, to conceal or disguise the nature, location or control of the proceeds of specified unlawful activity or to avoid transaction reporting requirements.

2.19.4 Section 1956 may be extra-territorial in scope. An offence under section 1956 may be committed outside the U S where the act in question is carried out by a U S citizen or, in the case of a non-U.S. citizen, any part of the transaction occurs within the U S (for example, the wire transfer of funds).

2.19.5 Penalties for breach of section 1956 include fines of up to $500,000 or twice the value of the property involved in the transaction, whichever is greater, and imprisonment for up to 20 years, or both.

2.20 Section 1957

2.20.1 Title 18 U.S.C. § 1957 prohibits individuals from knowingly engaging or attempting to engage in a monetary transaction in property worth more than $10,000 that is derived from *specified unlawful activity*. As in section 1956, specified unlawful activity covers a broad range of federal crimes. An offence under section 1957 will be committed where a defendant accepts funds greater than $10,000 which he knows are tainted or where he is wilfully blind to the source of the funds.

2.20.2 Criminal penalties for breaches of section 1957 include fines of up to $500,000 or twice the amount of the criminally derived property involved in a transaction, or both, and imprisonment for up to 10 years, or both.

2.21 The Bank Secrecy Act

2.21.1 The BSA and its implementing regulations impose anti-money laundering obligations on banks, securities brokers and dealers and other financial institutions. Certain financial institutions and their officers, directors, employees and agents are required to file suspicious activity reports ('SARs') to report any suspicious transactions relevant to a possible breach of law or regulation. The circumstances in which SARs must be filed include cases of transactions with a value of $5,000 or more where the institution knows, suspects, or has reason to suspect that the transaction involves funds from illegal activities or that the transaction has no business or apparent lawful purpose and the bank knows of no reasonable explanation for the transaction after examining the available facts.

2.21.2 The obligation to file SARs does not extend to all financial institutions. For example, broker-dealers and commodity trading advisers are not required by law to make SARs although they can do so on a voluntary basis.

2.22 The Patriot Act and the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 (IMLA)

2.22.1 As indicated above, the IMLA amends the scope of existing anti-money laundering legislation. Some of the significant changes are identified below. It extends the range of predicate crimes which give rise to money laundering offences under sections 1956 and 1957. The definition of *specified unlawful activity* has been expanded to include terrorist-related offences such as smuggling or export control violations involving an item controlled on the United States Munitions List, unlawful importation of firearms, firearms trafficking and any felony violation of the Foreign Agents Registration Act of 1938. The IMLA has also extended the jurisdictional scope of predicate offences. They now include offences committed outside the US where the US would be required by treaty to extradite the alleged offender or prosecute him were he found to be within the US.

2.23 Foreign banks

2.23.1 Section 318 of the IMLA amends the definition of *financial institution* in section 1956 to include any foreign bank. Accordingly, the offence under section 1956 may now be committed in relation to financial transactions taking place through a foreign bank.

2.24 Anti-money laundering compliance programmes

2.24.1 The IMLA amends the BSA to require financial institutions to establish anti-money laundering programmes including, at a minimum:

(a) the development of internal policies, procedures, and controls;

(b) the designation of a compliance officer;

(c) an on-going employee training programme; and

(d) an independent audit function to test programmes.

2.24.2 These changes were required to be implemented by 26 April 2002 and regulations will be issued by Treasury Department detailing requirements of such compliance programmes. The move towards the appointment of a money laundering compliance officer has been backed by the US Securities and Exchange Commission (SEC), which has requested broker-dealers and other financial institutions to appoint a compliance officer to communicate suspicions of money laundering.

2.25 Foreign shell banks

2.25.1 US financial institutions are now prohibited from establishing or maintaining correspondent accounts with foreign shell banks that have no physical presence in any country. This provision was effective from 26 December 2001 by which date all such accounts were required to be closed. In addition, US banks are also required to take reasonable steps to ensure that correspondent accounts are not used by intermediaries for foreign shell banks.

2.26 Enhanced due diligence for private banking and correspondent bank accounts

2.26.1 Special due diligence procedures have been imposed for US private banking and correspondent bank accounts involving foreign persons. Institutions are obliged to introduce procedures reasonably designed to detect and report instances of money laundering through such accounts. The minimum that must now be done in the case of a private bank account held by an overseas person is to identify the source of funds as well as the nominal and beneficial owners of the account. Enhanced due diligence requirements are also imposed for accounts held by politically exposed persons, off-shore banks and banks from countries which are of particular money laundering concern.

2.27 Primary money laundering concerns

2.27.1 Under the amendments introduced by the IMLA the Secretary of the Treasury can require *special measures* to be taken where there is a *primary money laundering concern*. The purpose of this is provision to provide flexibility to introduce further regulation where the need arises. The special measures that may be introduced must relate to specified foreign jurisdictions, financial institutions operating outside the US, classes of transactions in or involving a foreign jurisdiction or particular types of accounts. The measure may include additional obligations in relation to the maintenance of transaction records, identification of beneficial owners of US accounts opened or maintained in the U S by foreign persons and the identification of the underlying clients of other institutions holding accounts with a U S bank.

2.28 Provision of information

2.28.1 The IMLA also confers on federal banking agencies additional powers to compel the production of information. A bank must produce requested evidence within 120

hours of receiving a request by an appropriate federal banking agency for information relating to anti-money laundering compliance.

2.29 Suspicious activity reports

2.29.1 As explained above, the obligation to make SARs does not apply to all US financial institutions. The obligation to make SARs will now be extended to SEC registered broker-dealers, and under section 356 of the IMLA the Treasury has the power to prescribe suspicious activity report regulations for futures commission merchants, commodity trading advisors and commodity pool operators.

2.30 Know your customer requirements ('KYC')

2.30.1 Under the IMLA regulations will also be made prescribing minimum KYC standards with which financial institutions will have to comply. These regulations will require financial institutions to implement procedures for verifying the identity of any person seeking to open an account, maintaining records of the information used to verify a person's identity, including name, address, and other identifying information and consulting lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency to determine whether a person seeking to open an account appears on any such list.

2.31 Information sharing

2.31.1 The IMLA also contains provisions to encourage information share in relation to money laundering and terrorist activities. In particular:

(a) regulations will be adopted to encourage regulators and law enforcement authorities to share with financial institutions information regarding individuals, entities, and organisations engaged in terrorist acts or money laundering activities.

(b) financial institutions will be permitted to share information with one another regarding individuals, entities, organisations and countries suspected of possible terrorist or money laundering activities, without liability for disclosure.

(c) international co-operation in investigations of money laundering, financial crimes, and the finances of terrorist groups.

CHAPTER 3

The Law in Context

3.1 How much terrorist financing is done through banks?

3.1.1 It appears that published information and analysis of terrorist financing is currently very scarce. Rueven Paz, the former Academic Director of the International Policy Institute for Counter-Terrorism, said, in October 2000, that there had only been a few academic articles published on the issue.[150] A search of the internet and of a number of on-line academic and business bibliographies illustrates that, despite recent developments, little appears to have changed.

3.2 Typologies of terrorist funding

Typologies of terrorist funding have been issued by the Joint Money Laundering Steering Group[151] and FATF[152].

Joint Money Laundering Steering Group

3.2.1 The December 2001 Guidance Notes contain a section on terrorist financing which is intended to 'help financial institutions to recognise terrorist transactions by identifying some of the most common sources of terrorist funding and business areas which are at high risk.' The sources of terrorist financing are listed as:

- Donations – the Islamic practice of donating a 'zakat', one tenth of one's income, to charity is cited, although, of course such donations will normally have no connection to terrorist funding. It is also suggested that many wealthy Middle Eastern individuals may be making donations which amount to little more than protection money;

---

[150] Reuven Paz, 'Targeting Terrorist Financing in the Middle East', 23 October 2000. www.ict.org.il/articles/articledet.cfm?articleid=137. Paz cites James Adams, 'The Financing of Terror' in P Wilkinson and AM Stewart (eds), *Contemporary Research on Terrorism* (Aberdeen University Press, 1987), John Horgan and Max Taylor, 'Playing the Green Card – Financing the Provisional IRA' in *Terrorism and Political Violence Vol 11, No 2 (summer 1999)* and Richard Labeviere, 'Dollars for Terror: The United States and Islam', (New York, Algora Publishing, 2000).

[151] Joint Money Laundering Steering Group, Guidance Notes for the Financial Sector, December 2001 edition, pp 136-139.

[152] FATF – XII Report on Money Laundering Typologies 2000-2001 (1 February 2001), http://www.fatf-gafi.org/fatdocs_en.htm#Trends.

- Criminality – major sources of income listed are extortion, smuggling, fraud including credit card fraud, charities fraud, thefts and robbery and drug trafficking.

3.2.2 In the case of smuggling, the profits are often channelled by courier to another jurisdiction and enter the banking system by means of short-term shell companies (including Bureaux de Change) that disappear after about three months. There have been cases recently, however, where monies are paid into the banking system along with the normal turnover of legitimate businesses, making detection more difficult.

3.2.3 The Guidance Notes list a number of ways in which bank accounts have been used in terrorist financing:

- **Legitimate accounts:** There are instances where individuals have had a number of accounts with different banks. Accounts with one bank are to be used for domestic purposes, receiving salaries and benefits, while those at another bank are for 'business purposes'. The latter accounts will receive money transfers and cheque payments.
- **Dormant accounts**: Accounts with small balances can be held with a number of banks, with the intention of activating them when funds are required (eg for the purchase of 'terrorist material'). They will then be emptied fairly quickly by a series of cash withdrawals. Dormant accounts have also been used as the basis for obtaining bank loans, not subsequently repaid.
- **Telegraphic transfers**: Certain wire companies are said to be used in preference to others, although the notes do not specify which ones. The key factors appear to be the ease of sending and receiving money, the extent to which documentation is required and the location of the outlet.
- **Money Service Businesses**: Bureaux de change, money changers and other dealers in foreign currency are often a channel for funds, with funds often passing through several jurisdictions before they reach their final destination.

3.2.4 While this information provides some general data on the source of terrorist financing, there is no information on quantum and no detailed examples, apart from those on money laundering in general.

Financial Action Task Force (FATF)

3.2.5 The FATF experts set themselves the task of determining 'whether the distinction between legal and illegal sources of funding has an effect on the ability of countries to use anti-money laundering measures to detect, investigate and prosecute potential terrorist related money laundering.' The major sources of terrorist funding were identified as drug trafficking, extortion and kidnapping, robbery, fraud, gambling, smuggling and trafficking in counterfeit goods, direct sponsorship by certain states, contributions and donations, sale of publications (legal and illegal) and funds derived from legitimate businesses. It was suggested that a decline in direct state sponsorship has led to the increased use of criminal activity as a source of funding and that, in these cases, there was little difference between the methods of terrorists and of organised crime groups.

3.2.6 The report lists three examples. The first is a general example designed to illustrate how regional liberation movements use the same laundering method as traditional criminal groups, using certificates of deposit which are deposited in offshore tax havens, through intermediary companies. The second example is a genuine case where the person who opened the account is unable to provide a plausible explanation for the source of the funds (approximately USD7 million), which are believed to have a terrorist connection. The third example deals with an investigation of a large cigarette smuggling operation, involving a suspected terrorist cell.

3.2.7 The report says that there was a certain amount of disagreement amongst the experts about the extent to which anti-money laundering laws could (or should) play a direct role in the fight against terrorism. Some felt that terrorist-related money laundering is a distinct sub-type of money laundering and should, for this reason, become 'a specific focus of anti-money laundering measures', while others felt that the current money laundering counter-measures on serious crime (including terrorism) were sufficient and that any specific focus on anti-terrorist measures should take place elsewhere.

3.2.8 In respect of contributions and donations, sales of publications and funds derived from legitimate business, the FATF report acknowledges that these activities are more problematic. The fact that it may not be possible to show a connection between these funds and any criminal act which generated them, might make it difficult, in many jurisdictions, to target the funds using anti-money laundering legislation. The

second problem, which the report does not explicitly mention, is that it may be difficult to detect this source of terrorist financing in the first place, particularly using traditional anti-money laundering techniques.

3.2.9 The FATF report also describes a number of alternative remittance systems, including the Black Market Peso Exchange, the Hawali or Hundi system and Chinese and East Asian system. The report notes that it is extremely difficult to trace money flows through these systems or indeed to separate legal from illegal money flows. Suggested solutions included further study of each of the system and their use for money laundering and making the banking service more competitive to reduce the attractiveness of alternative remittance systems as a method for moving legal funds.

Examples

The 11 September 2001 attack

3.2.10 The 11 September attack has enabled the authorities in the United States to examine how a terrorist operation is financed. Dennis M Lormel, Chief of the Financial Crimes Section of the FBI distinguishes between 'Mission Specific' Terrorist Cells and 'Sleeper' Cells[153]. In the case of the September 11 'mission', he gives details of the account profile, transaction profile, international activity and non-financial profile of the hijackers. Many aspects of the profile which emerges could be attributable equally to social groupings and forms of activity that are not of a terrorist nature.

3.2.11 In respect of account profile, for example, the 19 hijackers opened 24 domestic bank accounts at four different banks with deposits averaging between US$3,000 and US$5,000. None of the hijackers had a social security number. They tended to open the accounts in groups of three or four individuals. Addresses were not permanent and changed frequently.

3.2.12 In respect of transaction profile, for example, some accounts would receive and/or send wire transfers of small amounts to foreign countries. Hijackers would make numerous cash withdrawals which would often exceed the limit of the debit card and there were a very high proportion of cash withdrawals as opposed to cheques written. One deposit would be made and the money would trickle out a little at a time, with

[153] Dennis M Lormel, Congressional Statement before the House Committee on Financial Services, Subcommittee on Oversight and Investigations, Washington, 12 February 2002, http://www.fbi.gov/congress02/lormel021202.htm.

account transactions not reflecting normal living expenses for rent, utilities, insurance etc. Transactions were generally below the reporting limit. In respect of non-financial profile, for example, the hijackers were all born in a Middle Eastern country, had poor English, came into the bank in groups, usually with a spokesman and preferred to deal with one person at the bank.

3.2.13 According to Lormel, the Department of Justice and the FBI have established a Financial Review Group (FRG), which is developing a centralised terrorist financial database. He states that 'Anti-terrorism financial investigations represent a comprehensive labour-intensive long-term commitment. It is anticipated that, in order to prepare predictive analysis in support of this effort, tens of millions of documents (bank records, travel records, credit cards and retail receipts etc) will need to be collected, thoroughly analysed, and placed in a central database for relevant financial evidence'. He states that, to date, the FRG has catalogued and reviewed over 321,000 documents and that, therefore, the work is just beginning.

3.2.14 Sleeper cells are an even bigger problem for the authorities as, in these cases, income is often derived from legitimate employment and/or businesses within the country in which the cell is operating. This was, for example, the case with many of the hijackers when they were living in Germany, prior to relocating to the US.

Use of legitimate businesses

3.2.15 The case of bin Laden and his organisation is a good example of how legitimate business can be used as a cover for terrorist organisations and financing. Yael Shahar, a researcher at the International Policy Institute for Counter-Terrorism[154], lists a number of legitimate businesses owned by al-Qaida and states: 'Bin Laden's organisation is believed to have enough cash to sustain a worldwide empire. Al-Qaida has at one time operated ostrich farms and shrimp boats in Kenya, bought tracts of forest in Turkey, engaged in diamond trading in Africa and acquired agricultural holdings in Tajikistan. Many of these minor enterprises – such as the fishing business in Kenya – served as a cover for terrorist operations.'

[154] Yael Shahar,'Tracing Bin Laden's Money: easier said than done', 21 September 2001, http://www.ictorg.il/articles/articledet.cfm/articleid=387.

3.2.16 In one of the few articles to concentrate exclusively on terrorist financing[155], Stefan Leader states that Palestinian terrorist groups were believed to have 'accumulated extensive investment portfolios, including stocks, bonds, real estate holdings and various other instruments believed to be worth billions of dollars. Income from these investments has provided support for terrorist operations for many years and made the Palestinian movement essentially self-supporting'. Leader also notes that the Popular Front for the Liberation of Palestine operated a number of legitimate businesses including a metal works factory in Lebanon.

Donations and charitable organisations

3.2.17 In addition to the well-documented use of Islamic charitable organisations by al-Qaida, Leader notes that at least four terrorist groups, the Provisional IRA, Hezbollah, Hamas and Palestinian Islamic Jihad, have raised substantial sums of money from covert support networks in the United States. The Tamil Tigers are believed to receive as much as USD2 to USD3 million per month from an international network of 650,000 or so Tamils and the Algerian Armed Islamic Group (GIA) is believed to have 'a significant logistical infrastructure' in Western Europe, which provides it with funding.

Quantum of funding for terrorist cells

3.2.18 Both Shahar and Paz note that funding for specific al-Qaida cells has often been minimal, with cells expected to be largely self-sufficient. In the case of a group arrested in Jordan in December 1999, for example, no more than about US$2,000 had been received and the group were planning robberies to fund themselves.

3.2.19 Campaigns by other terrorist organisations have also cost very little to implement. For example, according to Stephen Segaller[156], the IRA bomb attempt on the British Cabinet in 1984 probably cost less than £10,000 to set up, while a detailed breakdown of an earlier bombing campaign showed that bombs were planted in 16 British cities for an overall cost of about £25,000 (including travel, property rental, explosives and weapons). Given the small amounts involved, it is possible for operations to be carried out with funds that are couriered to the destination and with minimal use of bank accounts. Where bank accounts are used, the quantum of the transactions involved will have been unlikely to have drawn attention to them. As the

[155] Stefan Leader, 'Cash for Carnage: funding the modern terrorist', *Jane's Intelligence Review*, 1 May 1998.
[156] Stephen Segaller, *Invisible Armies: Terrorism into the 1990s,* Sphere Books, 1987, p 279.

New York Times noted:[157] 'Terrorists tend to use the banking system to distribute relatively small amounts from large deposits overseas. Banks are geared to monitor accounts for the opposite type of activity, as when drug cartels collect relatively small proceeds from drug sales, disguise the origin of the money and move it into large accounts offshore.'

3.3 Financial Crimes Enforcement Network (FinCEN)

3.3.1 FinCEN issued a bulletin in January 2002[158] illustrated by five cases involving Suspicious Transaction Reports (SARs). The bulletin sought to provide indicators which 'should raise the level of concern about potential terrorist financing or other criminal context'. The indicators, while not in themselves providing conclusive evidence of terrorist activity, were said to add up to suspicious activity. Some of the indicators correlate with indicators of laundering of criminal funds and some are redolent of the profiling of the bank activities of the September 11 hijackers. Examples include:

- Use of a business account to collect and then funnel funds to a small number of foreign beneficiaries, both individual and foreign, in a Persian Gulf state;
- Unusual volume of wire transfer activity in a business account that would not normally generate such high levels;
- Large currency withdrawals from a business account not normally associated with cash transactions;
- Same day transactions at the same depository institutions using different tellers; and
- Involvement of multiple nationals of countries associated with terrorist activity acting on behalf of similar business types.

3.3.2 The FinCEN bulletin can hardly be taken as definitive. Many of the indicators are similar or identical to those used by organised criminal gangs and some of them, on their own, could be consistent with many legitimate business activities. The

[157] Kurt Eichenwald and Joseph Kahn, 'US seeking a stronger role for banks on terrorists' cash', *New York Times*, 19 October 2001.
[158] Financial Crimes Enforcement Network, 'Aspects of Financial Transactions Indicative of Terrorist Funding', available from http:www.treas.gov/fincen.

methodology of extracting indicators from a number of real-life examples, however, seems to be a sound one.

3.4 Conclusion

3.4.1 There seems to be very little published material on the mechanics of terrorist financing. It seems likely that the portion of funding which derives from criminal activities can be pursued under existing money laundering procedures and legislation. More difficult questions arise in respect of how to deal with those funds which do not come from illegal sources and how to detect monies which are being used to fund terrorist cells. In these instances, one has to weigh up what it is reasonable to expect from the banks, in terms of the difficulty of detection.

3.4.2 It may not all be bad news, however. A recent report[159] suggests that a compliance database called World-Check, to which 62 banks have encrypted access, had listed 15 of the 19 September 11 hijackers as terrorist suspects before the attack. The methodology by which they had done this is not known, but it gives some hope that it is perhaps not so easy for such individuals to remain undetected. The absence of any clear typology for the operation of 'terrorist' accounts means that financial institutions (at present at least) rely principally upon information (as to the identity of suspects) given or made available to them from outside sources in order to detect terrorist funding within their accounts. Essentially such information comprises lists the names of known or suspected terrorists/their supporters. The issues surrounding the provision and use of such information is considered in the following two sections.

3.5 Provision of information (domestic)

Introduction

3.5.1 As has been pointed out above, terrorist 'money laundering' differs from money laundering in relation to other forms of criminal activity. All crimes anti-money laundering legislation targets the proceeds of criminal conduct and is dependent upon the commission of a predicate office. Given that under the Terrorism Act 2000

[159] 'British banking database listed 15 of 19 hijackers before 11 September', *The Canadian Press*, 21 February 2002.

'terrorist property' includes property which is likely to be used for the purpose of terrorism (and need not be derived from any underlying criminal activity), identifying 'terrorist property' is significantly more difficult.

3.5.2 Know your customer procedures, including establishing the source of funds and wealth of the customer or prospective customer, are designed in part to establish whether the customer has a legitimate business which has generated the funds that the customer is proposing to pass through or to the relevant institution. The same know your customer procedures, even if properly carried out, will not guarantee the discovery of terrorist property because the source of such property may be legitimate.

3.5.3 As an example, there is evidence to suggest that Islamic charities are a significant source of funding for terrorist activities. Press reports indicate that there are 1500 Islamic Charities in the United States and that in Saudi Arabia $1.6 million is raised daily by such charities. Clearly only a small number of Islamic charities will be engaged in terrorist financing. However, without proper direction it is difficult if not impossible for firms to separate the true charities from those funding terrorist activities. While financial sector firms are clearly willing to assist law enforcement authorities in identifying terrorist funding, given the underlying nature of such activities, firms are dependent on the relevant authorities providing intelligence that will enable them to take appropriate action.

Lists and sources

3.5.4 The sources of information available to firms to enable the identification of individuals and organisations involved in terrorist activities include:

(1) The Bank of England Sanctions Unit Consolidated List of Names. This list contains details of individuals and entities against whom financial sanctions have been applied (pursuant to resolutions of the UN Security Council) and individuals and entities engaged in terrorist financing. The list is accessible on the Bank of England's website and is currently available in pdf, plain text, comma delimited and Microsoft Excel formats.

(2) The United States Office of Foreign Assets Control ('OFAC') list of individuals and entities against whom sanctions have been imposed by the United States government. Although this is not a UK list, given the

international nature of financial services and that many UK firms are subsidiaries or branches of US firms, many firms in the UK refer to the OFAC list.

(3) Press reports. Since 11 September there has been significant press interest in the financing of terrorist activities. Names of individuals or entities involved in such activities are frequently report. Many firms with the necessary resources review press information and refer any names reported as being involved in terrorist financing against their customer records.

(4) Authorities. Investigations into terrorist financing are being carried on by a large number of government bodies and public authorities and not just law enforcement agencies. For example, in the UK the Charities Commission has been investigating the Bin Mahfouz family's alleged links with Usama bin Laden. Notably, however, no list has been published by the FSA.

Resources/tools for monitoring the various sanctions and other lists

3.5.5 The above are examples only; the websites which list terrorist entities are very numerous. Most jurisdictions create and publish their own lists, and indeed entities within jurisdictions (eg US embassies) also do so. The FSA website states that the Bank of England is responsible for issuing lists of terrorist names which are subject to financial sanctions. This is a hybrid version of the OFAC list and those names selected by the UN security council (mainly Taliban government). However, the FSA also directs financial institutions to the FBI list of suspects and to the OFAC website. This illustrates the problems that any institution (either national or international) will encounter when trying to gather information on terrorist entities.

3.5.6 Monitoring the lists, which are often updated, and press and other reports places a demand on resources. A large investment bank with IT, compliance and legal resources will be able to develop software to check information in lists against customer information, to carry on monitoring of publicly available sources and to deal with any issues arising from these monitoring processes. However, for small and medium sized firms it may be difficult to find the additional resources to carry out any systematic monitoring of available information.

3.5.7 The European Banking Federation (EBF) has recently commented upon the practical difficulties faced by financial institutions in this regard. The identification of subjects of European Union regulations, imposing financial sanctions should be more

precise, according to the EBF. The industry body has tabled seven recommendations aiming to improve the implementation of EU sanctions in practice (see below).

3.5.8 The EBF has recommended that lists of targeted persons and organisations should be provided to banks in a form which can be processed electronically without further preparation, for instance in Excel. At present the usual process has been for the lists to be presented either as a fax, in computer txt format, or as a pdf file. This means all the information has to be transferred by hand into databases.

3.5.9 Further, it has stated that... 'very often, the lists provided by the authorities contain very few elements enabling the banks to make such identification. In addition to the full name of the person, including all the first names, lists should at least include the date of birth, at least the year of birth, and the place of birth.' In the absence of such details, simple lists of names generate so many 'false positive' results that they become effectively unmanageable. Furthermore, comparison between the Bank of England, OFAC and other lists reveals anomalies in the spelling and format of names. There appears to be no common standard for presenting names and there are inconsistencies within some of the lists as to the order in which the forenames/surnames are presented. Financial institutions sometimes find it difficult to distinguish the correct name order.

3.5.10 While these comments from the EBF come from the Banking sector, they reflect the position for many institutions in relation to the various sanctions lists. At the most fundamental level, institutions need a single, definitive list of targeted persons, entities, and states to be provided in an electronic form in a way that easily interfaces with the institution's own client database. This should provide information from all the lists that affect UK financial institutions, and should be continually updated by the body tasked with its upkeep. The data could be made available to institutions by the Government direct, or via third party data providers.

3.5.11 At present, for many smaller institutions, keeping up to date with the disparate lists is nothing short of a logistical nightmare. Institutions with a small compliance resource will not be able to check the Bank of England website daily in order to keep track of changes to the various lists, or buy in specialist systems to monitor them. At present, either an institution has a large resource for monitoring developments, and/or its own database of relevant sanctions, or it relies on a third party provider of information such as Complinet's Sanctions and Enforcement website, or it relies on 'hit and miss' notifications from a trade body or regulator (which may only deal with a particular

resolution or directive in any event). Even if an institution does subscribe to an information provider, this does not help in terms of being able to compare the latest sanctions list(s) with its client database. For many institutions, it is a manual process for which there is little resource in terms of time or expense, given the regularity of changes to the lists, particularly in the months since 11 September. As at 4 March 2002, there is one consolidated list of terrorist suspects on the Bank of England website, and several other lists relating to individual countries, made under different UN resolutions or EU directives. Even the Bank of England cannot provide at the present time a single list of all persons, entities and states which are the subject of UK sanctions. Further, it is by no means clear that by monitoring the Bank of England list alone institutions will be complying with the legislative and regulatory initiatives.

3.5.12 Other countries seem more organised with the dissemination of their Government's sanctions lists, and may present valuable exemplars. For example, institutions in the US can buy in from a third party provider an electronic data-feed from the OFAC lists. Against this feed, they can check daily in respect of all new accounts opened the previous day. They can also carry out regular checks to ensure that no new accounts fall through the cracks, and that the full client list is monitored on a regular basis. Updates from OFAC are automatically downloaded into the data-feed. There are other options available allowing institutions to feed into other agencies' lists too and/or to customise their own lists of people they do not want to do business with – these could be people on non-OFAC lists or on overseas lists if these affect the firm. Various US government agencies let institutions know about changes to their lists (for instance OFAC and the FBI). Further they also update the Self-Regulatory Organisations, who in turn tell their members about changes to the lists. Therefore, update information is provided timely and free of charge.

3.5.13 The Bank of England Sanctions Unit has now made available a spreadsheet on its website. The intention is that institutions will be able to download the spreadsheet at times to suit them and compare it against their client lists. The spreadsheet is intended to combine the various sanctions lists into one consolidated list of all UK sanctions. The spreadsheet is intended to be updated automatically. Therefore, regular periodical downloads will pick up any changes since the last check. Alternatively, if the firm is on the Bank's distribution list, downloads can be conducted as a result of update notices being received. However, at present there

remains no central updating service for the industry. The spreadsheet will not include overseas lists affecting UK institutions such as the OFAC list, and will, therefore, be limited in its effectiveness for any institution which also does business in other jurisdictions. There are data managers who can provide a 'watchlist' function (for OFAC, UN and other compliance) as part of their anti-money laundering package (for example STB Systems). However, such systems may only be viable for the multi-jurisdictional or high-risk businesses, again leaving smaller or low risk firms out of the loop.

3.5.14 The recommendations of the EBF are applicable to any institution affected by sanctions lists, given the basic need to know what is on the sanctions lists from time to time, and how the content can be compared quickly and efficiently against their client lists. The full list of recommendations made by the EBF, quoted verbatim, reads as follows:

R1: the need for better identification of persons or organisations targeted by sanctions

R2: need for a clarification of the definition of the freezing of funds.

R3: the need for authorisation of exemptions within three weeks. In particular, collective authorisations for the banks' ordinary management of accounts should be provided for if such management is not explicitly taken into account in the definition of freezing of funds.

R4: the need for a quick unfreezing procedure. In cases of wrongful freezing , an unfreezing authorisation should be granted by EU member state authorities within no more than two working days.

R5: where partial embargos allow to continue to trade with persons or organisations subject to financial sanctions, these partial embargos should at the time allow banks to carry out customary methods of payment related to such trading.

R6: the need for a clarification of the notion of circumvention of offences.

R7: the need for an exemption of liability for banks and their staff.

The recommendations are based on a meeting of experts held by the EBF on 15 October 2001.

Impact of the legal provisions

3.5.15 The FSA have told firms to take a risk based approach to complying with anti-money laundering obligations. However, in order to assess the risk of being involved in terrorist financing firms clearly need proper information on which to make their assessment.

3.5.16 The need for proper guidance and information is emphasised by the fact that section 21A of the Terrorism Act 2001 imposes an objective standard on firms in relation to the reporting of suspicions of terrorist financing. Firms may be guilty of an offence of failing to make a suspicious transaction report when on reasonable grounds they should have known or suspected terrorist financing or money laundering. Given the large quantity of information that is available, there is a real risk that a firm may inadvertently not make a disclosure when acting for a person who has somewhere been publicly linked with terrorist activities. Such a firm may be exposed to the risk of a prosecution on the basis that since information was publicly available the firm should on reasonable grounds have known or suspected that the customer was engaged in unlawful activities.

Conclusions

3.5.17 The above matters illustrate the need for the broader dissemination of information to firms. It is accepted that much of the information relating to the funding of terrorist activities will be sensitive and not suitable for disclosure. However, consideration should be given to whether any additional information can be disclosed.

There should also be a central body in the UK responsible for disseminating information relating to those engaged in terrorist funding. The Bank of England Sanctions Unit plays an important role, however this role is limited since it is focused on banks and also it relates to sanctions rather than information generally in relation to terrorist funding. There is a certainly scope for the FSA to take on a broader role. As the entity that is now responsible for enforcing financial sector firms' compliance with money laundering obligations, the FSA should assist firms in discharging those obligations. The information ought to be disseminated from one definitive source, and ought to be available in a format (or choice of formats) enabling quick, computerised processing.

3.6 Provision of information (international)/international co-ordination

International organisations and customary law

3.6.1 Even before September 11, 2001, but especially after the events of that date, a varied number of inter-governmental institutions have been actively involved with the efforts to curtail terrorism. The attempts to identify and confiscate terrorist funds are central to such efforts. Within the United Nations, four principal organs (ie the Security Council, the General Assembly, the Economic and Social Council and the Secretariat of the Secretary-General) are dealing with terrorist financing in one form or another. Security Council Resolutions bind all member states, in contrast with decisions or other instruments adopted by the other principal organs. It is true, nonetheless, that consistent and widespread consensus over a certain issue within the context of the other principal organs, or indeed in other organizations, may create the potential for the emergence of customary international law, which itself is binding upon all states, even if they have not participated in the formation of the customary norm in question.[160] It has to be recalled that states which have persistently objected to the formation of a rule of customary international law are not bound by that rule (persistent objector rule), unless the particular rule is a *jus cogens* one (ie. a peremptory rule of international law), from which no derogation is permitted.[161]

3.6.2 Therefore, the potential for law-making through 'soft law' should not be underestimated, as the General Assembly has in the past produced customary norms, absent treaty or other agreement.[162] This is particularly important since besides the Security Council, the powers of organs of other international organisations are limited, and to the extent that enforcement measures are available, these consist of administrative measures (eg expulsion, condemnation, etc). As regards terrorism, the development of customary law may turn out to be very significant, because states have been unable to reach a uniform definition of the concept of terrorism and related issues (including the harmonization of financial institutions with regard to money laundering and terrorist financing). Hence, the emergence of a new customary norm, and indeed a *jus cogens* norm (if indeed that is the case) will remove the barriers of enforcement, since the said rules will be universally binding.

---

[160] Article 38, 1969 Vienna Convention on the Law of Treaties.

[161] Articles 64, 71, Vienna Convention, id.

[162] See for example, G.A Res. 2526 (1970), the 'Friendly Relations' Declaration, which, *inter alia*, established with clarity the 'non-intervention' rule, enabling it to emerge as a rule of customary law, absent an international treaty to that effect.

International regulation

3.6.3 As already noted, the United Nations has been actively engaged in all aspects of terrorist financing, and most recently the Security Council established a subsidiary organ, the Counter-Terrorism Committee. At a global level, the matter is currently on the agenda of a number of other international organizations, including the International Atomic Energy Agency (IAEA), INTERPOL and EUROPOL, the European Union (EU), the Criminal Justice Branch of the United Nations, the Organisation for Security and Co-Operation in Europe (OSCE), the World Trade Organisation (WTO) and related financial institutions. The common feature in the work of all the aforementioned organizations is a concentration on the use of assets in order to finance illegal activities falling within their ambit. It is difficult for these agencies to effectively co-ordinate for the following reasons:

- Since there does not exist a single definition of terrorism, they have no common working language with which to communicate;
- The Security Council has not made a serious attempt to co-ordinate their activities, and in the absence of central authority such co-ordination seems highly unlikely simply to 'emerge';
- Their scope of terrorist financing does not always coincide, and each organization examines a particular issue depending on its angle of interest;
- Bureaucracy;
- Lack of central database on terrorist financing, even in the absence of central co-ordination

3.6.4 The identification of these lacunae may explain the inefficiency of international organizations in this field and the adoption of *ad hoc* measures after the event. Moreover, it makes the task of national agencies more difficult (and potentially makes their efforts less effective than they could be), since they have to rely on their own resources, when in fact a rich pool of information remains unused.

Remedial measures - a proposed central database

3.6.5 There is an evident disparity between available resources and utilization by competent authorities. Co-ordination can only realistically commence by the establishment of a central database for use of all international organizations and state authorities. States may moreover decide to supplement this database with information obtained by them, although this is an exercise entailing significant national security difficulties, and can only realistically be achieved on an inter-state basis. Nonetheless, information that is deemed not to be classified may be downloaded on this central database, which in all probability will be confidential.

3.6.6 For the purposes of this database an *ad hoc* contextual definition must be adopted. States can adopt an all-inclusive, non-exhaustive list of financial activities they perceive fall within the concept of terrorist financing. This wide definition will enable participating international organizations with a marginal focus on terrorist financing to contribute to its resources, since they can include in the database all relevant information that meets the agreed guidelines, even if it does not *prima facie* seem to be relevant.

3.6.7 Ultimately, the resources contained in this database will be capable of use by national authorities in their pursuit of terrorist related activities. Although at a national level there may, and indeed do, exist a multiplicity of actors involved more or less with terrorist financing, the element of effective enforcement at the national level renders these institutions more competent to make some impact. There is a tendency in all bureaucratic institutions to resist change, initiative and harmonization. This is not true of private institutions, especially financial ones, since their existence generally requires the ability to adapt. The paradox at present is that, based on this assumption, it should be the private actors somehow pushing the government towards the aforementioned changes. If the discussed database were to be established, how is this information to be channelled to the proper authorities? One answer would be through government agencies, but there is a number of them, so which one? Is there a need for a single domestic channelling authority, or should convergence work on the basis of the proposed international organizations model? The problem is that if the database is to be accessed only by governments, then private financial institutions can receive information only through governmental permit. So, irrespective of the internal system established, it is imperative that a government entity exists that will facilitate access to the database by private actors,

and will moreover liaise with them on appropriate measures with regard to suspect accounts, freezing and others.

3.7 Regulatory questions

3.7.1 Analysis of the FSA Money Laundering Sourcebook, particularly Chapter 5 on national and international findings, the press releases that were emanating from the FSA in the aftermath of the attacks on 11 September 2001, and the Financial Services and Markets Act ('the Act'), reveals a gap in regulation insofar as terrorist financing is concerned. There is no specific reference to terrorism in the Sourcebook or the Act. The Act does cover handling the proceeds of crime, but many terrorist groups can be funded by legitimate means, such as donations, as well as by criminal activities.

3.7.2 The FSA has in the press releases 'reminded' all firms of their obligation to check their records for suspects named by US agencies OFAC and the FBI under a presidential order, and it has subsequently issued a release about public and non public lists of suspects that are in circulation. Furthermore the Bank of England has written to all Banks reminding them of long standing sanctions imposed by the UK in respect of al-Quaeda and the Taliban. It was being stressed that this was a legal, rather than a regulatory, obligation under money laundering legislation and the Terrorism Act 2000. However, the legal requirement to freeze suspect accounts of persons subject to sanctions may clash with the legal requirement not to 'tip off' persons reported to NCIS on suspicion of being engaged in criminal activity including terrorism. This conflict requires some guidance and clarification for institutions.

3.7.3 As yet there are no FATF findings or lists in respect of the Special Recommendations. The FSA refers firms to the Bank of England website for the UK Financial Sanctions lists. This is not on the FSA's own website, as provided for in the Sourcebook. What is on the FSA website is the FATF list of non-cooperative countries and territories, in force as at September 2001 (which has not been amended as at 4 March 2002).

3.7.4 The Bank of England has advised The Association of Private Client Investment Managers and Stockbrokers (APCIMS), a trade body in the UK, that the obligations affecting its members after 11 September arose from a Statutory Instrument following on from a UN Security Council Resolution in 2001. They confirmed that

all financial institutions are covered regardless of whether they have ever been recipients of Bank of England Sanctions Notices in the past, and from the date the sanctions became effective in the UK. These events post-dated the making of the text of the FSA Money Laundering Sourcebook. For many institutions that have never been regulated by the Bank of England, this was the first time they were aware of a requirement to check the Bank of England website. It was also a surprise to many UK institutions that they were obliged to check US government lists. Clarification is required as to exactly what legal and regulatory obligations are imposed on UK institutions in relation to various sanctions lists.

3.7.5 The December 2001 Joint Money Laundering Steering Group Guidance Notes incorporate terrorism related requirements, but many firms have yet to implement this version of the Guidance Notes. There is no set time limit for doing so, although the JMLSG indicates that firms will be expected by the FSA to be able to demonstrate that consideration is being given to the new Guidance, and that the firm has a timetable in place for implementing any changes (source: JMLSG website). It should be noted that compliance with the Guidance Notes is not a regulatory safe harbour in any event – the FSA will only have regard to a firm's compliance with the Guidance Notes in assessing whether a firm is in breach of its Rules

3.8 The possible conflict between the Data Protection Act 1998 and money laundering legislation

3.8.1 As mentioned in the previous chapter, a discrete issue that arises out of the anti-terrorism initiatives concerns a potential conflict between the Data Protection Act 1998 and the new legislation. While there has been a conflict between the Money Laundering Regulations 1993 and the data protection legislation for many years under the wording of the old 1984 act, in that the right of a data subject to access to data may clash with the prohibition on 'tipping off'[163], this problem has been flagged up as becoming slightly more acute due to:

(a) the substitution of an objective test for a reasonable suspicion rather than a subjective test. This has come in with the new Anti-terrorism legislation and the Proceeds of Crime Act 2002.

[163] Criminal Justice Act 1988 s 93D.

Section 21A Terrorism Act 2000[164] – Failure to disclose: regulated sector

(1) A person commits an offence if each of the following 3 conditions is satisfied:

(2) The first condition is that he –

(a) Knows or suspects, or

(b) has *reasonable grounds* for knowing or suspecting that another person has committed am offence under any of the sections 15 – 18.....

A similar provision is included in the Proceeds of Crime Act.

3.8.2 This is to be contrasted with the Money Laundering Regulations:
'there are some defences (to the crime of assisting another to retain the proceeds of criminal conduct....etc... another is that a person such as a banker discloses his or her belief to a constable (ie NCIS). *What is required is a subjective suspicion not reasonable grounds to suspect'*.[165]

3.8.3 The text of the current FSA Money Laundering Regulations simply refers, in relation to external reporting to NCIS *'if...the MLRO...suspects that a person has been engaged in money laundering he reports promptly to NCIS*[166]*'*.

(b) The fact that the new Data Protection Act 1998 now extends to records kept manually[167].

(c) It had been argued before that any conflict should be resolved in favour of the Money Laundering Regulations 1993 which were introduced to implement an EU Directive, and therefore should prevail over the Data Protection Act 1984 – a purely domestic measure. The new Data Protection Act has also been brought in to implement a directive so that the issue of supremacy is not so clear cut.

---

[164] Implemented by s 5(2) of the Anti-Terrorism, Crime and Security Act 2001.
[165] Joan Wadsley, 'Banks in a bind: the implications of the money laundering legislation, JIBL 2001, 16(5) 125-130.
[166] Money Laundering Sourcebook 4.3.2R.
[167] Section 2((1) includes within the definition of 'data', data which is recorded as part or with the intention that it should form part of a relevant filing system. According to the Guidance to the Act, data of this type is referred to as 'manual data'. Data Protection Act 1998 Guidance 2.1 at p8.

The conflict

3.8.4 Under the Data Protection Act 1998 section 7 a data subject has rights of access to data about him. The making of a suspicious transaction report to NCIS by a money-laundering officer at a bank/lawyers office etc could constitute such data. If the data is then provided to the data subject the data provider may be guilty of tipping off.

Exemptions to the right to data access

3.8.5 There are however exemptions to the rights of data access under the Data Protection Act 1998 section 29 for data processed for, inter alia, the prevention or detection of crime or the apprehension or prosecution of offenders. To the extent to which the application of those provisions to the data would be likely to prejudice those matters.

3.8.6 This seems *prima facie* to cover the point quite happily, but the Guidance to the Act provides at 5.3.4 that, under the statute, personal data are exempt from the non-disclosure provisions *in any case* where the disclosure is for the crime purpose, and in the case of *Equifax Europe Ltd v the Data Protection Registrar* the Tribunal held that, in the context of the equivalent provisions of the 1984 Act, 'in any case' means 'in any particular case'.

3.8.7 These exemptions only apply when there is *likely prejudice* to the crime purpose, and the Act does not explain the meaning of 'likely to prejudice'. The Guidance then goes on to explain that:

> 'This is not to be regarded as a blanket exemption that would justify the withholding of subject access to whole categories of data where in fact those purposes would not be likely to be prejudiced in the case of all data subjects. It would also not justify the withholding of all the personal data about a particular subject when only part of the personal data would be likely to prejudice those purposes. The Commissioner takes the view that for these exemptions to apply there would have to be a substantial chance rather than a mere risk that in a particular case the purposes would be noticeably damaged. The data controller needs to make a judgement as to whether or not prejudice is likely in relation to the circumstances of each particular case... The Data Controller can only disapply those provisions which would

be likely to prejudice one or more of the crime... purposes and then only to the extent to which prejudice would be likely to result'.

3.8.8 If challenged the data controller must be prepared to defend the decisions to rely on the exemption either to the Commissioner or to the court. It would therefore be advisable for data controller to ensure that each such decision is taken at an appropriately senior level within the data controller's organisation and for the reasons to be documented.

3.8.9 This is the nub of the problem. If it is felt that a blanket rather than case by case exemption should be provided for, eg, terrorism related transaction reports then it would appear that a change in the law is required.

3.8.10 The Treasury has now issued Guidance notes which address these issues. The Guidance emphasises that each request for information must be considered on its merits; that it is impossible to lay down any general rules as to how to deal with such a request, but that an individual STR does not have to show clear evidence of criminal conduct when viewed in isolation, as it might form part of a bigger money laundering picture. It further suggests that if a financial institution is in doubt it should approach NCIS for help.

3.8.11 This Guidance does little to allay the legitimate concerns of financial institutions that complying with these legal requirements in this ad hoc way may prove to be excessively time consuming and expensive and that the law may have to be changed to address the wholly new level of threat that has emerged since 11 September.

3.9 Financial intermediaries

3.9.1 The role of financial intermediaries presents constant problems in relation to traditional money-laundering, and those problems are no less acute when terrorist funding is concerned. We have therefore thought it appropriate to comment on their position in this paper.

3.9.2 In 2000 NCIS received 18,408 suspicious transaction reports (STRs); this represented a 27% increase on the previous year. Reports for October 2001 alone are 4,387 (almost four times as many as in October 2000). Out of 575 registered banks, only 170 institutions made any suspicious transaction reports during 2000. This means that less than 30% of banks reported to the Economic Crime Unit during the

period. When the figures for year 2000 STRs are broken down by sector, there is a significant disparity between banks versus solicitors and accountants:

Accountants	0.42%
Solicitors	1.35%
Banks	62.65%

3.9.3 NCIS have reported in press release 27/01 that 'Solicitors and accountants continue to give concern with very few reports being made, despite their relative attractiveness to launderers.' In many cases solicitors are essential in the initial placement and subsequent movement of criminal funds, often through the use of client accounts. As with solicitors, the professional status and expertise of accountants makes them attractive to money launderers, particularly in the more complex laundering cases.

3.9.4 Institutions that comply readily with the legislation and regulations tend to disclose transactions where they suspect non-terrorism/drugs crimes as well as terrorism/drugs trafficking. The Proceeds of Crime Act formally extends the disclosure regime to all crimes and introduce an objective test for disclosure for the regulated sectors.

3.9.5 NCIS expressed concern in press release 27/01 that some of the financial institutions and sectors lack sufficient adherence to the regulations and disclosure obligations, and may not have adequate training provisions and reporting systems in place, leaving themselves vulnerable to laundering attempts. Bureaux de change accounted for 11.71% of disclosures to NCIS in 2000. HM Customs and Excise now have powers of inspection and regulation of bureaux de change, cheque cashiers and money transmission agents under the new Money Laundering Regulations 2001. This is likely to lead to greater compliance with the regulations.

3.9.6 The Joint Money Laundering Steering Group is made up of the leading UK Trade Associations of the financial services industry. The scope of the Guidance Notes produced by the JMSLG covers all financial sector firms including intermediaries. However, where separate guidance is issued for accountants and lawyers by the appropriate regulatory bodies, these will clearly prevail. The Law Society and the Institute of Chartered Accountants are not members of the Joint Money Laundering Steering Group.

The position of solicitors and accountants is as follows:

Solicitors

3.9.7 Present position:

- The Money Laundering Regulations currently apply primarily to firms conducting 'relevant financial business', eg regulated activities.
- Most firms are not required to have an MLRO, but guidance issued by the Law Society in February 2002 now recommends that all firms, whether required to do so or not, appoint an MLRO.
- The Law Society recognises solicitors' responsibilities as gatekeepers, but appreciates also the importance of concerns about client confidentiality and access to legal advice. There is a desire to protect the 'special role of solicitors as trusted legal advisers'.

3.9.8 Recent changes and changes in the pipeline:

- The Proceeds of Crime Act 2002 increases the responsibilities and exposure of solicitors. In particular it is anticipated that they will be obliged to report when they suspect money is the proceeds of crime, rather than only the proceeds of drug trafficking or terrorism as at present. The objective (negligence) test will also be applied to this legislation, where solicitors conduct regulated activities.
- The Second European Money Laundering Directive, once fully enacted into UK legislation will extend the reporting regime into most areas of solicitors' work. Solicitors will then have to obtain confirmation of their clients' identity and comply with reporting and record keeping regulations.

The combined effect of these changes ought to result in many more disclosures from solicitors, provided that there are adequate inspection and enforcement arrangements.

Accountants

3.9.9 The Institute of Chartered Accountants has adopted a similar stance to that adopted by the Law Society. It has difficulty reconciling the requirements with professional confidentiality. Firms that conduct relevant financial business have a legal obligation to comply with the money laundering regulations. The Institute of Chartered

Accountants has issued its own 'Money Laundering Guidance Notes for Chartered Accountants'. The Proceeds of Crime Act 2002 and the Second European Money Laundering Directive will extend the scope of the existing regulations and ought to result in increased levels of reporting, subject to adequate inspection and enforcement.

3.9.10 Within their response to the FSA Consultation Paper CP46 the Institute of Chartered Accountants stated: 'In the meantime, the FSA should remain aware that there are frequently good professionally sound reasons why chartered accountants do not necessarily report the laundering of the proceeds of all crimes, outside their provision of investment business and that a failure to do so does not reflect on their probity'.

3.9.11 The above quotation demonstrates a surprising view in the current environment and highlights a very different approach to that adopted by the bankers governed by JMLSG Guidelines, who are more inclined override the professional duty of secrecy and report money laundering even when the crime is not thought to be drug/terrorist related.

3.10 Conclusion

3.10.1 In view of the money laundering/terrorist fund 'laundering' risks associated with solicitors and accountants, we believe that they should be regulated to the same extent as financial institutions, although of course the fundamentally different nature of their professions from the financial services industry will dictate differences in the regulatory regime applied to them. The combined effect of legislation in the pipeline will be to considerably extend the obligations upon solicitors and accountants, but there will also need to be a credible enforcement regime, with commitment from the professional bodies involved to ensure that these obligations are adhered to. At present it is not clear that such a regime will exist.

3.11 The Wolfsberg Principles

3.11.1 A number of the practical issues and difficulties canvassed above have been addressed by a group of banks, which has produced a set of principles designed to assist anti-money laundering and anti-terrorism initiatives. The principles are illuminating, and are summarised below.

3.11.2 On 30 October 2000, 11 of the world's largest banks agreed on a set anti-money-laundering guidelines which could be applied to international private banks. The original participating institutions were ABN AMRO, Barclays Bank, Banco Santander Central Hispano SA, The Chase Manhattan Private Bank, Citibank NA, Credit Suisse Group, Deutsche Bank AG, HSBC, JP Morgan, Société Générale, and UBS AG. Since then Goldman Sachs and Bank of Tokyo-Mitsubishi have also joined.

3.11.3 The guidelines state that: 'Bank policy will be to prevent the use of its world-wide operations for criminal purposes. The bank will endeavour to accept only those clients whose source of wealth and funds can be reasonably established to be legitimate.' Obviously the principles were formulated before the events of 11 September, and so did not take into account the implications of money-laundering in relation to terrorist financing. As a result the group met again in January 2002 to update the Principles to include comment on the role of financial institutions in the fight against terrorism.

3.11.4 The new statement (available at www.wolfsberg-principles.com) begins by explaining the new challenges of the financing of terrorism, since the funds do not necessarily derive from criminal activity. It goes on to say that global co-operation is required between the banks and governments if the fight against terrorist financing is to be successful. The subject is then addressed in six main areas:

Role of financial institutions

3.11.5 This looks at how financial institutions can help governments in the fight against terrorism. In particular they should seek to 'prevent terrorist organizations from accessing their financial services, assist governments in their efforts to detect suspected terrorist financing and promptly respond to governmental enquiries.'

Rights of the Individual

3.11.6 The Wolfsberg Group recognises that any actions/investigations taken should be on a non-discriminatory basis and adhere to the rights of individuals.

Know your customer

3.11.7 Here the group identifies the importance of traditional 'KYC' policies in relation to the fight against terrorism. Specifically Wolfsberg is committed to:

- Devising procedures to identify whether a prospective or existing client is on any list of terrorists/individuals supporting terrorist activities issued by a regulatory authority.
- Reporting to the relevant authority any possible matches in line with current laws on the disclosure of customer information.
- Looking at ways of improving information exchange between governmental agencies within and between jurisdictions
- Improving the ways customer information is stored to make cross referencing of terrorist lists easier.

High risk sectors and activities

3.11.8 This looks at businesses which are considered to be 'high risk' in relation to the financing of terrorism, with Wolfsberg stating that enhanced due diligence procedures should be put in place on acceptance of business from such entities. In particular Wolfsberg identifies 'remittance businesses, exchange houses, casas de cambio, bureaux de change and money transfer agents' as such 'high risk' entities.

Monitoring

3.11.9 Wolfsberg understands the problems in identifying those financial transactions which are linked to the financing of terrorism, and is committed to the continued use of monitoring procedures to identify unusual or suspicious transactions. In addition they highlight four main areas:

- Heightened scrutiny in relation to customers involved in sectors mentioned as 'high risk'.
- Monitoring account and transactional activity against lists of suspected terrorists/individuals supporting terrorist activities.
- Working with governments and agencies to recognise patterns and trends identified as related to the financing of terrorism.
- Considering the modification of existing monitoring procedures to assist in the identification of such trends.

Need for enhanced global co-operation

3.11.10 In summary, Wolfsberg states its commitment to continued co-operation with law enforcement and government agencies in the fight against terrorism. In particular it identifies eight main areas for discussion with the relevant agencies in order to improve the contribution of financial institutions:

- Global co-ordination of the issuing of official lists of suspected terrorists and terrorist organisations by in each jurisdiction.
- The inclusion of details and information on official lists to help in the identification of named entities in the financial institution's customer base. For instance: date of birth; place of birth; passport/id number; in the case of corporations; place of establishment; details of principals; if possible reason for inclusion on list.
- Providing prompt feedback to institutions on reports made following circulation of such lists.
- The provision of meaningful information in relation to patterns, techniques and mechanisms used in the financing of terrorism to assist with monitoring procedures.
- The provision of meaningful information about corporate and other types of vehicles used to facilitate terrorist financing.
- The development of guidelines on appropriate levels of heightened scrutiny in relation to sectors or activities identified by competent authorities as being widely used for terrorist financing.
- The development by governments and clearing agencies of uniform global formats for funds transfers that require information which may assist their efforts to prevent and detect the financing of terrorism.

Wolfsberg ensures that national legislation:

- Permits financial institutions to maintain information derived from official lists within their own databases and to share such information within their own groups.
- Affords financial institutions protection from civil liability for relying on such lists.

- Permits financial institutions to report unusual or suspicious transactions that may relate to terrorism to the relevant authorities without breaching any duty of customer confidentiality or privacy legislation.
- Permits the prompt exchange of information between governmental agencies of different nation states.

3.11.11 Obviously Wolfsberg membership is targeted at those larger financial institutions which work on a global basis, but the Wolfsberg Statement on Terrorism, and the Wolfsberg Principles in general, provide a framework for all institutions in the United Kingdom to work from. In particular the statement addresses a number of issues which could help smaller institutions in identifying possible terrorist-associated accounts.

CHAPTER 4

Confidentiality and the Duty of Disclosure

4.1 Introduction

4.1.1 In this chapter we examine the consequences of the disclosure of confidential information in light of the provisions of sections 19 and 20 of the Terrorism Act 2000. We do not examine the Terrorism Act 2000, sections 21A, 21B and 38B here, as we believe that our comments on sections 19 and 20 apply with equal force to these new sections, even though the wording of the new sections differs somewhat from the wording of section 19. Nor do we examine the relevance of the Human Rights Act 1998, the relevance of property rights, or the relevance of professional conduct rules. We address the circumstances to which sections 19 and 20 apply from the point in time when a person forms a belief or suspicion that another person has or may have committed an offence under sections 15 to 18 of the 2000 Act. We are not *concerned with the situation in which a person has failed to form a belief or* suspicion.

4.2 Criminal Law

The Statutory Obligation

4.2.1 Subsections (1) and (2) of section 19 provide that a 'person' commits an offence under the section if that person does not 'disclose' to a 'constable' a 'belief or suspicion' that 'another person' has committed 'an offence' under any of the sections 15 to 18 inclusive.

4.2.2 Section 19(1)(b) requires that the belief or suspicion of a person as to the commission of an offence is to be based on 'information' which 'comes to his attention' in the course of 'a trade, profession, business or employment'.

4.2.3 Subsections (5) and (6) appear to exclude from the ambit of the statutory offence (i) information obtained by a 'professional legal advisor' in 'privileged circumstances', and (ii) a belief or suspicion formed by the professional legal advisor based on such information.

Defences

4.2.4 Subsection (3) of section 19 provides that a person who can prove that he has a 'reasonable excuse' for not complying with section 19(2) has a defence to any charge under the section.

4.2.5 Subsection (4) of section 19 provides a defence to an employee who complies with his employer's 'procedure for the making of disclosures' required by the section.

Penalties

4.2.6 Subsection (8) of section 19 provides that a person who is found guilty on indictment under section 19 can be imprisoned for up to five years and fined, or can suffer up to five years of imprisonment or a fine. The same applies on summary conviction save that the period of imprisonment must not exceed six months and the fine must not exceed the statutory minimum.

4.3 Intermediate law

Permission

4.3.1 Section 20(1) of the Act provides that a person 'may disclose' to a 'constable' his 'suspicion or belief' that any 'money or other property' is, or is derived from 'terrorist property' and also 'any matter' on which 'the' suspicion or belief is based.

4.3.2 Section 20(2) also permits a person to make a disclosure in the circumstances of section 19 of the Act.

4.3.3 Where a person is an employee and his employer has 'a procedure for the making of disclosures' under section 19, the employee may disclose under that procedure anything falling under the provisions of subsection (1) and (2) of section 20.

4.4 Civil law

Common law and equitable duties of confidence

4.4.1 An obligation of confidentiality can arise under the express or implied terms of a contract. An obligation of confidentiality can also arise otherwise than by contract. It is clear from cases such as *Attorney-General v Observer Ltd* [1990] 1 AC 109 and *Attorney-General v Blake* [2001] 1 AC 268 that the English courts will recognise an express contractual term of confidentiality. It is also clear that the English courts will imply, as a matter of general law, a term of confidentiality into contracts of differing kinds. In the case *Weld-Blundell v Stephens* [1919] 1 KB 520 the Court of

Appeal held that there is implied into contracts of employment an obligation not to disclose information of the employer received by the employee in confidence.

4.4.2 In *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461 the Court of Appeal held that there is a duty of confidence owed by a bank to its customer. At 471-2 Bankes LJ thought that it could be 'asserted with confidence that the duty is a legal one arising out of contract'. As to the extent of the information covered by the obligation, Atkin LJ said (at 485) that it:

> 'clearly goes beyond the state of the account, that is, whether there is a debit or a credit balance, and the amount of the balance. It must extend at least to all transactions that go through the account, and to securities, if any, given in respect of the account. ... I further think that the obligation extends to information obtained from other sources than the customer's actual account, if the occasion upon which the information was obtained arose out of the banking relations of the bank and its customers - for example, with a view to assisting the bank in conducting the customer's business, or in coming to decisions as to its treatment of its customers'.

4.4.3 Similarly, in *Ali Shipping Corporation* v *Shipyard Trogir* [1999] 1 WLR 314 the Court of Appeal held (at 326) that an obligation of confidence is implied into an arbitration agreement 'as a matter of law' and that 'the court is propounding a term which arises "as the nature of the contract itself implicitly requires"' (applying the test for implied terms laid down in *Liverpool CC v Irwin* [1977] AC 239, 254 (Lord Wilberforce)).

4.4.4 An obligation of confidentiality can also arise in English law by virtue of the rules of equity. It is clear from cases such as *Seager* v *Copydex Ltd* [1967] 1 WLR 923 that an obligation not to disclose confidential information is imposed by equity. Lord Denning MR said (at 931) that:

> 'The law on this subject does not depend on any implied contract. It depends on the broad principle of equity that he who has received information in confidence shall not take unfair advantage of it. He

must not make use of it to the prejudice of him who gave it without obtaining his consent'

4.4.5 So, in English law there are rules of common law and principles of equity which recognise or imply obligations of confidentiality on a very wide range of persons who are subject to English law. A person claiming that another person has breached his obligation of confidentiality must first prove to the court that there is an obligation owed by the confidant to the confider and then that it has been breached. For example, in *Coco* v *A N Clark (Engineering) Ltd* [1969] 2 RPC 41, Megarry J identified three elements, two of which went to the existence of the equitable obligation of confidentiality and one of which went to breach.
Where the claim is made out, it is then for the other party to defend by proving that he had the right to disclose.

Defences

4.4.6 In the case of employment contracts it was held in *Initial Services Ltd* v *Putterill* [1968] 1 QB 396 that disclosure in breach of an obligation can be defended successfully where the disclosure was in the public interest. In that case the employer and other launderers reached agreement on prices for their services which was not registered under the Restrictive Trade Practices Act 1956. The employee resigned and disclosed the information to the press. The employer took action against the employee for damages. The employee filed a defence alleging the breach of the terms of the Act. The Court of Appeal refused to allow that defence to be struck out because the allegations revealed a potential exception to the obligation of confidentiality which ought to be tried.

4.4.7 At 405 Lord Denning MR said this:

'The exception should extend to crimes, frauds and misdeeds, both those actually committed as well as those in contemplation, provided always - and this is essential - that the disclosure is justified in the public interest. The reason is because "no private obligations can dispense with that universal one which lies on every member of the society to discover every design which may be formed, contrary to the

> laws of the society, to destroy the public welfare"'. see *Annesley v Earl of Anglesea* (1743) LR 5 QB 317, n 17.

4.4.8 The leading case on the duty of confidence owed by a bank to its customer is *Tournier* v *National Provincial and Union Bank of England* [1924] 1 KB 161, where the Court of Appeal held that the obligation of confidentiality is not absolute but qualified. At 473, Bankes LJ classified the qualifications under these four heads:

(a) where disclosure is under compulsion by law;

(b) where there is a duty to the public to disclose;

(c) where the interests of the bank require disclosure;

(d) where disclosure is made by express or implied consent of the customer.

Bankes LJ gave as an example of the first qualification 'the duty to obey an order under the Bankers' Books Evidence Act'. As to the second qualification, Bankes LJ quoted the passage from Lord Finlay's speech in *Weld-Blundell* v *Stephens* [1920] AC 956, 965, 'where he speaks of cases where "danger to the State or public duty may supersede the duty of agent to principal."'

4.4.9 In *Hassneh Insurance Co of Israel* v *Mew* [1993] 2 Lloyd's Reports 243, which was a case on confidentiality in relation to an arbitration agreement, Colman J quoted from the judgments in the *Tournier* case and (at 249) went on to say that the:

> 'essence of the matter is that ... [the bank] ... might need to disclose the information ... as the foundation of a defence to a claim by a third party. ... In my judgment a similar qualification must be implied as a matter of business efficacy in the duty of confidence arising under an agreement to arbitrate'.

4.4.10 This finding was subsequently approved by the Court of Appeal in the leading case on confidentiality in arbitration, *Ali Shipping Corporation* v *Shipyard Trogir*. Here, Potter LJ alluded to *Tournier* case, without expressly identifying it by name, and he identified the following five exceptions to the duty: (i) consent of the other party; (ii) order of the court; (iii) leave of the court; (iv) reasonable necessity; (v) public interest. At 327, Potter LJ said that:

> 'on the analogy of the implied obligation of secrecy between banker and customer, leave will be given in respect of (iv) disclosure when, and to the extent to which, it is reasonably necessary for the protection of the legitimate interests of an arbitrating party. In this context, that means reasonably necessary for the establishment or protection of an arbitrating party's legal rights vis-à-vis a third party in order ... to defend a claim ... brought by the third party'.

4.4.11 Whilst an arbitrator is not a party to the arbitration agreement, he is responsible for ensuring that the agreement is performed. It seems likely, therefore, that the obligation and exceptions implied into the arbitration agreement will apply equally to the arbitrator. The mechanism for this is possibly the agreement between the parties and the arbitrator, or perhaps the professional ethics of the arbitrator.

4.4.12 In the cases of the equitable duty of confidentiality and fiduciary duty, there appears to be no case which directly considers a defence. However, as the confider's rights are equitable, the courts will by apply the 'clean hands' maxim and refuse to let the confider enforce his rights if he has behaved in a manner which is unacceptable to the court, and his behaviour has had 'an immediate and necessary relation to the equity sued for': *Deering* v *Earl of Winchelsea* (1737) 1 Cox Eq 318, 319 (Lord Mansfield).

4.4.13 Furthermore, equity would follow the law in applying the principle in *Gartside* v *Outram* (1856) 26 LJ Ch 113, which was said by Lord Denning MR in *Initial Services Ltd* v *Putterill* [1968] 1 QB 396, 405, to extend to:

> 'any misconduct of such a nature that it ought in the public interest to be disclosed to others. Wood V-C put it in a vivid phrase: "There is no confidence as to the disclosure of iniquity"'.

Defences: statutory interpretation

4.4.14 F A R Bennion, *Statutory Interpretation: A Code* (3rd edn, 1997), 626, writes that it is:

> 'legal policy that law should be altered deliberately rather than casually, and that Parliament should not change either the common

law or statute law by a sidewind, but only by measured and considered provisions. ... The court, when considering, in relation to the facts of the instant case, which of the opposing constructions of the enactment would give effect to the legislative intention, should presume that the legislator intended to observe this principle'.

Similarly, in *National Assistance Board* v *Wilkinson* [1952] 2 QB 648, 661, Devlin J (as he then was) held that it is:

> 'a well-established principle of construction that a statute is not to be taken as effecting a fundamental alteration in the general law unless it uses words that point unmistakably to that conclusion'

Remedies

4.4.15 In his review of remedies in *Attorney-General* v *Blake* [2001] 1 AC 268, 278, Lord Nicholls of Birkenhead said the following:

> 'As with breaches of contract, so with tort, the general principle regarding assessment of damages is that they are compensatory of loss or injury. The general rule is that, in the oft quoted words of Lord Blackburn, the measure of damages is to be, so far as is possible, that amount of money which will put the injured party in the same position he would have been in had he not sustained the wrong: *Livingstone* v *Rawyards Coal Co* (1880) 5 App Cas 25, 39. Damages are measured by the plaintiff's loss, not the defendant's gain.

At 279, Lord Nicholls went on to say that:

> 'Courts of equity went further than the common law courts. In some cases equity required the wrongdoer to yield up all his gains. In respect of certain wrongs which originally or ordinarily were the subject of proceedings in the Court of Chancery, the standard remedies were the injunction and, incidental thereto, an account of profits. These wrongs included ... breach of confidence'.

Foreign element

4.4.16 The English law of confidentiality is reflected in the laws of other common law countries. In non-common law countries it is likely that similar rules - or rules having similar effect - will exist. So, for example, it is well known that in Switzerland there are rules relating to banking secrecy. They are, probably, different in content from those in England but they may have a similar effect on banks, customers and third parties.

4.4.17 Where foreign rights of confidentiality are broken in England, the confider - whether English or foreign - may be able to sue for compensation either in the country in which the foreign right exists or in England. The availability of a remedy for such breaches will depend on the jurisdiction of a court to try the issues, the governing law of the relationship between confider and confidant, and also the existence of any overriding laws of the jurisdiction in which the issues are tried.

4.4.18 Where a disclosure of confidential information is made in compliance with the Act, the question is whether the Act provides any defence in respect of the foreign claim.

4.5 Analysis

The scheme of the Terrorism Act 2000: sections 19 and 20

4.5.1 Section 19 appears to seek to protect the general population against some elements of terrorist activity by requiring persons - in England, Wales, Scotland and Northern Ireland - to divulge relevant information to the UK authorities (via a 'constable') regardless of the civil obligations of persons who divulge the information (the confidants), and at the expense of the person whose information is divulged (the confiders).

4.5.2 In order to avoid imprisonment or a fine or both under the provisions of section 19, a person who gains information in a commercial capacity and which causes that person to form a suspicion or belief as to a terrorist offence under sections 15 to 18 of the Act must disclose to the police the belief or the suspicion, and the supporting information.

4.5.3 It follows that a person with a belief or suspicion within the provisions of section 19 must disclose someone else's information in order to protect himself from prosecution. In this situation the confidant may be seen as obtaining a personal benefit from the use of another person's information.

The relationship between sections 19 and 20

4.5.4 Section 20 appears to be available for persons who clearly are not within the ambit of section 19 because, for example, they are not carrying on a commercial activity. As section 19(1) omits reference to 'vocation', a priest, for example, would not be within the ambit of the section. Someone in this situation can disclose information and the suspicion or belief which arises from that information and will take the benefit of section 20(3). In this situation there is no benefit to the person making the disclosure.

4.5.5 Where someone believes that he may be within the ambit of section 19 but is not sure if that is correct, section 20 may offer a solution. A person in this situation would be able to disclose information and the relevant belief or suspicion under section 20. In this situation there may still be a benefit to the person making the disclosure.

Breach of obligations - defences in English law

4.5.6 Where, pursuant to the obligation or permission in the Act, a person discloses information in breach of contract, or in breach of the equitable obligation of confidentiality, or in breach of fiduciary duty and is sued for compensation, that person will hope for an effective defence.

4.5.7 Three questions arise out of the application of sections 19 and 20 of the Act, which we shall address in turn:

- whether the Act has removed any defences which would otherwise be available;
- whether the Act has provided any additional defences; and
- whether there is any difference between disclosure which is, and disclosure which is not, based on a belief or suspicion which turns out to be well founded?

Removal of defences

4.5.8 In a case which clearly does not fall within the provisions of section 19, section 20(3) does not clearly prevent any common law defence from applying. As a matter of statutory construction the subsection cannot be interpreted as cancelling any common law defence. It is not an express denial of common law defences to a claim for breach of contract, equitable duty of confidentiality or breach of fiduciary duty. The word 'notwithstanding' is directed at the restriction (eg. the obligation of confidentiality) and not at any defence to such restriction.

Additional defences

4.5.9 On the other hand, section 19 does not purport to provide any defence for confidants who disclose confidential information pursuant to that section: the section does not provide a statutory defence to claims for breach of common law and equitable duties. It probably does not need to, given the defences which already exist at common law and in equity, which we have discussed above. As has been seen, where a person is compelled to act in conformity with a statute, the common law and equity allow that as a defence.

4.5.10 Section 20(3) is more difficult. The section provides that the disclosure permitted by subsections (1) and (2) 'shall have effect notwithstanding any restriction on the disclosure of information imposed by statute or otherwise.' If this is a defence to what would otherwise be a breach of a common law or equitable obligation of confidentiality it seems to be an oblique defence. Subsection (3) does not provide specifically that a confidant has a defence; the subsection provides only that no other provision can prevent subsections (1) and (2) from taking effect.

4.5.11 If there were no subsection (3) it might be contended that section 20 is inoperable because a person would not be acting in compliance with a statutory compulsion and, therefore, the recognition at common law and in equity that statutory compulsion is a good defence would not be available. In consequence, subsection (3) makes it clear that voluntary disclosure is to be allowed notwithstanding the lack of defence in the common law and in equity.

4.5.12 Although this is not a clear provision of a defence - the word 'defence' is not used - this is not a case in which statute is attempting to change the common law or equity. There is no general change of law by a 'sidewind' but a specific statutory provision for a specific statutory problem.

4.5.13 It follows that disclosure under section 20 appears to be a defence to any claim for compensation for breach of confidence. Whether a disclosure is under section 19 or section 20, and irrespective of the correct section to be used for any particular situation, there is a defence for the confidant unless, perhaps, the confidant was mistaken as to the nature of the information on which the belief or suspicion was founded.

Unfounded suspicions

4.5.14 Does the fact that a suspicion or belief which turns out later to be unfounded - but which was genuinely held at the time of disclosure - put the confidant into a worse position vis à vis the confider than if the suspicion or belief turns out to be well founded?

4.5.15 A person who discloses information pursuant to section 19 must (a) have formed a belief or suspicion that an offence has already been committed, and (b) that the offence is one which falls within the provisions of sections 15 to 18. If there has been no offence or if there has been an offence but it does not relate to sections 15 to 18, has the confidant disclosed in compliance with the Act?

4.5.16 Section 19(1) does not require certainty as to the commission of an offence or that an offence is within the ambit of sections 15 to 18. Section 19 is clear: if a person has two concurrent beliefs or suspicions then there must be disclosure. The first suspicion is that an offence has been committed; the second suspicion is that the offence is within the ambit of sections 15 to 18. Thus, if there is an error as to the fact of an offence or an error as to the offence being within those sections, the confidant is, nevertheless, acting in compliance with the Act provided that there is a link between the two elements.

4.5.17 If the person forming the belief or suspicion does so where no other person would have done so, has the disclosure been made pursuant to the Act? For example, if a person suspects that an offence has been committed but is irrationally convinced that it must be one of a terrorist nature, but any other person would see that it has nothing to do with terrorism (and it turns out to be unconnected to terrorist activity), has the confidant acted in compliance with the Act or as a result of fear?

4.5.18 Because of the severity of the penalty under section 19(8) it may be the case that commercial entities, lawyers and other professionals will fear for their liberty if they do not disclose every slight suspicion. Although section 19(3) provides a defence to non-disclosure where there is a 'reasonable excuse', it is quite possible that commercial people will not wish to risk using section 19(3) for fear of being wrong in their understanding of what it means in practice. Are they acting under compulsion? It seems so and, therefore, entitled to any statutory and common law defences for breach of confidence.

4.5.19 Section 20 is equally clear, or unclear.

Remedies

4.5.20 As already noted, English law can provide a confidant with compensation where there has been a breach of contract or of equitable obligation. The courts would look to the loss of the confider and not to the gain of the confidant. The fact that the confidant has not gained materially would not matter. There would be a breach but also a defence to relieve the confidant of liability. So the problem seems to be that the confidant will have a defence in England provided he acts in genuine conformity with the Act.

Uncompensated and compensated loss of rights

4.5.21 Sections 19 and 20 refer to disclosure to a 'constable'. It is clear that if the information disclosed is of use to the police in their work against terrorist activity, the information will be used by more than the 'constable' to whom the information is divulged. It will, for example, be included in police databases and made available to a great many persons. There is a very great risk that the information will no longer be within the private domain of the confider and his confidants.

4.5.22 Disclosure may, therefore, amount to the release of confidential information into the public domain for the first time. Such release may be very damaging for the confider whose information has been disclosed. If it is proved that the disclosure is in fact related to terrorist activity then there would be no compensation for the confider from the confidant. There would also be no compensation for the confider from the confidant where the disclosure to the constable turns out to have been an error of fact or judgment, or both. The confider loses in each situation.

4.5.23 The question which follows is how can a confider be recompensed in the situation where he has not committed any offence under the Act and has not acted in such a way as to deny himself any common law or equitable compensation but who, nevertheless, is unable to obtain compensation from the confidant?

4.5.24 One possibility is for the confider to sue the confidant in another country where compliance with a United Kingdom statute may not be grounds for a defence for breach of confidence. That person may seek to obtain compensation of some sort from the confidant in a country other than in the United Kingdom either for breach of English law or breach of a foreign law. In this situation it is the confidant who loses if the foreign claim succeeds.

4.5.25 The kinds of commercial persons who are likely to be involved in transactions carrying the risk of terrorist connection are also likely to be persons with cross-border links. They are likely, therefore, to be at risk from actions in foreign countries for breach of obligations of confidence by the confidant made in England pursuant to the Act.

4.6 Synthesis

4.6.1 What appears from the foregoing statements of the law and analysis is that confiders and confidants are at risk from each other (depending upon the country in which civil action is taken) because of the requirements of the Act. It is not possible to say how many situations will arise under sections 19 and 20, but if investigations reveal that the problem is likely to be widespread or very damaging to the commercial interests of the United Kingdom, or both widespread and very damaging, then something must be done. The sections may be clear in their import for criminal law purposes but they are not entirely clear when civil, commercial considerations are taken into account. Two particular problems are the requirement for disclosure to a constable and the foreign element.

4.6.2 In his speech in *Attorney-General* v *Observer Ltd* [1990] 1 AC 109, 131, Lord Keith suggested the following:

> 'Consideration should be given to the possibility of some international agreement aimed at reducing the risks to collective security involved in the present state of affairs. The First Amendment clearly poses problems in relation to publication in the United States of America, but even there there is the prospect of defence and intelligence secrets receiving some protection in the civil courts, as is shown by the decision of the Supreme Court in *Snepp* v *United States* (1980) 444 US. 507. Some degree of comity and reciprocity in this respect would seem desirable in order to promote the common interests of allied nations.'

If such an agreement were ever forthcoming it may well be kept confidential by the governments concerned. However, the real point is this. If disclosures in compliance with the Act - and similar anti-terrorist measures around the world - are

likely to result in substantial difficulties for commercial entities around the world then consideration should be given to a convention between allied nations for the purpose of preventing civil disputes arising out of the concerted action to deal with the terrorist threat.

4.7 Conclusions

4.7.1 Although the Terrorism Act 2000 may function well as a criminal law statute it does not necessarily function well as a statute dealing with the civil issue of breach of confidentiality.

4.7.2 Notwithstanding the attempts in sections 19 and 20 to provide what are, or appear to be, defences to claims for breach of confidence, commercial entities are at risk.

4.7.3 As the legislation stands at present, there will be disputes where a confidant discloses confidential information where there is in fact no offence at all. It is these disputes which should be prevented from arising. One answer to this problem would be an amendment - whether in compliance with a convention or not – so that disclosures of the confidential material do not amount to disclosure for civil law purposes.

CHAPTER 5

Knowledge and Suspicion under the Terrorism Act

5.1 Introduction

5.1.1 The Anti-terrorism, Crime and Security Act 2001 by Schedule 2, Part 3 amends the Terrorism Act 2000 and inserts a new section 21A into the 2000 Act, as follows:

> (1) A person commits an offence if each of the following three conditions is satisfied.
>
> (2) The first condition is that he -
>
> (a) knows or suspects, or
>
> (b) has reasonable grounds for knowing or suspecting,
>
> that another person has committed an offence under any of sections 15 to 18 [ie of the 2000 Act].
>
> (3) The second condition is that the information or other matter -
>
> (a) on which his knowledge or suspicion is based, or
>
> (b) which gives reasonable grounds for such knowledge or suspicion,
>
> came to him in the course of a business in the regulated sector.
>
> (4) The third condition is that he does not disclose the information or other matter to a constable or a nominated officer as soon as is practicable after it comes to him.

5.1.2 The intention of the new section is clearly to impose an obligation of disclosure upon a person who, *in the course of his business in the regulated sector*, knows or suspects *or has reasonable grounds for knowing or suspecting* that another person has committed an offence under any of ss 15-19 of the 2000 Act. The obligation represents a further statutory inroad into the (qualified) duty of confidentiality owed by a bank to its customer and is an illustration of the conflict that can arise between the competing public interest in the suppression of crime and private rights (a tension that is touched upon by Lord Woolf in his judgment in *C v S* [1999] 1 WLR 1551, 1555). Disclosure under compulsion of law is one of the exceptions to the duty of confidence identified in *Tournier* v *National Provincial and Union Bank of England* [1924] 1KB 461, as has been discussed in the previous chapter.

5.1.3 The regulated sector is identified in Schedule 3A, Part 1 of the 2001 Act. The new section, by introducing an objective test without the requirement for *mens rea*, represents (at least on the face of it) a significant increase in the obligations of disclosure already imposed by section 19 of the Terrorism Act 2000, which requires disclosure by a person who, on information received by him in the course of his trade, profession, business or employment, believes or suspects that another person has committed an offence under sections 15-18.

5.1.4 Once it is established that objective grounds existed for knowing or suspecting an offence under sections 15-18 has been committed, criminal liability is imposed subject only to:

- disclosure to the police (effectively NCIS) as soon as practicable; or
- disclosure to a nominated officer as soon as practicable (in accordance with sub-section 7); or
- having a reasonable excuse for not disclosing the information or other matter; or
- being a legal adviser, and having received the information in circumstances protected by privilege (as further clarified by sub-sec 8). (Privilege is nonetheless not absolute.)

5.1.5 Section 21A(6) of the Terrorism Act 2000 now provides that in deciding whether or not a person has committed an offence the court must consider whether a person followed any relevant guidance which was at the relevant time:

(a) issued by a supervisory authority or any other appropriate body,
(b) approved by the Treasury, and
(c) published in a manner it approved as appropriate in its opinion to bring the guidance to the attention of persons likely to be affected by it.

5.1.6 Whilst disregard of guidance will aggravate an offence under section 21A, it seems reasonably clear that compliance with relevant guidance is not sufficient, in itself, to establish a defence.

5.2 JMLSG Guidance Notes N2

5.2.1 Chapter 3 (in para 3.2.1) referred to the Joint Money Laundering Steering Group, which is an advisory group composed of various UK Trade Associations in the financial services industry. Its aim is to promulgate good practice in countering money laundering and to give practical assistance in interpreting the UK Money Laundering Regulations. This is primarily achieved by the publication of Guidance Notes. Membership and other information about the JMLSG can be obtained from its website (www.jmlsg.org.uk).

5.2.2 The JMLSG has recently promulgated Guidance Notes (N2 version December 2001) updating its February 2001 Guidance Notes. The N2 version relating to Terrorist Financing, under paragraphs 2.32-2.37, has been both drafted and approved by the HM Treasury.

5.2.3 Paragraph 2.33 of the Guidance Notes provides that:

> 'Any individual not complying with the requirement to report where there are reasonable grounds for suspecting terrorist funding faces criminal penalties, and any firm handling such transactions faces major reputational risks'.

5.2.4 Paragraph 2.34 of the Guidance Notes highlights the major difficulty for regulated business in that there are two important differences between the use of terrorist and criminal funds:

- often only small amounts are required to commit a terrorist atrocity; and
- terrorism can be funded from legitimately obtained income and it is not clear to a financial institution at what stage legitimate funds become transformed into terrorist assets.

5.2.5 Paragraph 2.36 of the JMLSG Guidance provides that the risk of terrorist funding entering the financial system may be reduced if firms apply satisfactory anti-money laundering strategies particularly in relation to KYC ('know your client'). (Paragraph 2.35 adverts to the existence of information available to assist in due diligence, including website information such as that provided by the US Treasury Office of Foreign Assets Control (OFAC) which lists assets blocked and transactions

prohibited with persons who commit, threaten to commit or support terrorism.) Assessments should be made of countries with the highest risks and transactions emanating from countries reputed to be a source of terrorist financing should be carefully scrutinised.

5.2.6 Paragraph 2.37 of the Notes provides a series of 'Terrorist Financing Typologies' with the promise of more to be added in the course of 2002 by the FATF.

5.3 Wolfsberg Principles

5.3.1 On 30 October 2000, 11 of the world's largest banks agreed on a set of anti-money-laundering guidelines which could be applied to international private banks. These guidelines, known as the Wolfsberg principles, were updated in January 2002 to include comment on the role of financial institutions in the fight against terrorism. Further information on the Wolfsberg principles is available on-line at: www.wolfsberg-principles.com.

5.3.2 The Wolfsberg Statement on the Suppression of the Financing of Terrorism of January 2002 (Annex B) sets out three key areas of institutional responsibility: (1) KYC, (2) High Risk Sectors and Activities, and (3) Monitoring. The Statement emphasised the requirement for Enhanced Global Co-operation in eight specific areas.

5.3.3 The Statement recommends that national legislation should:

- permit financial institutions to maintain information derived from official lists provided by competent authorities (such as OFAC) within their own databases and to share that information within their own groups;
- afford financial institutions protection from civil liability for relying upon official lists;
- permit the reporting of unusual or suspicious transactions without breaching confidentiality or privacy obligations; and
- permit the prompt exchange of information between governmental agencies of different states.

5.4 The institutional dilemma

5.4.1 The questions which most obviously arise for institutions confronted with section 21A are:

- what to do when they have actual knowledge or suspicion that an offence under sections 15-18 has been committed;
- what protection is provided against civil liability; and
- when may an offence be committed whether or not there was actual knowledge or suspicion that an offence under sections 15-18 has been committed?

5.4.2 There are two main ways in which institutions might suspect, or have reasonable grounds for suspecting, that an offence under ss 15-18 of the Terrorism Act had been committed:

- through internal procedures such as account/transactional monitoring and such like; and
- by notification from an external source through, for example, being alerted by NCIS or other governmental agency.

5.4.3 Criminal liability is imposed by section 21A (and thus the duty to notify to notify arises) in two circumstances:

- when the institution *has knowledge or suspicion* that an offence under sections 15-18 has been committed; and
- when there are *reasonable grounds for knowing or suspecting* that such an offence has been committed, whether or not there is actual knowledge or suspicion.

5.4.4 The obligation in relation to actual knowledge or suspicion follows closely the provision under section 52 of the Drug Trafficking Act 1994, which made it an offence for a person not to disclose to a constable as soon as reasonably practicable his knowledge or suspicion that a person was engaged in drug money laundering where the information or other matter came to his attention in the course of his trade, profession, business or employment. There must be material upon which knowledge or suspicion is, or could be, based. This is clear from the second condition under s 21B of the Terrorism Act, which provides protection against liability for disclosure that might otherwise follow where the 'information or other material' causes the

discloser to know or suspect or gives him reasonable grounds for knowing or suspecting that an offence has been committed.

5.4.5 Section 21B provides protection to the discloser where three conditions are fulfilled:

(1) A disclosure which satisfies the following three conditions is not to be taken to breach any restriction on the disclosure of information (however imposed).

(2) 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.

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

(a) causes the discloser to know or suspect, or

(b) gives him reasonable grounds for knowing or suspecting, that another person has committed an offence under any of sections 15 to 18.

(4) The third 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.

5.4.6 The protection afforded by section 21B is therefore limited. It does not appear to protect the bank other than from liability in relation to *disclosure* to a third party. It is thus a statutory provision that reflects the common law exception to the duty of confidence owed by a bank to its customer: disclosure by compulsion of law. It does not appear to protect against civil liability generally. In particular it does not protect from the consequences of stopping a transaction or freezing assets. In contrast with money laundering, where there is an obvious interest in stopping payments being made, in the terrorist context the immediate interest of NCIS and the intelligence services will be in identifying the source and destination of funds. In the first instance it is perhaps unlikely that the bank will be required to freeze an account. But this is by no means necessarily the case, and the bank itself may wish in any case to freeze the account in order to avoid being fixed with civil liability in subsequent proceedings by a third party for knowing receipt of trust property or dishonest assistance in a breach of trust, as in *Bank of Scotland* v *A Ltd* [2001] 1 WLR 751.

5.4.7 In the *Bank of Scotland* case it was accepted that the bank was genuinely concerned that if it made payments it might be held liable as a dishonest assistant in a breach of trust. The bank's suspicion was nevertheless subsequently found to be unfounded.

The problem facing the bank was that if the account was frozen that might have amounted to the offence of 'tipping-off' under s 93D of the Criminal Justice Act 1988. Despite it not being questioned that the bank was genuinely suspicious, Laddie J at first instance (discharging the order) was critical of the bank and pointed out that without dishonesty there can be no liability as a dishonest assistant, and that there was no evidence of the actual or suspected wrongdoing before the court and upon which the court could have granted the injunction. Mere suspicion without evidence was not enough. The Court of Appeal agreed with Laddie J that the injunction should never have been granted.

5.4.8 What is reasonably clear from the *Bank of Scotland* case is that:

- in cases of genuine difficulty the institution may seek the guidance of the court by way of a declaration under CPR Part 25.1(1)(b);
- where the assistance of the court is sought it is virtually inconceivable that an institution should subsequently held to have acted dishonestly;
- the institution should seek to co-operate with authorities and the investigating authority is the appropriate respondent to any application (in the Bank of Scotland case this was the SFO, in circumstances involving terrorism it may well be the DPP); and
- in the ordinary case where an application is made to the court by an institution, unless the investigating/prosecuting authority acts unreasonably each party will bear its own costs.

5.4.9 It remains something of a paradox that there is a requirement for actual dishonesty for a person to be fixed with civil liability as a dishonest assistant in a breach of trust, whereas there is criminal liability for a failure (without reasonable excuse) to make disclosure where there are reasonable grounds for knowing or suspecting that an offence has been committed under sections 15-18, *whether or not there is actual knowledge or suspicion, still less a dishonest state of mind.* The difference is clearly explicable only as a matter of public policy. Knowing what constitutes 'reasonable grounds for suspicion' is thus of critical importance to an institution.

5.4.10 Section 21A is nevertheless not new (in this particular context) in creating a strict liability offence without any requirement for *mens rea* to be proved.

5.4.11 Section 18 of the Terrorism Act 2000 already provided that it was an offence for a person, in any way to enter into or become concerned in an arrangement that facilitates the *retention or control* by or on behalf of another person of terrorist property. In contrast with the money laundering legislation there is no requirement under section 18 of the Terrorism Act to prove *mens rea* (the proof of actual knowledge or suspicion *q.v.* s 50(1) of the Drug Trafficking Act 1994: *R* v *Colle* 95 CrAppR 67). A person's actual state of mind is therefore strictly irrelevant. It is nevertheless a defence under sub-section 18(2) for a person charged to prove that he did not know and *had no reasonable cause to suspect* that the arrangement related to terrorist property. There is nothing to suggest that the evidential burden under sub-section 18(2) is other than the balance of probabilities in line with the evidential burden upon a defendant for the analogous defence under the Drug Trafficking Act 1994, s 50: *R* v *Butt* [1999] Crim LR 414.

5.4.12 By section 49 of the Drug Trafficking Act 1994 a person committed an offence 'if knowing or *having reasonable grounds to suspect* that any property is, or in whole or in part directly or indirectly represents another person's proceeds of drug trafficking, he (a) conceals or disguises that property or (b) converts or transfers that property or removes it from the jurisdiction for the purpose of assisting any person to avoid prosecution for a drug trafficking offence or the making or enforcement of a confiscation order.'

5.4.13 Section 93C of the Criminal Justice Act 1988 (by amendment under s 31 of the 1993 Act) followed s 49 of the Drug Trafficking Act and references to 'drug trafficking' were replaced by references to 'criminal conduct' and the reference to 'prosecution for a drug trafficking offence' was replaced by a reference to 'prosecution for an offence to which this Part of this Act applies'.

5.5 Reasonable grounds for suspicion

5.5.1 The concept of 'reasonable grounds for suspecting' is not without difficulty. Circumstances that might provide grounds for suspicion may vary widely from, at one end of the spectrum, those which would not be noticed save by someone with special knowledge or of a particularly suspicious disposition, to circumstances that everyone, save the most morally obtuse or willfully blind, would recognize as suspicious. Interposed is the objective hypothetical reasonable person in the position of the accused, diligent and careful, but not overly suspicious and with the same

information and material available to him. In a different context reasonable grounds for suspicion have been held to be an objective test as to what a reasonable person, knowing the law and told of the facts would believe in the circumstances.

5.5.2 The relevant knowledge or suspicion is that an offence under sections 15-18 has been committed. It is not suspicion of *any* wrongdoing. Hence it appears that a defendant who has some suspicion of general, unspecific, wrongdoing is not required to disclose this fact by s 21A. This rule may be compared with several cases on liability for dishonest assistance in breach of trust. In *Grupo Torras* v *Al Sabah* [2001] Lloyd's Rep Bank 36, the Court of Appeal endorsed Rimer J's view in *Brink's Mat Ltd* v *Abu Saleh* [1996] CLC 133 (in each case expressed *obiter*) that without knowledge of the breach of trust in which a person was assisting, a person cannot be liable as a dishonest assistant, because he cannot have been relevantly dishonest. However, it is hard to agree that this view is really to be preferred to Millett J's contrary opinion in *Agip (Africa) Ltd* v *Jackson* [1990] Ch 265, that a person acts dishonestly if he handles funds which he knows to have a tainted source, regardless of whether he knows precisely what legal wrong was committed by the person who passed them to him - and there is nothing in the recent House of Lords decision in *Twinsectra Ltd* v *Yardley* [2002] UKHL 12 to alter this conclusion.

5.6 Corporate Liability

5.6.1 The leading case on the question when it is appropriate to fix a corporate body with criminal or civil liabilities is *Meridian Global Funds Management Asia Ltd* v *Securities Commission* [1995] 2 AC 500, the 'essential point' of which was recently summarized by Robert Walker LJ in *National Union of Rail, Maritime and Transport Workers* v *London Underground Ltd* [2001] ICR 647 as follows:

> 'in determining the mental state of an artificial person (when some statutory rule requires that rather fictional exercise to be carried out) it may be necessary to look, not only at the body's formal constitution, but also at the way it actually organises its activities, and at the scope and purpose of the statutory rule'.

5.6.2 Applying this test to s 21A, we might say rather crudely that the purpose of the section is to fix financial institutions, as well as their employees, with liability for

non-disclosure, with a view to making banks police the activities of their customers in order to make life more difficult for terrorists. Some further light is also thrown on the question of how this may work out in practice by *Tesco Supermarkets Ltd* v *Nattrass* [1972] AC 153 and *Re Supply of Ready Mixed Concrete No 2* [1994] 3 WLR 1249, in both of which it was recognised that the intention of a statute may be to impose upon an employer strict criminal liability for the acts of an employee within the course of his employment:

> 'even where this is not explicitly provided for, and notwithstanding that the employer does not know of, and may indeed have prohibited, the acts in question'.

5.6.3 In the *Tesco* case (at 194) Lord Diplock added the qualification that the rational and moral justification for imposing liability did not extend to:

> 'penalising an employer or principal who has done everything that he can reasonably be expected to do by supervision or inspection, by improvement of his business methods or by exhorting those whom he may be expected to control or influence to prevent the commission of the offence'.

5.6.4 However, in the *Ready Mixed Concrete* case, Lord Nolan observed that once the proscribed act has been established so as to constitute the offence, the actual state of the employer's knowledge is only relevant in mitigation. At 1264 he considered that:

> 'There are, of course, many areas of business life, not only in the consumer protection field, where it has become necessary for employers to devise strict compliance procedures. If the burden is in fact intolerable then the remedy must be for Parliament to introduce a statutory defence for those who can show that they have taken all reasonable preventive measures.'

5.7 Defences

5.7.1 The statutory defences to non-disclosure under s 21A are limited: (1) 'a reasonable excuse for not disclosing the information'; or alternatively, (2) legal privilege. A qualified defence is provided under 21A(6). That it is qualified is clear from the fact that the court must consider, in deciding whether a person committed an offence under s 21A, whether the person followed relevant guidance. The following of guidance is not however enough (otherwise this would fall under sub-section (5): 'a person *does not commit an offence* if ...'. It appears that section 21A(6) will be used to establish to determine both whether the employer has done 'everything that he can reasonably be expected to do' in Lord Diplock's formulation and whether the relevant procedures were in fact followed by the employee.

5.7.2 The safest course for institutions is to:

- follow, and enforce amongst staff, clear and thorough KYC/reporting procedures;
- follow guidance issued by bodies such as JMSLG/Treasury/FATF; and
- ensure that staff are aware of 'terrorist typologies'.

5.7.3 But what of a customer whose name appears upon, for example, lists of proscribed transactions published by the US Treasury Office of Foreign Assets Control (OFAC)? Is the publication of a person's name on such a list sufficient to give rise to suspicion for the purposes of s 21A, whether or not the customer's name is actually spotted by the institution concerned? It might be said that at best such publication is evidence only that someone else considers that the person in question commits or threatens to commit or to support terrorism. But publication, and knowledge of publication of a person's name on such a list, might be expected to lead a careful person to monitor the account. The Wolfsberg Statement makes it clear that the participating institutions consider that the publication of lists of names, without more, to be insufficient material to enable an institution to provide meaningful assistance to the public authorities.

5.7.4 The acute difficulty for institutions to which section 21A applies is that which is identified by both JMLSG and the Wolfsberg Statement, namely the interpretation of information. Commonly it will be impossible for an institution to assess whether or not an offence under sections 15-18 has been committed.

5.7.5 The purpose of section 21A(2) appears to be to deny to terrorists the facilities of the international banking system through the exposure of institutions and their employees to criminal penalties. It is likely that the attainment of this objective will only be achieved if institutions are provided with meaningful and useable information required to enable them to draw conclusions from transactional patterns sufficient to raise reasonable grounds for knowing or suspecting that an offence under ss 15-18 of the Act has been committed.

5.7.6 The Guidance Notes promulgated by the JMLSG and approved by the Treasury set out principles of good industry practice, in particular KYC (paragraph 2.36) and due diligence including checking terrorist listings (paragraph 2.35). It may nonetheless be doubted whether the 'Terrorist Financing Typologies' identified under Appendix B are likely will be sufficient to assist an institution in putting in place procedures necessary to identify a particular transaction or series of transactions as giving rise to reasonable grounds for suspicion that offences under ss 15-18 have been committed.

CHAPTER 6

Forfeiture of Terrorist Property and Tracing

6.1 Introduction

Schedule 1 of the Anti-terrorism, Crime and Security Act 2001

6.1.1 Section 1(1) of the Anti-terrorism, Crime and Security Act 2001 brings into effect Schedule 1, which provides for the seizure, detention, and forfeiture of terrorist cash by authorized officers in civil proceedings before a magistrates' court or (in Scotland) the sheriff.

6.1.2 Terrorist cash is defined in section 1(1) as (a) cash which is intended to be used for the purposes of terrorism, (b) cash which consists of resources of an organization which is a proscribed organization, or (c) cash which is, or represents, property obtained through terrorism.

6.1.3 Schedule 1, para 1, specifies that the schedule applies to terrorist cash, which it defines as either cash which is within section 1(a) or (b), or cash which is 'property earmarked as terrorist property'.

6.1.4 Schedule 1, para 12, essentially provides two definitions of 'property earmarked as terrorist property', viz:

- 'property obtained through terrorism' which is held by the person who obtained the property through terrorism; and
- 'property obtained through terrorism' which is no longer held by the person who obtained the property by terrorism, but which has instead come into the hands of a person into whose hands it may be followed.

6.1.5 Schedule 1, paragraph 16, lists the persons into whose hands the property may not be followed; they include bona fide purchasers for value without notice of the fact that the property is earmarked, and judgment creditors of the person who obtained the property through terrorism.

6.1.6 Schedule 1, paragraph 17, provides that 'property' includes money, all forms of property, real or personal, heritable or moveable, things in action and other intangible and incorporeal property.

The underlying purpose of the seizure, detention, and forfeiture provisions

6.1.7 The underlying purpose of the seizure, detention, and forfeiture provisions contained in Schedule 1 does not appear on the face of the 2001 Act, and this schedule received almost no attention on its way through Parliament. However, it is stated in the Explanatory Notes issued for the Anti-terrorism, Crime and Security Bill 2001 that these measures are intended to 'cut off terrorist funding' (para 3) and to 'prevent terrorists from gaining access to their money' (para 5), and the few remarks on this subject that can be found in Hansard also bear out the view that the underlying purpose of these provisions is to reduce the incidence of terrorism by preventing terrorists from using forfeited assets as a means of financing terrorist activity - i.e. to the extent that MPs considered the matter at all, they envisaged that the forfeiture powers would be used against defendants who would otherwise use the assets in question for terrorist purposes.

6.1.8 So, in his statement to the House of Commons announcing the scope of the Anti-terrorism, Crime and Security Bill 2001, the Home Secretary stated that 'the emergency legislation will build on the provisions of the Proceeds of Crime Bill to deal specifically with terrorist finance through monitoring and freezing the accounts of suspected terrorists' (HC Debs, 15 October 2001, col 923). In the course of the House of Lords debates on the bill, Lord Rooker also stated for the Government that the power to freeze assets contained in the bill 'modernizes an existing power and allows us to counter the risk of assets being used to finance terrorism' (HL Debs, 27 November 2001, col 144), and for the opposition, Lord Kingsland accepted that the power to seek a forfeiture order 'is a valuable weapon in our armoury to defeat terrorism because it is self-evident that, without funding, terrorism cannot flourish' (HL Debs, 28 November 2001, col 301).

6.1.9 It should be noted, however, that Schedule 1 does not merely enable authorized officers to bring forfeiture proceedings against terrorists; it also enables them to bring forfeiture proceedings against any third party recipient of terrorist property who is not a bona fide purchaser for value of the property. To the extent that a third party recipient can be shown to have some guilty knowledge of the tainted source of the property, one might say that such a person might well hand the property over to be used for terrorist purposes at a later time. This suggests that it would be consistent with the objective of preventing the property in question from being used for terrorism, if a forfeiture order were to be made against him.

6.1.10 However, it is far less clear that ordering an innocent, good faith recipient of terrorist cash to forfeit the property would be consistent with this purpose, if he had no intention of doing anything with the property other than using it for his own innocent purposes - which might even be charitable purposes, the pursuit of which would be for the public good. Since no other reason for the forfeiture provisions has ever been articulated by the Government or Parliament, it is therefore mysterious why the 2001 Act should empower authorized officers to seek a forfeiture order against innocent donees, and it is accordingly a matter for regret that the position of third party recipients caught by Schedule 1 of the Anti-terrorism, Crime and Security Act 2001 was never considered in Parliamentary debate. This point was indeed made at the time by Douglas Hogg MP, when he said that:

> 'The plain truth is that, because of the time constraints, we are not going to discuss the substance of [clauses including those giving Customs the power] to go to the magistrates to get a seizure order in respect of 'terrorist cash'. ... From any viewpoint [these] are extremely important obligations and powers that are backed by penal sanctions. Furthermore, they apply to people's property and may also affect the property of innocent third parties. However we are not going to discuss them at all ... . A sunset clause is one way at least of expressing our dismay about the position'.(HC Debs, 21 November 2001, col 357)

6.1.11 The potential impact of forfeiture provisions on innocent third party recipients of tainted money was drawn to the Government's attention by the Charity Commission in its response to the Government's draft Proceeds of Crime Bill in May 2001, in a memorandum which is available on-line at http://www.homeoffice.gov.uk/proceeds/pdfs/charity.pdf. The Charity Commission made a number of comments in this memorandum which are relevant in the present context:

> 'It is proposed that a civil recovery action could not be taken against a person who acquires criminal property for full value, in good faith and without notice of its criminal origins. This would not seem to cover donations to charities (which would not be for 'full value') and we

would suggest that this is extended. There could, for example, be a specified power to take no proceedings if, say, a charity had received and spent a donation subject to its having done so in good faith and so on. It might be, of course, that a charity in these circumstances would want to repay such tainted donations - the nature of some offences might make it particularly keen to do so. But if it could only do so by stopping all of its activities and selling or transferring its property this might well outweigh the benefits of recovery. Particularly if no previous owner could be identified - as would be the case with drug trafficking money, for example.

It would also be possible, of course, for criminals to establish and fund a charity out of their ill-gotten gains. It could, as above, be argued that it might be better to allow the charity to continue, perhaps subject to our using our protective powers to ensure that fit and proper trustees were in place. Again, this would be a particularly strong argument where no owner of the property could be identified.

Generally, therefore, we feel there are circumstances in which it would be harmful to recover assets from charities which, by definition, must be doing work in the public benefit. It seems to us that there should be some discretion for the appropriate authority in cases where the public interest would be better served by allowing a charity to retain the property at issue'.

6.1.12 No such discretion is given to a magistrates' court by the Anti-terrorism, Crime and Security Act 2001, to allow the innocent recipients of terrorist cash to retain the property. As we shall see, though, there is some scope at common law to treat such innocent recipients more kindly than terrorists or guilty recipients of terrorist cash, when the rules governing the following and tracing of assets, forfeiture of profits, and defences, come into play in the context of forfeiture proceedings. Ultimately, however, it is a policy question whether such favour should be shown to innocent recipients, and there is unfortunately nothing in the Act itself or in *Hansard* to help us determine how this policy question should be answered.

Issues arising

6.1.13 It is proposed to comment on three broad issues in this chapter:

- the extent to which the Schedule enables an authorised officer to trace the value inherent in earmarked property through substitutions and mixtures by the person who obtained the property by terrorism, with a view to seizing, detaining, or applying for the forfeiture of property in that person's hands, on the ground that the value inherent in this property represents the traceable proceeds of the value inherent in the earmarked property;
- the extent to which the Schedule enable an authorised officer to follow earmarked property or its traceable proceeds into the hands of a third party recipient who is not protected by paragraph16 because he has not given value in exchange for the property; and then, if necessary, to trace the value inherent in the earmarked property through any mixtures or substitutions in which the innocent volunteer has engaged, with a view to seizing, detaining, or applying for the forfeiture of property in his hands, on the ground that the value inherent in this property represents the traceable proceeds of the value inherent in the earmarked property; and
- the appropriateness of the magistrates' courts as a forum for the determination of forfeiture proceedings under Schedule 1.

6.1.14 In the following discussion, the terms 'following' and 'tracing' are used in the senses advocated in L D Smith, *The Law of Tracing* (1997), and adopted by Lord Millett in *Foskett v McKeown* [2001] 1 AC 102, 127. It should also be noted that in *Foskett v McKeown* [2001] 1 AC 102, 113 and 128, Lord Steyn and Lord Millett respectively confirmed that because tracing is simply a process of identifying assets there is nothing inherently legal or equitable about the tracing exercise, and that it follows from this that there is no need for English law to support separate tracing rules at law and in equity. The following discussion will therefore proceed on the basis that there is only one set of tracing rules in English law.

6.2 Tracing the value inherent in earmarked property through substitutions and mixtures by the person who obtained the property by terrorism

Tracing through 'straight substitutions'

6.2.1 Schedule 1, paragraph 13 deals with 'straight substitutions' of earmarked property for other property. It provides that if a person enters a transaction in which he disposes of earmarked property, whether this is the original property obtained through terrorism or its traceable proceeds, and he obtains other property in place of the earmarked property, then this other property represents the earmarked property, and will therefore become earmarked property itself.

6.2.2 This is a simple rule which can be easily applied in simple situations. For example, if X is a person who has obtained £10,000 by terrorism, and he uses the money to buy a car, then the car will 'represent' the £10,000, and so will itself be earmarked property. Another way of expressing this conclusion is to say that paragraph 13 enables an authorized officer to trace the value inherent in the £10,000 into the value inherent in the car, with a view to treating the car as earmarked property.

6.2.3 Although paragraph 13 does not expressly spell this out, it is possible that the rule which the paragraph embodies might also be brought into play in two more complex situations as well. To explain the first of these requires us to describe the concept of 'backwards tracing'; to explain the second requires us to describe the concept of 'reviving subrogation'.

'Backwards tracing'

6.2.4 Let it be supposed that X borrows £10,000 from Y, and uses this money to buy a car, and that X then uses money which he has obtained by terrorism to pay off his debt to Y. In these circumstances, assuming that Y is a bona fide purchaser for value without notice, it might be thought that the terrorist property is effectively dissipated when it is paid to him, and that it does not survive anywhere in a traceable form (under the scheme of Schedule 1, Y is protected as a bona fide purchaser under paragraph 16(1)(b)). However, recent authority indicates that in these circumstances an authorized officer can 'trace backwards' through the payment of the debt with terrorist property into the car which was purchased with the borrowed money, and identify the value inherent in the car as the traceable proceeds of the value inherent in the terrorist property, in order to arrive at the conclusion that the car is earmarked property.

6.2.5 This analysis was first suggested by Lionel Smith in his article 'Tracing into the Payment of a Debt' [1995] CLJ 290, esp pp 292-5, and it can now be found in his

book, *The Law of Tracing* (1997), pp 146-152. It has the judicial support of Dillon LJ in *Bishopsgate Investment Management* v *Homan* [1995] Ch 211, 216-7, approving Vinelott J at 1st instance (although in the same case it was disapproved by Leggatt LJ at 221-2); it was also adopted by Scott V-C in *Foskett* v *McKeown* [1998] Ch 265, 283-4 (not considered on appeal to HL: [2001] 1 AC 102). Scott V-C added that where X is a wrongdoing trustee it is only possible to 'trace backwards' through X's payment of the debt into the asset if it can be shown that it was X's intention at the time of borrowing the money that he would later wrongfully use the trust money to repay the creditor. However, this seems likely to cause all kinds of evidential difficulties, and although possibly relevant to the question whether trust beneficiaries should be allowed to assert a claim to the asset, it should in principle be irrelevant to the separate preliminary process of identifying the asset as the traceable product of trust money. There seems to be no good reason in principle why Scott V-C's suggested limitation should apply in the present context.

'Reviving subrogation'

6.2.6 Let it be supposed that X borrows £100,000 from Y, and to secure his repayment of the loan he mortgages property in his possession to Y. X spends the money on his own purposes and it is now gone. X then uses money which he has obtained by terrorism to pay off his debt to Y, with the result that the mortgage is extinguished. In these circumstances, assuming that Y is a bona fide purchaser for value without notice, then again it might be thought that the terrorist property is dissipated, and does not survive anywhere in a traceable form. However, there is authority for the proposition that in these circumstances, an authorized officer can trace the terrorist property into the extinguished mortgage, and ask the court to put him in the same position as the one which he would have occupied, had the mortgage not been extinguished, but assigned to him instead. That it lies in the court's power to 'revive' the extinguished mortgage by a legal fiction, and allow the authorized officer to be treated as though he were now the mortgagee, was most recently confirmed by the HL in *Banque Financière de la Cité* v *Parc (Battersea) Ltd* [1999] 1 AC 221, esp 236 (Lord Hoffmann).

6.2.7 In the examples of backwards tracing and reviving subrogation presented here, it is given that the debts owed to Y are paid off solely with terrorist property, with the result that they can be understood as examples of 'straight substitutions' of a slightly

complex kind. It should not be forgotten, however, that in practice a person who obtains property by terrorism might first mix the terrorist property with other money of his own before paying Y out of the mixture, in which case the rules governing tracing through mixtures would also have to be brought into play. To these we now turn our attention.

Tracing through mixtures

6.2.8 Schedule 1, paragraph 14 deals with mixtures: it provides that if a person who has obtained property by terrorism mixes this property with other property (whether his own or somebody else's), then 'the portion of the mixed property which is attributable to the property earmarked as terrorist property represents the property obtained through terrorism' (para 14(2)).

6.2.9 This, too, is a rule that can be straightforwardly applied in simple situations. For example, if a person obtains one thousand £50 notes by terrorism and he mixes them with one thousand £50 notes already in his possession, then provided that he does not spend any of the £50 notes, an authorized officer can simply identify half of the two thousand £50 notes as representing the property obtained through terrorism. However, it will be appreciated that matters can quickly become more complicated than this, and there are two situations which might arise in practice, which are not expressly dealt with in the Schedule, but which merit our attention, namely: (a) the situation where a person mixes property obtained by terrorism with other property and then makes gains and losses out of the mixture; and (b) the situation where a person borrows money on the strength of his possession of terrorist property, mixes this money with property obtained by terrorism, and buys an asset with the mixed funds that increases in value.

Gains and losses out of mixed funds

6.2.10 If a person mixes property obtained by terrorism with other property, and then withdraws funds from the mixture and dissipates them, or withdraws funds from the mixture and uses them to purchase new property which either increases or decreases in value, then an authorized officer will need to know whether it is the terrorist property or the other property which has been withdrawn from the mixture, and dissipated or used to purchase the new property. It is provided by Schedule 1, paragraph 15, that 'where a person who has property earmarked as terrorist property

obtains further property consisting of profits accruing in respect of the earmarked property' then 'this further property is to be treated as representing the property obtained through terrorism'. However, this does not resolve the difficulty, since it merely tells us what the consequences will be if new property that has risen in value or generated profits was bought with terrorist property - it does not tell us how to determine whether property withdrawn from a mixture of terrorist property and other property should be regarded as terrorist property in the first place.

6.2.11 The rules governing an analogous question in the law of trusts, where a trustee wrongfully mixes trust money with his own money and then makes withdrawals from the mixture, are predicated on the principle that trustees owe a duty to segregate trust property from their own property, and that they accordingly commit a civil wrong in the event that they mix the two together. Thus, any evidential uncertainty created by the fact that one cannot identify the provenance of withdrawals made from the mixture is produced by the trustee's wrongdoing, and it is a principle of the law of evidence that where evidential uncertainty is created by wrongdoing, evidential presumptions will be made against the wrongdoer. Hence, the rules in *Re Hallett's Estate* (1880) 13 Ch D 695 and *Re Oatway* [1903] 2 Ch 356 dovetail with the rule in *Armory* v *Delamirie* (1722) 1 Str 505 and *Infabrics Ltd* v *Jaytex Ltd* [1985] FSR 75.

6.2.12 Conceivably, it might be thought appropriate for evidential uncertainties to be resolved against a person who mixes property obtained by terrorism with other property in a similar way. However, it might seem rather artificial to say that a person who obtains property by terrorism owes a duty not to mix it with other property, and the principle that evidential uncertainties should be resolved against him might therefore be more soundly and simply based on the need to deter terrorism by making life tough for terrorists.

Borrowing money on the strength of possessing terrorist property

6.2.13 Banks and other lending institutions are likelier to lend money to people who already have some money than they are to lend it to people who have nothing. Hence, for example, a person who has obtained £100,000 by terrorism might be able to borrow a further £100,000 in order to buy a house against the security of a mortgage on the house, where he would not have been able to borrow anything if he had not been able to present himself to the lender as a good credit risk. If the house then increases in

value, then he might attempt to argue that although half of the increase in value represents property obtained by terrorism (following Sched 1, para 15), the other half does not, because it represents the fruits of the money which he borrowed and promised to repay. However, there is authority for the view that in these circumstances the other half of the increase in value represents property obtained by terrorism as well, because the bank would not have lent the money but for the borrower's possession of the terrorist property: *Paul Davies Pty Ltd* v *Davies* [1983] 1 NSWLR 440 (and cf *Wagstaff* v *Wagstaff* [1992] 1 WLR 320).

6.3 Following earmarked property into the hands of innocent volunteers and tracing through their mixtures and substitutions

We now turn our attention to the position of innocent volunteers who receive property obtained by terrorism without knowing that the property has been obtained by terrorism, but without giving value in exchange for the property. Innocent volunteers in this position do not fall within any of the classes of people listed in Schedule 1, paragraph 16, into whose hands earmarked property may not be followed. Hence, if an authorized officer can identify property in their hands as terrorist property or its traceable proceeds, he can seize it, detain it, or seek an order for its forfeiture.

6.3.1 There are three questions which arise in this connection: (1) if an innocent volunteer uses earmarked property to purchase an asset which rises in value, should he be entitled to argue that if he had known that the source of the earmarked property was tainted he would have used other resources of his own to purchase the asset, suggesting that an authorized officer should not be able to strip him of the asset's increase in value; (2) what rules should govern the situation where an innocent volunteer makes gains and losses out of a mixture of earmarked property and his own property; and (3) should an innocent volunteer be entitled to raise a change of position defence against an authorized officer?

Use of earmarked property when other resources were available

6.3.2 David Hayton has argued that an express trustee who wrongfully uses trust money to purchase an asset which rises in value should not be entitled to say that he could just have easily have bought the asset out of his own resources, so that the increase in value should not be attributable to the trust; but he has also argued that where a

defendant does not know that he is a constructive trustee and has acted in good faith, like the defendants in *Phipps* v *Boardman* [1967] 2 AC 46, for example, then he should be entitled to make this argument: D J Hayton, 'Equity's Identification Rules' in P Birks (ed), *Laundering and Tracing* (1995) 1, pp 11-12. Lord Steyn found this argument attractive in his dissenting speech in *Foskett* v *McKeown* [2001] 1 AC 102, 113, but the majority of their Lordships did not agree that it was applicable on the facts of the case. On the right set of facts, however, it may be that it will be considered appropriate to allow the innocent recipient of earmarked property to make this argument: specifically, where he can show that at the time when he used the earmarked property to purchase a new asset, he had alternative resources at his disposal which he could have used instead, a presumption should be made in his favour that he would have used these alternative resources, because he is an innocent volunteer who acted in good faith. This would lead to the conclusion that the profits should not be treated as the proceeds of earmarked property for the purposes of Schedule 1, paragraph 15.

Gains and losses out of mixtures

6.3.3 It would not be appropriate for evidential presumptions to be made against an innocent volunteer who mixes earmarked property with his own property and then makes gains or losses out of the mixture, because he is not a wrongdoer in the same way that a trustee who mixes trust property with his own property is a wrongdoer, nor is he a wrongdoer in the same way that a person who obtains property by terrorism is a wrongdoer. This leaves us with two possibilities: either evidential presumptions should be made in his favour, so that gains are always attributed to him, and losses to the terrorist property; or gains and losses should be shared pro rata. The latter rule is used where the innocent recipients of wrongfully distributed trust property mix it with their own property and then makes gains and losses out of the mixture, following *Re Diplock* [1948] Ch 465, 533, 534, and 539 (per curiam). However, it is a question that can only be decided by reference to the principles of public policy, which of the two approaches should be adopted in the present context.

6.3.4 A complication in the present law governing the recovery of misappropriated trust assets is that the English courts have adopted a different rule from pro rata sharing of gains and losses out of mixtures, where an innocent volunteer's money is mixed with trust property in a current bank account. In this case, as the Court of Appeal held

most recently in *Barlow Clowes* v *Vaughan* [1992] 4 All ER 22, the basic rule is 'first in, first out' - i.e. the amounts which are first withdrawn from the account are deemed to be the traceable product of the amounts which were first paid in.

6.3.5 The source of this rule is commonly said to be *Clayton's case* (1816) 1 Mer 529, but in fact *Clayton's case* was itself concerned only with a dispute centring on the appropriation of payments as between a bank and its customer, and as a matter of authority it need not have been pressed into service in the present context (for discussion, see L D Smith, *The Law of Tracing* (1997), pp 183-194). Moreover, the rule in *Clayton's case* is predicated on an understanding of the nature of a bank account - that it consists of stacked units of value - that cannot be reconciled with Lord Millett's understanding of the nature of a bank account - that it consists of a uniform mixture of value - in *Foskett* v *McKeown* [2001] 1 AC 102, 127-8. Moreover, in principle, the 'first in, first out' rule is undesirable, as it produces arbitrary and unprincipled results, and for this reason various Commonwealth courts have refused to apply it, and have used the rateable proportion approach instead: the New Zealand CA in *Re Registered Securities* [1991] 1 NZLR 545; the Ontario CA in *Re Ontario Securities Commission* (1985) 30 DLR (4^{th}) 30; the New South Wales CA in *Keefe v Law Society of New South Wales*, 10 September 1998; and the Jersey Royal Court (Samedi Division) in *Abacus (CI) Ltd* v *Grupo Torras SA*, 17 January 2002.

6.3.6 For all these reasons, it is submitted that the rule in *Clayton's case* should not be used to resolve evidential uncertainties when an innocent volunteer mixes his money with earmarked property in a current bank account.

Change of position

6.3.7 By analogy with a surge of cases concerned with claims in the law of unjust enrichment over the past 10 years, following *Lipkin Gorman* v *Karpnale Ltd* [1992] 2 AC 548, an innocent volunteer who receives earmarked property and thereafter incurs extraordinary expenditure might wish to argue that because he has changed his position he should have a defence to any seizure, detention, or forfeiture order. In principle, innocent volunteers should be allowed to rely on such a defence, since it cannot be the policy of the 2001 Act to render them worse off than they were before they were given the earmarked property.

6.3.8 If this is correct, then recent decisions that might prove to be relevant in this context include the following:

- *Phil Collins Ltd* v *Davis* [2000] 3 All ER 808, where Jonathan Parker J took a remarkably relaxed approach to the question of what a defendant has to prove in order to show that he has relevantly changed his position: although the judge was 'unable to find that any particular item of expenditure was directly referable to the overpayments of royalties' received by the defendant musician (at 829), he went on to hold nonetheless (at 830) that in a 'general' way, D's outgoings were larger than they would have been, had he received no overpayments, because he adopted a general life strategy of spending all his income whenever he got it - adopting a 'broad approach' the judge therefore allowed a defence to half the claim.
- *Scottish Equitable plc* v *Derby* [2001] 3 All ER 818, where Robert Walker LJ held (at 827) that in principle it is not always necessary for a defendant relying on a change of position defence to show that he changed his position in reliance on his receipt of the benefit - hence he considered that e.g. an innocent recipient of a payment which was later stolen from him should be entitled to the protection of the defence; at 827 he also considered that in principle a defendant who decides to forgo an income-generating opportunity because he has received a benefit should be entitled to the defence, a view which should be preferred to Potter LJ's view to the contrary in *National Westminster Bank plc* v *Somer* [2002] 1 All ER 198, 215.
- *Dextra Bank and Trust Co Ltd* v *Bank of Jamaica*, PC, 26 November 2001, where the court held that a defendant is entitled to rely on the defence where he has incurred expenditure prior to his receipt of the relevant benefit, provided he has done so in reliance on his understanding that the benefit will be transferred to him.

6.4 Jurisdiction

6.4.1 Section 1(1) provides that civil proceedings for the forfeiture of terrorist cash should be brought before a magistrates' court or (in Scotland) the sheriff. It may be doubted whether a magistrates' court is an appropriate forum for the determination of such proceedings, given their potential sensitivity and complexity. This point was made

by various critics of the legislation both inside and outside of Parliament, but it was not accepted by the Government.

6.4.2 So, in its response to the Anti-terrorism, Crime, and Security Bill 2001, the Law Society stated that it was:

> 'concerned that the Bill proposes that the seizure and restraint powers will be dealt with by lay benches and district judges in magistrates courts. That is unsatisfactory. Terrorism is such a sensitive and complex matter that it is far more appropriate for it to be dealt with in the High Court, at an appropriately senior level of the judiciary'. (Quoted in House of Commons Library Research paper 01/99, p 12).

6.4.3 Again, in the course of the House of Lords debate on the Anti-terrorism, Crime and Security Bill 2001, it was argued that the court deciding on forfeiture orders should be the High Court, or at least the Crown Court, because the rules of tracing (which will be considered below) raise complex issues that are unsuitable for determination by lay magistrates unfamiliar with the legal niceties and often unable to sit for the several consecutive days which might be needed: HL Debs, 28 November 2001, col 304, Viscount Bledisloe (adding that 'tracing and mixing property are normally matters dealt with in the Chancery Division because mere common lawyers cannot understand them'); col 306 (Lord Thomas of Gresford); and col 307 (Lord Kingsland).

6.4.4 Speaking for the Government, Lord Rooker replied that the system for the forfeiture of terrorist property was intended to replicate that used by the Terrorism Act 2000, and by the Drug Trafficking Act 1994, both of which lay down a procedure for hearings in the magistrates' courts. However, he gave no reasoned answer to the objection that in 1994 the Runciman Report (which followed an investigation into the workings of the 1971 Misuse of Drugs Act) stated (at para 53) that:

> 'At present, except where a receiver is appointed by the High Court, the magistrates' courts are responsible for recovering the assets named in a confiscation order. They may find themselves called upon to enforce an order in an amount of several million pounds with a default term of up to ten years. These are amounts and sentences wholly

inconsistent with the maximum penalties that a magistrates' court can impose on conviction, and we doubt whether they are the appropriate jurisdiction for the task. We therefore recommend that the responsibility for the enforcement should lie with the Crown Court not with the magistrates' courts'.

6.4.5 It may be that if forfeiture orders were reserved to a District Judge (Magistrate), and kept out of the hands of lay magistrates, this would go some way to meeting the problem, but even then there is much to be said for placing their resolution in the hands of the High Court, particularly in light of the great reduction in the judicial workload at High Court level which has resulted from the Woolf reforms to civil procedure.

6.5 Conclusion

6.5.1 The forfeiture provisions in the 2001 Act raise many tricky questions to which the Act itself gives no answer. To some of these, for example questions relating to the proper rules to be applied when tracing terrorist property through substitutions and mixtures by terrorists, one might confidently predict that the courts will take a generally unfriendly approach, consistently with the 'tough on terrorists' spirit of the legislation. However, when one considers the position of innocent third party recipients of earmarked property who are not protected as bona fide purchasers, it is hard to see what line the courts should take, since it is hard to see what the Act intends to achieve by exposing them to forfeiture orders. It is therefore a matter of considerable regret that the legislation received so little Parliamentary attention before it was enacted.

CHAPTER 7

Investigation and Enforcement

7.1 Introduction

7.1.1 This chapter is primarily devoted to the impact of initiatives on the operational areas of investigation and enforcement. Detailed reference has already been made to, *inter alia*, terrorist-related legislation, and the effect on banks and financial institutions. The Group felt that consideration should be given to the cause and effect on the key aims of intelligence gathering, leading to disruption of terrorist activities (these activities include training, funding, operations, and recruitment), and arrest and prosecution. It was felt that the relatively low level of seizure of terrorist property should not be allowed to overshadow the significant success in disruption by the authorities. There are however many areas of conflict between and within the areas of intelligence gathering, and investigation and enforcement. When counter terrorist operations started, aims included consideration of 'turning' terrorists, and, inter alia, disruption of terrorist operations. Conflicts arise when arrests publicise these tactics, although it was felt that whilst prosecution of terrorist activities may be 'impractical' for this reason, the successful prosecution of peripheral activities (theft, smuggling, tax evasion, etc,) must be regarded as a positive alternative. Members of the group also felt that there should be a greater involvement of lawyers, accountants, and also more liaison with the private/commercial sectors.

7.1.2 Earlier in 2001, the Financial Action Task Force (FATF) had identified the following major sources of terrorist funding:

Drug trafficking
Extortion and kidnapping
Robbery
Fraud
Gambling
Smuggling and trafficking in counterfeit goods
Direct sponsorship by states
Contributions and donations
Sale of publications (legal and illegal)
Legitimate business activities

7.1.3 FATF's pre-11 September discussions concluded that with the decline in state sponsorship of terrorism, terrorist groups increasingly resort to criminal activity to raise the funds required. The world has now moved on. Consequently, FATF has decided to expand its mission to focus on combating terrorist financing as well as money-laundering. This makes redundant previous disagreements about funds raised by terrorist organisations from non-criminal activity and whether this could strictly be said to constitute money-laundering. There is still disagreement about the need for special legislation. Some FATF experts believed existing legislation adequate for dealing with terrorist money-laundering while others thought terrorist money-laundering to be a distinct variety of money-laundering that required special measures. The origin of terrorist funds is often quite legal, but the purposes to which they are put are not. They thus can behave differently from funds derived from illicit business in that they do not have to be moved around quite so quickly. They can be invested and accumulate before being diverted to illicit purposes. This has led to the growth of perfectly legal business enterprises that in effect wholly or partly belong to terrorist organisations.[168]

7.1.4 In the context of the issues raise above, it was decided by the subgroup to concentrate on the following key areas as a remit for discussion:

- **Investigation powers** – are the investigation powers that practitioners currently have adequate, or do they need to be expanded in some areas? (The Group defined practitioners as members of all agencies engaged in counter-terrorist workpolice: Special Branches, Security Service, Secret Intelligence Service, Customs and Excise, Special Forces etc).
- **Terrorist finance offences** – is the law sufficiently comprehensive?
- **Measuring success** – how should success in relation to the interdiction terrorist property be measured, whether this be by confiscation, forfeiture, freezing assets, etc?
- **Culture** – why is the traditional special branch officer weak in the area of financial investigation, and what can be done to remedy the situation?
- **Organisational structures** – *if we are making the interdiction of terrorist* property a priority, how do we need to adjust our structures to reflect this?

1 'The Business of Terror', a presentation by WA Tupman, at the Institute of Advanced Legal Studies, University of London, on 29 November 2001.

- **Resources** – do we have sufficient resources to do the job?
- **International** – what are the implications of 11 September for international co-operation in the area of terrorist finance investigations?

INVESTIGATION POWERS

7.2 Introduction

7.2.1 The powers available when investing terrorist financing are set out in the Terrorism Act 2000,[169] which consolidated and developed earlier legislation, and the Anti-terrorism, Crime and Security Act 2001[170]. The 2001 Act reflected the need for enhanced powers following the events of 11 September. The police powers conferred by the 2000 and 2001 Acts are additional to powers available at common law or by virtue of any other enactment, and shall not be taken to affect those powers. They would include powers available to police and other law enforcement officers under proceeds of crime legislation where the terrorist finances were interwoven with the proceeds of non-terrorist crime, and to obtain authorisation under the Regulation of Investigatory Powers Act to intercept telephone communications

7.2.2 The definition of a terrorist investigation in the Terrorism Act 2000 includes two direct references encompassing the financing of terrorism – 'an act which appears to have been done for the purposes of terrorism" and "the resources of a proscribed organisation"'. The improved definition of terrorist property[171] and the duty to disclosure provided where a person believes or suspects that another person has committed an offence under the Act based on information which comes to his attention in the course of a trade, business or employment[172], creates a significant demand for terrorist investigations.

7.2.3 The legislation recognises that specific powers of investigation are necessary if this commitment is to be addressed effectively. These powers are contained in the Terrorism Act 2000 as follows:

- Schedule 4 Part I, which relates to restraint orders;
- Schedule 5 which provides power to obtain information; and

[169] Chapter 11, s 32.
[170] Chapter 24.
[171] Chapter 11, s 14, and Chapter 24, Sched 1.
[172] Chapter 11, s 19.

- Schedules 6 and 6A which relate specifically to financial information.

The original powers in the 2000 Act have been amend by provisions of the Anti-terrorism, Crime and Security Act 2001 which also introduced freezing orders.

7.3 Power to restrain terrorist property

7.3.1 The original power to restrain terrorist property contained in Schedule 4 of the 2000 Act prevented someone accused of a terrorist offence selling property they own, manage or control. This meant that until someone was charged with a terrorist-related offence or charges were imminent the suspect property could be disposed of even though in due course it could be subject to forfeiture. The Anti-terrorism, Crime and Security Act 2001[173] amended this power to allow the use of restraint orders at any time after an investigation has started. This change provides time for investigators to advance investigations prior to charging where persons are aware of the police action

7.4 Power to obtain a search warrant[174] to seize and retain any relevant material

7.4.1 This power authorises a police officer to enter the premises specified in the warrant, to search the premises and any person found there, and to seize and retain any relevant material which is found on a search. To seize and retain relevant material a police officer must have reasonable grounds for believing that it is likely to be of substantial value, whether by itself or together with other material, to a terrorist investigation, and must be seized in order to prevent it from being concealed, lost, damaged, altered or destroyed. A search warrant shall not authorise the seizure and retention of items subject to legal privilege.

7.4.2 While under normal circumstances applications for search warrants are made through the courts, special procedures are provided for urgent cases. Under these procedures a police officer of at least the rank of superintendent may by a written order signed by him give the authority for a search warrant. Such orders shall not be made unless there are reasonable grounds for believing that the case is one of great emergency and that immediate action is necessary.

---

[173] Chapter 24, Sched 6A, Pt 2.

[174] Chapter 11, s 37, and Sched 5, Pt I, paras 1 and 11, and Pt II, para 28.

7.4.3 The Act also provides that where anything is seized by a constable under a power conferred by the Act, it may (unless the contrary intention appears) be retained for so long as is necessary in all the circumstances.

7.5 Power to require production and access to particular material (including excluded and special procedure material)[175]

7.5.1 A court may issue an order in respect of particular material, or material of a particular description, which consists of or includes excluded material or special procedure material. Such orders require a specified person, which may include a government department[176]:

(i) To produce to a constable within a specified period for seizure and retention any material which he has in his possession, custody or power and to which the application relates;

(ii) To give a constable access to any material of the kind mentioned in paragraph (i) within a specified period (normally seven days) and may order any person who appears to be entitled to grant entry to the premises to allow any constable to enter the premises to obtain access to the material;

(iii) To state to the best of his knowledge and belief the location of material to which the application relates if it is not in, and it will not come into, his possession, custody or power within the period specified under paragraph (i) or (ii).

Where the material to which an order relates consists of information contained in a computer it shall have effect as an order to produce or to give access the material in a form in which it can be taken away and in which it is visible and legible.

7.6 Power to require an explanation of material

7.6.1 An order may require any person specified to provide an explanation of any material seized in pursuance of a warrant, or produced or made available to a constable. A person's response to an explanation order represents information given under compulsion and cannot normally be used in evidence against him, as this would be a breach of the right against self-incrimination (or 'right to silence'). Such orders shall not require any person to disclose any information which he would be entitled to

[175] Chapter 11, Sched 5, para 5.
[176] Chapter 11, s 37 Sched 5, Pt I, paras 9, 18 and 26.

refuse to disclose on grounds of legal professional privilege in proceedings in the High Court, but a lawyer may be required to provide the name and address of his client. A statement by a person in response to a requirement imposed by an order may be made orally or in writing.

7.6.2 The 2000 Act provides special procedures for urgent cases. These allow a police officer of at least the rank of superintendent may by a written order signed by him. Such orders shall not be made unless there are reasonable grounds for believing that the case is one of great emergency and that immediate action is necessary.

7.7 Power to require a financial institution[177] to provide customer information[178] for investigation purposes

7.7.1 This investigative tool enables a constable to identify accounts in relation to terrorist investigations. It is therefore intended for use at an earlier stage in an investigation than production and explanation orders under Schedule 5 to the 2000 Act. This method of investigation is sometimes known as a 'general bank circular'. The power requires information to be provided in such manner and within such time as is specified and notwithstanding any restriction on the disclosure of information imposed by statute or otherwise.

7.7.2 An order may be made only if 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.

The Anti-terrorism, Crime and Security Act 2001 added Schedule 6A to the Terrorism Act 2000 which extended the powers available for terrorist investigations.

7.8 Power to monitor accounts held by financial institutions

7.8.1 Experience with the power to require production of particular material under the Terrorism Act 2000[179] found that in respect of information on accounts held by financial institutions it was 'not well suited to information relating to transactions. In particular it only relates to material in the possession, power or custody of the financial institution or such material, which will come into existence within 28 days

[177] Chapter 11, Sched 5, para 6 defines 'financial institution' and provides powers to amend the definitions through subordinate legislation as and when necessary.
[178] Chapter 11, Sched 5, para 6 defines 'customer information' and provides powers to amend the definitions through subordinate legislation as and when necessary.
[179] Chapter 11, Sched 5, paras 5 and 11.

of the order. As a result such production orders cannot require the "real-time" disclosure of the fact that a transaction on the account has occurred, as there may well be a delay before the material recording the fact is produced.'[180]

7.8.2 There are also opportunities available in respect of terrorist investigations where the property or inquiries relate to, or reside in, other countries or where the investigation originates in a third country. Cooperation and assistance has been fostered through INTERPOL and EUROPOL, and direct contact with law enforcement bodies in other countries and contacts established through United Kingdom embassies or foreign embassies in the UK. In other instances reliance is placed on conventions, mutual assistance treaties and agreements applied by the governments of many countries – for example, the International Mutual Legal Assistance Treaty which facilitates the interchange of banking and financial information between the UK and the USA, and the European Convention on Mutual Assistance which allows cooperation by law enforcement authorities in many European counties.

7.8.3 Part 2 of the Anti-terrorism, Crime and Security Act contains measures to allow the United Kingdom to take action to freeze the assets of overseas persons or governments who are threatening the economic interests of the United Kingdom or the life or property of UK nationals or residents. The provisions replace section 2 of the Emergency Laws (Re-enactments and Repeals) Act 1964.Under the 2001 Act, the Treasury is able to freeze the assets of overseas governments or residents, including of groups or individuals, when there is a threat to the United Kingdom economy or to the life or property of UK nationals or residents. These provisions allow the United Kingdom to impose sanctions in cases of urgency, where neither the United Nations nor the European Union has yet agreed a course of action, or in cases where it is appropriate for the UK to impose sanctions unilaterally.

7.9 Assessment

7.9.1 The tools available in the United Kingdom to investigate terrorist financing are extensive and comprehensive – a position confirmed by law enforcers. On an operational level some of the measures are considered cumbersome, especially where urgent action is required, but the consensus view was that safeguards built into the application procedures served to eliminate excessive or inappropriate usage.

[180] Home Office Circular No 30/2002 issued 14 December 2001

Comments were also noted on the inability to obtain, and/or delays in obtaining, information from some other countries, particularly given the constraints prescribed in legislation, or when it is reasonable for delays to occur (eg when property is restrained).

7.9.2 A recent Northern Ireland development which amended the Proceeds of Crime (Northern Ireland) Order 1996[181] provided investigation powers in relation to solicitors which could also be adopted for use in terrorist investigations throughout the United Kingdom. The measure permits an investigator, where it appears that a specified person may have benefited from any conduct for which a confiscation order could be made, to give notice in writing requiring a solicitor to furnish specified information within a specified time and in a specified manner. The information which may be specified is whether at any time during a specified period the specified person was a client of the solicitor in respect of any land or business; a company, firm, partnership or trust; a bank or other account; or any assets in the nature of investments, being assets of the specified person. Where the specified person was a client the solicitor shall provide the full name of the client; the most recent and all known previous addresses of the client; the date of birth (if known) of the client; other evidence of identity of the client obtained in accordance with the Money Laundering Regulations 1993; and specified details of the nature of any transaction relating to any matter mentioned in the notice.

7.9.3 There are also a number of issues giving increasing cause for concern which the Financial Action Task Force in particular has highlighted. The FATF issued a consultation document on 30 May 2002 which sets in train a review of the 40 recommendations relating to money laundering originally drawn up in 1990. The document provides detailed background on the areas of concern and sets out options for amendments to the anti-money laundering recommendations. Whilst in some areas they reflect provisions already incorporated into United Kingdom terrorist or proceeds of crime legislation, there are issues where detailed consideration would be merited. These include... 'The availability of information on the persons that are the true owners and controllers of assets derived from criminal activity. Such persons have increasingly used various types of legal entities or arrangements to conceal their ill-gotten wealth, as part of the money laundering process.'

[181] Statutory Instrument 2001 No. 1866 made 14 May 2001.

7.9.4 Areas highlighted where the Financial Action Task Force has indicated that law enforcers would benefit from 'timely availability of information on beneficial ownership to, and sharing of that information between, investigators, FIU and regulators, both at national and international levels' include beneficial ownership of companies and trusts, and bearer shares. The FATF also continues to be concerned about the risk for investigators posed by bank secrecy.

TERRORIST FINANCE-RELATED OFFENCES

7.10 Terrorism Act 2000: Part III –Terrorist Property

7.10.1 The following terrorist finance-related offences are contained in Part III of the Terrorism Act 2000:

Section 14 defines terrorist property as including 'money or other property which is likely to be used for the purposes of terrorism..'

Section 15 prohibits fund-raising for the purposes of terrorism, and creates an offence of inviting another to provide money, receiving money or providing money in this regard.

Section 16 provides that a person commits an offence if he uses money or other property for the purposes of terrorism.

Section 17 creates an offence of making money or other property available for the purposes of terrorism.

Section 18 creates an offence in connection with money laundering and states as follows:

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

(a) by concealment,

(b) by removal from the jurisdiction,

(c) by transfer to nominees, or

(d) in any other way'

A defence is provided if it can be shown that the person charged did not know and had no reasonable cause to suspect that the arrangement related to terrorist property.

Section 63 extends the scope of criminal jurisdiction in respect of matters which fall within sections 15 -18 to acts which are undertaken outside the United Kingdom as well as those done within the United Kingdom

Section 19 creates a duty to disclose to a police constable any belief or suspicion that an offence contrary to sections 15 -18 has been committed. Unless the information is subject to legal professional privilege (and in that regard is not received other than with a view to furthering a criminal purpose, it must be disclosed. A defence is provided where an individual has reasonable excuse for not making such disclosure, such as where he has disclosed matters in accordance with any internal procedure.

Section 20 permits the disclosure to a constable of a belief or suspicion that money or other property is terrorist property or is derived from such property, notwithstanding any restriction on the disclosure of information imposed by statute or otherwise.

Section 21 provides that no offence is committed under specified provisions of the Act where a person acts with the express consent of a constable or discloses information to a constable.

Section 22 sets out the penalties for an offence under sections 15 –18.

Section 23 empowers the court by or before which a person is convicted of an offence under any of sections 15 -18 to make an order for the forfeiture of any money or other property which would or might be used for the purposes of terrorism.

Section 25 empowers an authorised office to seize and detain for 48 hours any cash (cash and authorised officer being defined by s 24) being exported or imported into the United Kingdom if he suspects that the cash is intended to be used for the purposes of terrorism, it forms the whole or part of the resources of a proscribed organisation, or it is terrorist property.

Section 26 provides for the application by an authorised officer or the Commissioner of Customs and Excise ('CCE') to a magistrates' court for an order authorising the further detention of cash seized under section 25 for a period of up to three months

Section 27 deals with the holding of the detained cash and for applications for its release.

Section 28 provides for the application by an authorised officer or the CCE to a magistrates' court for an order forfeiting cash being detained under section 25.

Section 29 provides for appeals against an order under section 28.

Section 30 provides for the payment of forfeited cash into the Consolidated Fund.

Section 31 makes provision for the making of rules of court about the procedure on applications or appeals to any court under sections 26-29

7.11 Mutual legal assistance ('MLA')

7.11.1 MLA is that process which is directed towards the gathering of evidence (and sometimes, the preservation of assets) in the United Kingdom by its authorities at the request of the authorities of a foreign state ('the requesting State'). The process is potentially reciprocal, which means that the UK may also seek similar assistance from foreign States. In the UK, the Home Secretary is the decision-maker with ultimate responsibility for considering and deciding upon MLA requests.

7.11.2 At the inter-governmental level over the past 40 years, steps have been taken to facilitate co-operation at the level of the Council of Europe (the European Convention on Mutual Legal Assistance in Criminal Matters 1959), and in the Commonwealth (the Harare Scheme), as well as upon a bilateral basis between States. More recently, separate treaties have been agreed as between Member States of the European Union, and Member States of the United Nations.

7.11.3 In the United Kingdom, the relevant legal framework in respect of MLA is provided by the Criminal Justice (International Co-operation) Act 1990 ('the 1990 Act'). Pursuant to the1990 Act, the requesting State must submit a request in writing for MLA which identifies the existence of criminal investigations or proceedings in the requesting State in pursuit of which the MLA request is made. If it is able to do this and show the nexus between those matters and evidence/assets in the United Kingdom, the Secretary of State may exercise his discretion to accede to the MLA request. That can enable evidence to be gathered in the UK by means of search warrants or production orders, or the exercise of investigative powers by the Serious Fraud Office under section 2 of the Criminal Justice Act 1987.

7.11.4 Some of the issues that have arisen in the recent (but fairly limited) challenges to decisions made by the Secretary of State in respect of MLA requests include;

- Whether MLA requests are made in pursuit of bona fide investigations/criminal proceedings.
- Whether such investigations/criminal proceedings are politically motivated or otherwise violate ECHR rights (especially Arts 3, 6 and 8).
- Whether asset restraint is available in the UK in aid of a MLA request (the requesting State must have legal provisions which enable it to make extra-

territorial asset restraint orders to enable asset restraint to be obtained in the UK pursuant to a MLA request).

7.11.5 The MLA process is potentially very effective in combatting crime which has a multi-jurisdictional aspect. For example, in 1999 the Nigerian Government made MLA requests from various States (which in June 2000 included the UK) in respect of monies allegedly wrongly taken from Nigeria by the late General Sani Abacha and his associates. As a consequence of the MLA process, more than US$ 1 billion was frozen in various jurisdictions and repatriated to Nigeria in May 2002.

MEASURING SUCCESS

7.12 Cost of mounting a terrorist campaign

7.12.1 The cost of mounting a terrorist campaign will depend on a number of factors, including the size of the group and the nature of the campaign.

7.12.2 The size of a terrorist group may affect its financial requirements in that smaller groups, such as those involved in animal rights terrorism, may require more limited finance than larger organisations. The finance necessary to carry out violent attacks on persons or property may amount to a small proportion of the funds needed to finance the organisation as a whole. Terrorist groups, like all other organisations, will require money to pay their overheads. Infrastructures are expensive. Larger terrorist groups require greater amounts of finance to recruit and train their members. As with any business, employees' skills need to be created. The investment in terrorist competences is likely to have a financial cost since, just as any business needs to pay for training to develop competences, so too do terrorist organisations. Business costs may be divided into fixed and variable costs, and the fixed costs of a larger business will be larger than those of a smaller one. For example, there may be a need for an organisation to provide financial aid to their prisoners' families [182] because without this supporters' commitment might wane.

7.12.3 The nature of a terrorist organisation's campaign will also affect its financial requirements. For the past 30 years various terrorist organisations in Northern Ireland have carried out sustained campaigns and to achieve this they have required significant finance. While individual terrorist acts, for example the hijacking and

[182] *Inquiry into Legislation Against Terrorism*, Lord Lloyd of Berwick, Cm 3420, 1996, (hereafter referred to as 'Lord Lloyd'), Vol 1, para 13.1.

setting alight of a bus, may not require significant finance, a sustained terrorist campaign is more likely to. The purchase of weapons, particularly sophisticated ones, may often represent a significant expense. The cost of developing a nuclear capacity will inevitably exceed that of a capacity to explode car bombs. Mounting operations in a foreign jurisdiction is likely to be more expensive than conducting operations in a domestic one. A terrorist organisation may spend a proportion of its total income on non-terrorist activities in order to retain sympathetic supporters.

7.12.4 To assemble and train the terrorist team for the 11 September operation required considerable financial resources. One suspect paid for 12 hours' flight training at $88 per hour and then followed this by enrolling in a Florida flight school, paying $10,000 by cheque, finally training at other flight schools on bigger planes 183 and spending $1,500 for three hours in a Boeing 727 simulator. 184 Investigators discovered that, while two of the suspects had lived in Hamburg for five years where they had been enrolled as electronics students, they had had no student grants and did not claim state benefits. 185 When five of the suspects attempted to buy mobile telephones, they were initially refused because they offered no form of identification, but staff relented when they offered $3,000. 186 Accommodation in the USA for one suspect cost $1,400 per month. 187 In total, over $500,000 in overseas funding was transferred into bank accounts used by the hijackers. Of course, by comparison, many al-Qaida attacks were carried out on a much more limited budget [188] and the 1993 World Trade Centre bombing is believed to have cost just $20,000. [189]

7.13 Evaluating the impact of measures against terrorist finance

7.13.1 The evaluation of the impact of measures against terrorist finance and, indeed, against money laundering generally, is in its infancy. Success to date has tended to be measured crudely in terms of the amount of funds frozen, irrespective of whether or not these sums will be confiscated after final legal determination, and though the headline figure thus generated is doubtless politically satisfying to some, it is not a

---

[183] 'When our world changed for ever', *The Observer*, 16 September 2001.

[184] 'Mohamed Atta: profile of a terrorist', *The Observer* 16 September 2001.

[185] 'When death came out of a blue sky', *The Sunday Times*, 16 September 2001.

[186] Ibid.

[187] 'When our world changed for ever', *The Observer*, 16 September 2001.

[188] 'Bin Laden's money takes hidden paths to agent of terror', *The Washington Post*, 21 September 2001.

[189] 'US ties hijackers money to Al Qaeda', *The Washington Post*, 7 October 2001.

measure of effectiveness but of partial efficiency. Conceptually, to judge the potential impact of measures to restrict the flow of funds to people who wish commit terrorist acts, one would have to know (a) how much money the would-be terrorists need to carry out their plans (which plans of course might be a function of what funds and other instrumentalities of crime were available); and (b) what legitimate and illegitimate means of financial support they have available at any given moment in time. In a broader, longer-term time frame the background support might include training and recruitment opportunities & processes, which would require a different level of funding than individual operations. Terrorists who do not intend or expect to live beyond the operation have less need for secrecy infrastructure such as networks of safe houses than do those who intend or seek to stay around for lengthy periods. Even if terrorist finance were restricted more severely than in the past, proceeds of fresh crimes could be funnelled into the purchase of goods and services needed for operations: as in other areas of crime, the need for funds is also a function of expenditure flows, and Islamic terrorist groups are more frugal and therefore need less funds than many others.

7.13.2 Even excluding the concerns of those who doubt that frozen charitable funds are all proceeds of and/or funds intended for terrorism[190], the total stock and flow of funds available for terrorist activities remains both unknown and dynamic, dependent as it is on (i) shifts of attitudes of support and opposition to existing terrorist movements[191], and (ii) which new terrorist movements come into existence. The total stock of funds available for terrorist use therefore should not be seen as an absolute sum but as conditional upon a flexible set of factors: the *flow* of funds (i.e. the part of the stock that is required for current operations) is a different and probably much smaller figure, though how much smaller depends on how much support the terrorist groups, networks or individuals have.

---

[190] This is not the place for debates about whether or not funds disbursed to the families of dead or disappeared terrorists should analytically count as terrorist finance.

[191] Including the attitudes of those who label movements as terrorist or not: a far from banal point, as controversies over which Israeli/Palestinian behaviour should be called 'terrorist' demonstrate. When bin Laden was supported by the CIA, he presumably was not to be considered to be benefiting from 'terrorist finance'. No good is served by attempting to hide the difficulties involved in these issues for the reservoir of terrorist funding, even though we can resolve the issue practically by legislative fiat, ie terrorist finance is funding available to those organisations and persons designated as terrorists at any given moment in time, irrespective of whether or not such persons were our allies in the past or will become so in the future.

7.13.3 Terrorist finance generates a threat to both the security of international capital and the lives of financial services employees, so (to a greater extent than with drugs trafficking or tax evasion, for example) self-interest may reasonably temper profit maximisation if institutions believe that the identification of terrorist finance can protect them or activities in which they have a stake[192].

7.13.4 From the perspective of the financial community, it is arguable that the ideological and value threat of terrorism thus constitutes a distinction from organised crime and other 'threats to society'. One of the special features of terrorist funds laundering is that it explicitly aims to examine the proceeds of legitimate-source activity actually used or intended to be used for (rather than deriving from) a criminal purpose: in that sense, its closest analogues are (1) the corporate and political 'slush funds' used for transnational corruption and political finance, and (2) tax evasion on non-criminal activities. This broad approach is crucial if anything approaching a plausible effort is to be made in restricting terrorists' access to funds, though on a harm reduction model, it may make some sense to restrict flows to particular terrorist groups from particular sources without necessarily having a major impact on the totality of terrorist finance[193]. Indeed, to avoid the paralysis that results from the view that if we cannot do everything there is no point in doing anything, it must be emphasised that the reduction of even one terrorist attack is a worthwhile objective, and that the objectives of terrorist finance controls are the *reduction* of terrorist harms (preferably to zero)[194].

7.13.5 As studies of how suspicious financial transaction reports come to be constructed and followed through demonstrate[195], few bankers know what types of crime – if any – their customers may be engaged in: with the exception of some ideologically or culturally sympathetic bankers and non-bank financial services such as money transmitters, this would apply *a fortiori* to terrorist finance. If clients fool bankers or

---

[192] This stake might include businesses or governments to which they have loaned money, whose security as well as whose business plans may be disrupted both by actual and fear of terrorism. Contrariwise, the reporting of suspected terrorist finance also can bring physical risks to staff should they be identified – directly or by logical deduction - as the source of the information.

[193] To avoid accusations of naivety, it is as well to recognise that terrorist funding can come from the West as well as from 'rogue states' as defined by the US.

[194] Though estimates of what the level of terrorist attacks might have been can be an area of much dispute, since sceptics may not be inclined to accept intelligence agencies' estimates on the grounds that these may be self-serving, while the intelligence community will normally be unwilling to submit its data to external gaze.

[195] Levi, M (1991) Customer *Confidentiality, Money Laundering and Police-Bank Relationships*, London: Police Foundation; Gold, M. and Levi, M (1994) *Money-Laundering in the UK: an Appraisal of Suspicion-Based Reporting*, London: Police Foundation

lawyers into believing that at most, the funds constitute 'merely' tax 'dodging', then it is plausible that no suspicious transaction report will be made[196]. Therefore, it is only if all crimes are included within the obligation to report suspicions that the layer of rationalizations falls away (save, perhaps, for labelling the behaviour tax avoidance).

7.13.6 The US Treasury on 3 May 2002, summarised the blocking of assets of 210 alleged Terrorist-related entities and individuals in the US as amounting to $34 million and by its international partners as $82 million, totalling $116 million worldwide. So far, 161 countries and jurisdictions have been involved in this campaign. At the end of March 2002, the UN estimated that 144 countries had been involved in blocking $103.8 million in assets of which approximately half represents (they asserted) assets connected with Usama bin Laden and al-Qaida. The majority of these funds had been blocked by December 2001. The April 2002 UK progress report to the International Monetary and Financial Committee (IMFC) on the international fight against terrorist financing stated that:

> 'The UK took effective action to freeze funds soon after UNSCRs 1267 and 1333 were adopted. Before 11 September, some $90 million of Taliban assets had been frozen; since 11 September some $10 million has been frozen. Efforts are now underway to return the bulk of these assets - around $85 million - to the new legitimate Government in Kabul. Some $15 million remains frozen.'

7.13.7 However, since there is little knowledge of how these sums relate to the actual and replenishable stocks and flows of funds needed by different sorts of terrorists to finance their intended activities, the impact of such measures on actual and intended terrorist plans remains only modestly understood. The work of the Terrorist Finance Unit and its successors in Northern Ireland demonstrated the capacity to restrict the free availability of funds to the Provisional IRA from crime and 'black economy'

---

[196] The 1999 FATF interpretative note tries to find an intermediate position and to get financial and other regulated bodies to report suspicions even when a 'tax' explanation is given, at least where it is not obvious that tax evasion actually is involved. This states:

> 'In implementing Recommendation 15, suspicious transactions should be reported by financial institutions regardless of whether they are also thought to involve tax matters. Countries should take into account that, in order to deter financial institutions from reporting a suspicious transaction, money launderers may seek to state *inter alia* that their transactions relate to tax matters.'

work in the North by situational criminal opportunity reduction *inter alia* in requiring licenses for certain types of taxi work, and tighter regulation of gambling settings from which funds were extorted as well as freely granted by sympathisers. The proportion of such funds that were banked and saved/laundered by PIRA rather than being simply redistributed as cash wages to 'soldiers' and intermediaries was far smaller than the totals obtained from crime, from tax evasion and from sympathisers in Ireland, let alone world-wide.

7.13.8 Where a few hundred credit card frauds can generate sufficient cash to fund the 9/11 tragedy, the difficulties of incapacitating those terror groups by financial means cannot be overstated, though valuable leads that can disable terrorist cells can be and have been generated by reports from financial institutions[197]. Intelligence data such as the debriefing of terror suspects and the yields from suspicious and unusual transaction reports may in time give us a better clue, but whether some or all of these analyses will ever reach the public domain is a matter for speculation. In the case of fairly regular volume crime, crime reduction studies are capable of reasonably robust measures of prevention and displacement, but for relatively rare catastrophe events and for 'market crimes' such as the supply of illegal goods and services, the measures of prevention are often indirect and much more speculative.

CULTURE

7.14 Introduction

7.14.1 Why has the interdiction of terrorist finance in the UK been relatively unsuccessful? If, as has been suggested earlier in this report, the investigation powers available to police are adequate and the terrorist finance offences available to prosecutors are similarly adequate, then we must look to how law enforcement agencies are being managed for answers to this question. It is self-evident that the success of terrorist finance interdiction can only be based on whether there is an effective financial investigation capability in anti-terrorist agencies. Three issues therefore require consideration:

A Does the organisational culture of UK law enforcement agencies sufficiently value the function of financial investigation?

[197] This applies *a fortiori* to the suicide bombings in Israel and Israeli-held territory.

B Is UK law enforcement organisationally structured so that there is a national financial investigation capability?

C Is the UK financial investigation capability sufficiently resourced?

7.14.2 Questions must also be asked concerning the status of financial investigation in UK police circles generally. Levi and Osofsky's seminal 1995 research into financial investigation and confiscation of the proceeds of crime in the UK[198] discovered that officers attached to Financial Investigation Units felt isolated from many of their fellow officers (particularly at the upper management level) in the sense that many of these other officers appeared to have no real idea of what financial investigation entailed and the importance of these investigations. While some forces felt that the management to whom they reported was supportive of their efforts, the vast majority were distressed at what they perceived as an 'outdated' view held by these same managers that, unless an officer is locking up criminals, he or she was not doing 'real' police work. Even where managers supported financial investigations in theory, police officers were sometimes frustrated by the lack of real understanding about what their work involved.

7.14.3 The findings of the 2000 Cabinet Office report *Recovering the Proceeds of Crime* suggested that many of the weaknesses identified by Levi and Osofsky still exist. The Cabinet Office carried out its own survey and discovered three main features of financial investigation in UK law enforcement:

A Financial investigation is underused and undervalued.

B Financial investigation is under-resourced with a shortage of people with the right skills.

C There is little cross agency co-operation or sharing of best practice.

7.14.4 The Cabinet Office also found that management information in respect of financial investigation was scarce, which it considered to be a worrying sign. It was concluded by the Cabinet Office that financial investigation should be made central to UK law enforcement (clearly implying that it was not currently central) in order to make it as

[198] 'Investigating, seizing and confiscating the proceeds of crime', Levi, M and Osofsky, L, Home Office Police Research Group, 1995.

routine to tackle criminals through their financial arrangements as it was to use techniques such as surveillance.

7.14.5 Given the weaknesses of the role of financial investigation in UK law enforcement generally, the question must be posed as to whether the same weaknesses are present in relation to the financial investigation function in the anti-terrorist field. The starting hypothesis must be that the position in respect of financial investigation is unlikely to be different in the anti-terrorism field unless senior management have consciously and conscientiously sought to produce a different culture from that established by their counterparts in respect of ordinary criminal investigations.

7.15 The concept of organisational culture

7.15.1 In the 1980's, business writers began to write about the concept of 'organisational culture'.[199] The concept has its main roots in social anthropology and refers to the shared cognitive and value orientations of an organisation's members. Culture can be thought of as the basic values, ideologies and assumptions which guide and fashion individual and organisational behaviour. Culture is 'the way we do things around here'. It is pervasive, but to a large degree implicit in an organisation. We may be familiar with the culture of an organisation and yet not aware of it. However an organisation's values are evident in factors such as stories, ritual and language. Culture also makes a difference to the way problem solving is approached. The language of organisational culture has now entered the way senior managers think and talk about organisations and organisational change; and there are many influential management writers and practitioners who stress the role of culture in organisational performance.

7.15.2 The corporate culture approach believes that organisational cultures can be assessed, managed, constructed, and changed in the pursuit of enhanced organisational effectiveness. The aim is to win the hearts and minds of staff in respect of the values that senior management wish to emphasise. Culture management is the process of developing or reinforcing an appropriate culture, that is one which helps the organisation fulfil its objectives. Successful management is accomplished by the management of meaning in an organisation and not simply by designing structures. Managers must recognise that there is often a need to distinguish between espoused

[199] For example, Peters, T J and Waterman, R H, *In Search of Excellence*, New York, Harper and Row, 1982.

organisational values and values-in-action as actually lived out on a day-to-day basis by members of the organisation.

7.16 Special Branch culture

7.16.1 The question therefore arises whether the organisational culture of UK anti-terrorist law enforcement agencies sufficiently values the function of financial investigation. One indication that financial investigation is not given appropriate value is the comment made by one financial investigation officer about the traditional Special Branch view :

> 'Guns and bombs are more sexy than money.'

7.16.2 While Special Branch offices throughout the UK will have aspects of culture in common, it should not be suggested that Special Branch culture is homogeneous. While there will be strong similarities in the Special Branch cultures in different forces, there will also be disparities, often caused by the way particular officers are being managed and by the type of leadership exhibited by particular managers. Since culture is pervasive but to a large degree implicit, there will never be a sign on a wall in a Special Branch office stating 'financial investigation is not valued here'. While it is inconceivable that officers would overtly state that financial investigation is unimportant in anti-terrorist work, financial investigation may simply be an issue that lip-service is paid to.

7.16.3 There are a number of ways of attempting to discover whether Special Branch culture sufficiently values financial investigation:

(i) How integrated is financial investigation into anti-terrorist investigations generally? What evidence is there that, just as it is now best practice for drug trafficking organisations to be investigated in terms of both drug flows and money flows, terrorist organisations are similarly investigated? Is a financial investigation officer attached to each significant anti-terrorist enquiry? Do agent handlers consistently seek information about terrorist finances or is this an area of investigation somewhat neglected?

(ii) It is now recognised that the stories people recount to one another in organisations, and especially to newcomers, reveal how they see their

organisations and what they value. What success stories do Special Branch officers tell? Do any of them celebrate how financial investigation played an important role in identifying members of a terrorist cell or frustrating a terrorist outrage?

(iii) An organisation reveals its values in part by those who are successful or become influential. Where individuals are excluded or isolated, that states something about the values of the organisation. Do officers involved in financial investigation get promoted into senior management or is financial investigation seen as a non-mainstream area that officers need to move out of if they are to achieve promotion? Do financial investigation officers plough a somewhat lonely furrow, separated from colleagues involved in other work?

(iv) What proportion of Special Branch staffing resources are devoted to financial investigation? The answer may give an indication of how important within the Special Branch culture that financial investigation is taken.

(v) For financial investigation to becoming a thriving discipline there needs to be a supportive group who have a vision for the importance of the financial investigation function. In certain parts of the country, however, Special Branch Financial Investigation Officers are isolated from Financial Investigation Officers in CID and hence there is a lack of interchange of knowledge and best practice between them. Sometimes Special Branch Financial Investigation Officers approach other Financial Investigation Officers for assistance, which may tend to indicate a lack of expertise in certain Special Branch units.

7.16.4 In summary we have found from our collective knowledge little evidence of the financial investigation function being valued sufficiently. Just as in ordinary criminal investigations there is a traditional view which places financial investigation outside the core work of investigators, so there is often a parallel view in Special Branch which sees financial investigation as peripheral to core activities. The significant exception to this conclusion must be the Financial Investigation and Special Access Centre of the Metropolitan Police Special Branch, which is accepted as the market leader in terrorist finance investigations. FISAC is currently the best resourced UK anti-terrorist financial investigation unit and has an informal national role in this field.

7.17 The way ahead

7.17.1 There is a consistent stream of research evidence that it is possible, within limits, to achieve change in corporate cultures. Nevertheless it must be recognised that staff behaviours are easier to change than values; and the more superficial levels of culture are easier to change than deeper assumptions. What suggestions can be made to try to change a traditionalist culture which does not place sufficient importance on terrorist finance? The following may be suggested:

- *Writers on corporate culture must stress the importance of visionary leadership.* The posture of senior managers is vital. If senior Special Branch managers do not truly believe and hold it as part of their personal value system that financial investigation plays an essential role in the function of their units and that the interdiction of terrorist property is an important aspect of the UK's anti-terrorist effort, then the staff they manage will not believe it either. This will inevitably affect organisational performance in this regard. Senior managers must be totally explicit about the desired corporate values and must communicate and stress them constantly. There must be no confusion about what is valued in the organisation. Senior managers must role model the importance of financial investigation. In order to assist in changing their own personal values, Special Branch managers without a financial background might usefully spend a number of days with a Financial Investigation Unit and visit it thereafter on a consistent basis.
- *The interdiction of terrorist finance must become a genuine corporate goal of terrorist investigations.* The introduction of targets and incentives will drive a more proactive approach to financial investigation. Just as the government has set an Asset Recovery Strategy with targets and objectives in respect of the amount of proceeds of crime that are recovered by law enforcement agencies, so too police forces should begin to set targets for terrorist finance removed from terrorist organisations.
- *Training serves a crucial function and members of Special Branch Financial Investigation Units should have an input into general Special Branch training so as to persuade new officers of the importance of financial investigation.* The

clear experience from the financial investigation field generally is that not all officers are suited to financial investigation.

- *The values of financial investigation must be 'operationalized' for officers so that they know what the values mean in practice.* For example Special Branch agent handlers should be given a checklist of financial questions to ask agents. Senior management should ensure that the financial questions are consistently being asked.
- *Processes need to be examined to ensure that financial intelligence is being optimally used in all investigations.* The function of financial investigation must be fully integrated with all Special Branch investigations. Each significant investigation must have a financial investigation element.
- *Stories about financial investigation successes should be encouraged.* Senior management should announce such stories as good news and celebrate them as good performance to enable them to become part of the cultural fabric of the organisation.
- *Inspections might usefully be carried out to determine how established and integrated the discipline of financial investigation is.* Such investigations could be carried out by investigators from other law enforcement organisations where financial investigation has been successfully integrated. Financial Investigation Officers should visit other units, such as the Metropolitan Police Clubs and Vice Unit where financial investigation is accepted to be well integrated with investigations generally.
- *New staff should be recruited to Special Branch and appraised in terms of their capacity and willingness to adopt the new values.* Resistance to change must be firmly met by officers being made aware of their shortcomings in this regard. Cross pollination could be achieved by bringing financial investigators in from other law enforcement agencies, such as the National Crime Squad, to strengthen the financial investigation discipline in police forces where it is weak.

ORGANISATIONAL STRUCTURES

7.18 Effective strategy against terrorist financing

7.18.1 An effective strategy against terrorist finance will require more than legislation. It will require organisational response and this may be examined under three heads

- cultural change;
- organisational change;
- resource management.

7.19 Cultural change

7.19.1 It may be suggested that the long-standing weaknesses present in financial investigation generally also exist in the terrorist field. A recent Cabinet Office report observed that financial investigation was underused, undervalued and under-resourced in the UK and concluded that it should be made central to UK law enforcement. [200] Similarly, there may be those in Special Branch who view finance as merely peripheral to their investigations. Even where officers do consider financial matters it may be that, just as in non-terrorist cases, investigators tend to focus on criminal offences that give rise to funds rather than also focus on the laundering of those funds. If so, the focus will be on shutting down counterfeiting rackets rather than attempting to discover how the finance is laundered, in order to destroy the laundering infrastructure by prosecution for laundering offences.

7.19.2 In practice, however, the focus on terrorist funding in the UK has been too weak. Just as the PIU Report observed that the lack of financial investigation focus hindered the fight against organised crime, so too it hinders the fight against terrorism. Arguably, there is a need to bring in financial investigators earlier and more centrally to terrorist investigations. This is undoubtedly true of many jurisdictions and not just the UK. The traditional focus of some agencies seeking to combat terrorism was on weapons and targets rather than finance, but it should be noted that the Security Service, Secret Intelligence Service and the CIA began significant collaboration on the financing of terrorist groups in the late 1980s. Indeed, in a model operation of its kind, this collaboration had exposed and disrupted some of the commercial banking and financing arrangements of the Abu Nidhal Organisation by 1990,

---

[200] 'Recovering the Proceeds of Crime', Performance and Innovation Unit, Cabinet Office, 2000.

although state sponsorship of Abu Nidhal was a different matter. But just as this sort of collaboration helped bring about changed working practices in the agencies involved, so the change in tactics against organised crime should also bring about a change in thinking in combating certain forms of terrorism. There is therefore a need for managers to bring about cultural change so that organisations with an anti-terrorist remit take account of financial investigation at all levels.

7.19.3 A cultural issue of a different kind is the question of whether there is a correct strategic balance currently being drawn between the use of financial information as intelligence and its use as evidence. The intelligence community and the law enforcement community each operate with inevitably differing priorities. Transforming intelligence into evidence may not be desirable if important intelligence assets are put at risk. It must be recognised, however, that seizing terrorist property is not always the pre-eminent objective of financial investigation. The question must be posed as to how important the seizing terrorist of finances is regarded in the overall strategy of the various agencies.

7.19.4 As we have said, the type of questions that need to be asked regarding the place of financial investigation in the anti-terrorist field in order to perform a proper cultural audit are:

- What proportion of Special Branch resources are devoted to financial investigation ?
- Following the increase in disclosures by financial institutions after 11 September 2001 did resources increase to enable these to be properly assessed?
- Do our staffing policies imply that financial investigation in terrorism is peripheral to the core investigation?
- Are any of the performance measures used to measure achievement and success in the anti-terrorist field ones which relate to the investigation of terrorist finances, prosecution for terrorist finance offences, or seizure of terrorist funds?
- Do senior officers lead their organisations in such a way that all staff perceive financial investigation to have a central role?

7.19.5 Even prior to 11 September this need for change was beginning to be recognised. The US Money Laundering Strategy 2000, as part of its effort to strengthen international co-operation to disrupt the global flow of illicit money, suggested a

training programme for investigators, prosecutors and judges which would concentrate specifically on terrorist financing for countries which face this problem.[201]

7.19.6 Cultural change is also required in the private sector to ensure that disclosures are made in appropriate cases. It has been suggested that 'the mindset of the entire banking system' requires change and that international bankers will have to be persuaded to show a great deal more curiosity than they have in the past. Disclosures by financial institutions in many jurisdictions following 11 September 2001 have greatly exceeded those preceding that date. The difference is that organisational cultures have been changed by that event and disclosers have been mindful of their obligations. Undoubtedly, however, still more change is necessary. Achieving this change is crucial as the private sector possesses monitoring systems and information that law enforcement cannot rival. The goal for financial institutions is do what they should have been doing all along, namely making disclosures in compliance with the legislation.

7.20 Organisational change

7.20.1 Cultural change without structural change in organisations will be insufficient. In the UK a new Terrorist Finance Team has been established within the NCIS Economic Crime Unit. [202] In addition, a new taskforce has been established, bringing together financial, commercial and academic expertise, including forensic accountancy expertise to look, in particular, at *hawala* banking.[203] However intelligence needs to be transformed into evidence if legal proceedings are to be instituted. To do so, the UK arguably requires a terrorist finance investigative capacity which is multi-disciplinary in nature. For example, not only will forensic accountancy skills be necessary but also a Customs presence where finance is being derived from complex VAT carousel frauds or smuggling activities. A multi-disciplinary Terrorist Finance Unit which included staff from police, Customs, Inland Revenue and accountancy backgrounds did exist in Northern Ireland between

[201] 2000 Strategy, p 72.
[202] NCIS press release, 27 November 2001. The US has also created a new task force, the Foreign Terrorist Asset Tracking Centre, which is designed to track and seize terrorist assets. Based in the US Treasury, it includes staff from both intelligence agencies and law enforcement agencies.
[203] Statement of the Chancellor of the Exchequer to the House of Commons, 15 October 2001.

1989 and 1996. Its role included intelligence gathering, assisting in investigations and developing regulatory solutions in areas that were being exploited by terrorists.

7.20.2 Organisationally, it left primacy for investigations with the police and very limited information is publicly available about the outcomes of its work. [204] If a multi-disciplinary Asset Recovery Agency is necessary to investigate and take appropriate legal action against the assets of organised crime, then arguably such an investigative capacity is necessary against terrorist funds. The question then arises as to where it should be organisationally located. The first option is to locate it within the Special Branch operations in each constabulary. This, however, would suffer from the weakness that the function might become dissipated throughout the UK. It might also be argued that Special Branch officers, particularly in smaller forces, will not always be equipped to do in-depth financial investigations since they do not carry out enough of them to develop specialist expertise.

7.20.3 A second option might be to increase the Financial Investigation Unit of the Metropolitan Police Special Branch. However, its objectives will necessarily always be influenced by the fact that the focus of the Metropolitan Police is London orientated rather than national in scope. In addition, any unit being given a national role would require other specialists and staff seconded from other agencies and these might not sit well in one police organisation. A third organisational option would be to expand the remit of the National Crime Squad to include terrorist finance. This would have the advantage of giving the responsibility to an existing national agency with a proven track record of incorporating financial investigations into criminal investigations. A fourth organisational option would be to expand the NCIS Terrorist Finance Team and grant it an investigative remit.

Intelligence gathering

7.20.4 Experiences of practitioners in all the agencies involved in counter-terrorist work vary. The following assessment covers mainly the Security Service (the Service), the Secret Intelligence Service (SIS), the National Criminal Intelligence Service (NCIS) and the various Special Branches (SB) within the UK.

---

[204] 'The Terrorist Finance Unit and the Joint Action Group on Organised Crime : New Organisational Models and Investigative Strategies to Counter "Organised Crime" in the UK', Norman P, (1998) *Howard Journal of Criminal Justice*, Vol 37, No 4, pp 375-92.

7.20.5 Since the inception of the Security Services Act in 1989, the lead agency for gathering intelligence in this field has been the Service, taking over this role from the UK's 43 Special Branches. The Service however has no executive powers and thus has to rely on Special Branches to assist it in its work, and to translate the intelligence gathered by the Service into evidence that can be presented at court. There is however no 'Special Branch Act' to give a lawful basis to the intelligence gathering undertaken by Special Branches, and this may need to be considered to ensure SB work is compliant with the Human Rights Act 2000. Presently Special Branches rely on Home Office guidelines and on powers given to the wider police, although their work is qualitatively different.

7.20.6 A possible issue here is that in any intelligence gathering operation, and in the absence of any clarity over precise roles and remits, the Security Service may be inclined to allow an investigation to run in order to maximise the intelligence they might be able to gather. The police however, in the form of Special Branch, may be inclined to take executive action once they feel there may be sufficient evidence to justify an arrest and charge. The issue here is one of 'control' and deciding which body is ultimately responsible to the British public for protecting them from terrorism.

7.20.7 There is thus a tension between the Service's responsibilities to gather intelligence and the police's duty to investigate offences and ensure the safety of the British public. In short we lack an effective and accountable decision-making or management process to control this work. It is for example an offence under the Terrorism Act 2000 to withhold evidence of terrorism from a constable, and this requires skilful handling by the Service of the terrorist intelligence they may gather.

7.20.8 Effective counter-terrorism depends greatly on quick, seamless and effective exchange of relevant intelligence as all the agencies involved in Northern Ireland learned quickly in the early 1970s. Mistakes made when individual agencies pursued their own agendas too purposefully (ignoring the potential contributions of others) led to the joint section approach – the Service and SIS pooling their resources first on Irish counter-terrorism and much later, in 1986, on Middle East counter-terrorism. This allowed the benefit of the SIS worldwide network of liaison services to flow directly into a joint unit which operated under Service disciplines in the UK and under SIS disciplines overseas.

7.20.9 In terms of international collaboration on counter-terrorism, however good the exchange of intelligence it is probably axiomatic that every nation state seeks to encourage other jurisdictions to take action which it might find problematic at home. US, French, Spanish and other countries' vexation with the UK over 'terrorists' who are allowed to speak freely at mosques and other public fora in London, Birmingham and elsewhere has been well publicised. Part of the problem has always been definition: when the Asala terrorist campaign against targets in France was at its height, the objective of the French agencies was to persuade other friendly services that all Armenian activities on their soil merited investigation and shared reporting. But not all services saw it like that. *Mutatis mutandis*, this sort of consideration has applied to many terrorist groups – which have proved ever more skilful at finding and relocating to benign environments from where they have continued planning and implementation. The constitution of al-Qaeda around Usama bin Laden and others in Afghanistan is the most extreme example of what terrorist groups have been doing in Europe and elsewhere for three decades.

7.20.10 For historical reasons, the Metropolitan Police Special Branch has national responsibility for supporting the Service's intelligence gathering, but not in cases of Irish loyalist terrorism, or for 'international' terrorism, eg Islamic extremist terrorism. To try and redress this, a new body has recently been established, the Police International Counter-Terrorist Unit (PICTU). PICTU is a police led body working within the Security Service intended to provide the National Coordinator with a vision of the Service's work with constabulary Special Branches on international terrorism. It started work on 1 April 2002, and while it is far too early to see what effect it will have, this may prove to be an ad-hoc response to a more fundamental problem.

7.20.11 In terms of international cooperation, and due to deficiencies in Interpol's constitutional arrangements, the Metropolitan Police set up the 'Special Branch European Liaison Section' under the auspices of the Trevi group to pass terrorist information directly to its counterparts in Europe, forming a group called the Police Working Group on Terrorism (PWGT). This has proved itself to be a very effective mechanism over the years. However in 1999 Europol, the European police agency set up under Third Pillar arrangements, was given a remit in the terrorist field, and has taken an interest in the work of the PWGT. According to its constitution, Europol uses NCIS as its contact point, although NCIS has no remit in the investigation of

terrorism. The PWGT has been mirrored by a similar group for intelligence services set up under the Third Pillar, notwithstanding that many agencies belong to both groups.

7.20.12 It could be argued that the entire mechanism for gathering and exploiting intelligence relating to terrorism could be revisited and restructured. Should, for example, Special Branches be placed on a national footing, possible under the auspices of NCIS? Or could the Service and Special Branches be merged into a new agency with executive powers?

Disruption

7.20.13 This is an undefined area of SB and Security Service activity, implemented when intelligence indicates unlawful activity is taking place, but in circumstances where there is insufficient evidence, or for reasons of national security the activity must be stopped as soon as possible. It can take the form of acting against such persons or groups through investigating unrelated criminal activity (eg a terrorist or spy who commits driving offences) or by letting the suspects know that the authorities are aware of their activities. It is also alleged that agencies have masqueraded as opposing criminal or terrorist groups in the hope of frightening away their targets.

7.20.14 The problem with disruption is that the activity is undefined, and thus in terms of the Human Rights Act might come close to being unlawful. There may be occasions where agencies have indulged in some of the activities outlined in the previous paragraph in circumstances that has caused their target to complain to the police. This is an area that may benefit from being governed by legislation.

Arrest and prosecution

7.20.15 In terms of investigating offences which have occurred after a terrorist incident, the responsibility lies with the Chief Constable in which the incident has occurred. However, *if invited*, the Chief Constable may call upon the services of the 'National Coordinator', and the Anti-Terrorist Branch of the Metropolitan Police, who have considerable expertise in investigating such offences. This is also an area that may benefit from being put on a national footing, but we would need to consider carefully whether Chief Constables should surrender their traditional operational autonomy to a national investigating force. This has caused difficulties in the USA, for example, resulting in disputes over primacy between local and national services.

7.20.16 The powers provided by the Terrorism Act 2000 and later acts are strong, and hopefully effective, but there are concerns within civil liberties groups over the 'certification' (internment) powers provided by the Anti-terrorism, Crime and Security Act. The Terrorism Act power to proscribe organisations has not been as effective as might have been hoped, particularly provisions on membership, and no case has been proceeded with. There is even evidence that some groups, such as *Al-Muhajiroun*, were disappointed not to have been proscribed as it detracted from their own self image.[205]

7.20.17 It is submitted that in general the present agencies involved in the field of counter-terrorism exist in a cluttered and muddled relationship, which breeds a potential for competition and inefficiency. It may be necessary for the UK to restructure its intelligence gathering and exploitation systems to clarify and simplify our response and to mirror more accurately developments at the European level. Primary legislation may be required to clarify roles and responsibilities.

The effect of human rights legislation and similar measures

7.20.18 There is no doubt that practitioners have been affected by the onward sweep of the 'rights but no responsibilities' culture. This was apparent in the 1980s when Palestinian refugee camps in Scandinavia campaigned publicly to keep the security authorities well away from them. Interpreters working in the UK in 2002 comment that even after a few weeks, asylum-seekers and clandestine immigrants who are detained know exactly how little they need to say about themselves at interview. Their right is indeed to remain silent.

7.20.19 Practitioners – who depend on human sources for intelligence on counter-terrorism – thus have a great deal more procedure to go through internally before making any sort of approach to potential sources. The environment in which they operate leaves them far less room for manoeuvre, the taking of calculated risks and independent initiatives. Most seem resigned to this new, and much more restrictive context, and argue that effective operations can still be approved and pursued. It goes without saying that the number of legal advisers working with today's practitioners has multiplied tenfold since the 1990s.

[205] Some thoughts for the SALS on the issue of counter-terrorism, Dr Paul Swallow, 20 February 2002.

7.21 Resource management

7.21.1 Well-drafted legislation without the necessary resources to carry out investigations is mere symbolism, even in culturally reformed and restructured organisations. A current difficulty is that terrorists, like their counterparts in organised crime, are often better resourced and more sophisticated than those who investigate them. The giving of additional resources to NCIS will improve the delivery of intelligence packages to agencies which have the responsibility of investigating them. However, unless these agencies receive similar increases in resources, the investigative product will not improve. Certain questions should be asked: How many staff are dedicated to investigating disclosures? If disclosures increased sufficiently after 11 September 2001, did agencies have sufficient staff to be able to examine them?

7.21.2 It has been suggested that the US authorities were deluged with thousands of reports from US banks. [206] What proportion of Special Branch resources in the UK are dedicated to tracing the finances of terrorists? Do staffing policies imply that financing of terrorism is not very important? The issue of lack of resources to investigate disclosure was raised in the House of Commons and the Chancellor admitted that the UK has so far lacked the asset tracking skills that would permit it to get at terrorist funding. [207] The need for evidence will take investigators into complex financial arrangements. This shows a need for the recruitment of specialised investigators. These are essentially management issues, requiring the recognition of a problem and the allocation of appropriate resources to it.

RESOURCES DEDICATED TO TERRORIST FINANCING

7.22 Staff dedicated to terrorist finance issues

7.22.1 Although there has been an increase in the number of staff dedicated to terrorist finance issues since 11 September it is difficult to ascertain with any precision the exact resources allocated in this field throughout the country. This is because rarely, outside of London and Northern Ireland, are police officers solely dedicated to the task.

7.22.2 The easiest part is to identify the resources that are employed full time carrying out terrorist finance investigations, although even here a note of caution is needed.

---

[206] 'US ties hijackers' money to Al-Qaeda', *The Washington Post*, 7 October 2001.
[207] *Hansard*, House of Commons, Vol 372, No 29, 15 October 2001.

Financial investigation does not mean exclusively (or even in the majority) that the purpose of the investigation is to prosecute an individual for one of the financial provisions of the Terrorism Act 2000 or to have their money confiscated under the various applicable legislative measures. The term would apply, for instance, to enquiries with a bank to establish how terrorist 'A' purchased a mobile phone. The current change of emphasis means that there is a real desire to prosecute for specific terrorist finance offences but this will never be the sole contribution that financial investigators can make against the total counter-terrorist effort.

7.22.3 The National Terrorist Financial Investigation Unit (NTFIU) of the Metropolitan Police Special Branch (MPSB), formerly known as FISAC has 26 staff either identified or in place. These consist of:

Detective Chief Inspector
Detective Inspector
Detective Sergeant x 4
Detective Constable x 15
Analysts x 2
Admin Officer x 1
plus two officers seconded to the Terrorist Finance Team (TFT) at NCIS.

7.22.4 This is an increase in staff prior to 11 September of 300%, and results partly from additional money being made available from the Treasury to increase the resources for financial investigation (£500,00 per annum for the next three years), and partly from the Metropolitan Police's Special Branch (MPSB) decision to increase resources in this field. The staff of the NTFIU all work exclusively on terrorist finance issues and are not available to be deployed elsewhere. Approximately 50% of the officers' time is spent investigating terrorist finance offences, and the rest in support of other counter-terrorist investigations.

7.22.5 The Police Service of Northern Ireland (PSNI) has four officers in its Special Branch dedicated to terrorist finance matters, and their work is apportioned similarly to the NTFIU. No other police force in the United Kingdom has dedicated terrorist financial investigators. Either financial enquires are carried out on a case by case basis by a Special Branch officer who will perform many other tasks, or the enquiry will be passed to the force's fraud or financial investigation unit which will have had an officer vetted to carry out any Special Branch enquiries.

7.22.6 Officers should attend the National Terrorist Financial Investigators' course in London (run by the NTFIU) before they undertake terrorist financial enquires. In reality some force areas are so small that trained officers have moved on before a live enquiry ever comes their way, and those that are in position do not often get the opportunity to use their skills. Indeed the impetus behind the change of name for the MPSB's financial investigation unit to the NTFIU is in recognition of the fact that the only pro-active capability rests with the NTFIU.

7.22.7 Further resources have been put into NCIS's Economic Crime Branch with the creation of the Terrorist Finance Team. This multi-agency team, which includes two secondees from the NTFIU, enhances the suspicion-based disclosures made by financial institutions under terrorist legislation or suspected by others (in sight of the intelligence picture) to be possibly terrorist related. The enhancement process produces an intelligence package that is passed to the NTFIU for further investigation.

7.22.8 The Treasury have moneys available to employ the use of 'professional' staff in terrorist financial investigations. This is likely to include solicitors and forensic accountants when a suitable investigation is identified.

7.23 Formal structure for dealing with terrorist finance issues

7.23.1 A formal structure for dealing with Terrorist Finance (TF) issues hardly existed prior to 11 September 2001. The subject was rarely treated as a stand-alone issue, but rather as a component part of the overall counter-terrorism response by the respective agencies and Government departments. Although the following will show that there is now a clear and identifiable strategy for dealing with TF issues, there remains an educational challenge to prove to some that a greater concentration in this field will yield tangible results.

7.23.2 In January 2002 the inter-agency terrorist finance review team presented their findings when they reviewed the current arrangements within the United Kingdom for countering terrorist finance and made a number of recommendations. Out of these recommendations came a more formal structure. The importance with which government views TF issues is evident by the fact that a Cabinet Office sub-committee has been created specifically to deal with this matter .

Official Committee On Domestic And International Terrorism (Terrorist Financing) [TIDO(TF)]

7.23.3 This committee was established to provide co-ordination and monitoring of UK efforts for countering terrorist financing. TIDO(TF) reports to and receives direction from the Ministerial Group on Protective and Preventative Security (DOP(IT)(T)) at which the Chairman of the Association of Chief Police Officers (Terrorism and Allied Matters Committee) (ACPO (TAM)) is the police representative. TIDO(TF) has established three sub-groups :

- The Investigative Planning Group
- The Financial Sanctions Group
- The Financial Services Contact Group

The Investigative Planning Group (IPG)

7.23.4 The IPG is an inter-agency co-ordinating group and will enhance terrorist financial investigations by:

- Ensuring effective multi-agency working to select, prioritise and progress financial investigations;
- Using financial investigations as part of the analysis of terrorist groups and identifying opportunities for enforcement and disruption;
- Providing feedback to TIDO (TF) on areas for development in priorities, co-ordination and legislation;
- Providing input to the Financial Sanctions Group and the Financial Services Contacts Group
- Providing a forum in which problems can be raise and resolved where possible.

7.23.5 The IPG is chaired by the Security Service, with the Metropolitan Police Special Branch (MPSB) National Terrorist Financial Investigation Unit (formerly FISAC) as the deputy-chair. NCIS Terrorist Finance Unit, GCHQ, SIS, HMCE and PSNI are also represented. Associate members from other government departments are invited where necessary.

The Financial Sanctions Group (FSG)

7.23.6 The FSG will be chaired by HM Treasury and will provide a formal framework for asset freezing and financial sanctions by:

- Agreeing which terrorist organisations and individuals will be subject to UK financial sanctions;
- Providing UK policy on multi-lateral action on financial sanctions against terrorists; and
- Informing and advising TIDO(TF) about policy issues arising from financial sanctions against terrorists;
- Identifying and ensuring compliance with UK and international law and to allies.

7.23.7 It is intended that the FSG will meet quarterly or as needs dictate. Policy responsibility for sanctions in general and asset freezing in particular would continue to be a matter for HM Treasury.

The Financial Services Contact Group

7.23.8 This Group will be chaired by the Terrorist Finance Team at NCIS, will meet quarterly and has been established to:

- Enhance the value of financial disclosures made to NCIS;
- Provide a forum for co-ordinating and facilitating effective information flows between law enforcement agencies and the financial services industry;
- Develop terrorist financial typologies for dissemination

7.24 Police arrangements

Terrorist Finance Team (TFT)

7.24.1 The TFT was formed in the immediate aftermath of 11 September as a multi-agency team, which provides the primary point of contact for financial disclosures made under terrorist legislation. The TFT comprises personnel from NCIS, NTFIU, the security and intelligence agencies, and the Financial Services Authority, and forms part of the Economic Crime Branch at NCIS working in support of existing structures.

7.24.2 The TFT has two key functions:

- Screening and enhancing financial disclosures received, for allocation to NTFIU for investigation; and
- In partnership with NTFIU, implementing the strategy for building closer working relationships with the industry and sharing typologies on terrorist financing.

National Terrorist Financial Investigation Unit (NTFIU - formerly FISAC)

7.24.3 The NTFIU is the only dedicated police unit that looks at terrorist financing on the mainland and provides training nationally for other police force's financial investigators which is intended to raise awareness of the additional powers available under terrorist legislation. Since 11 September there has been a significant increase in the number of staff allocated to terrorist financial investigations. In line with the 1994 'Home Office Guidelines on Special Branch Work', financial investigations under terrorism legislation were undertaken by FISAC (the 'Financial Investigation and Special Access Centre'). Following a review, the name of the Unit has been changed to the National Terrorist Financial Investigation Unit to more accurately reflect its national co-ordinating role. It is the sole customer of the TFT and increasingly is working with the Security Service in exploiting financial intelligence nationally. The NTFIU works increasingly with EUROPOL and the FBI and US Customs Service. Its staff also regularly represents the United Kingdom at international working groups and conferences around the world. The NTFIU prepares many papers for government and the Association of Chief Police Officers on a wide range of terrorist financing issues.

7.25 International co-operation

7.25.1 Individual terrorist finance investigations will often require close international co-operation. Even terrorists whose violent activities are restricted to one country may be funded by supporters in another or may attempt to conceal its funds outside the country in which it acts. In 1992 the Chief Constable of the RUC noted that investigators in this field in his force were in regular contact with police forces and other investigative agencies in the UK, Ireland, Canada and the United States. [208]

[208] Report of the Chief Constable, 1992, page 32.

This shows the need for financial intelligence units to pass relevant disclosures to partner jurisdictions for terrorist finance investigations.

7.25.2 The recognition of the need for global action is evidenced by the fact that a special plenary of the Financial Action Task Force was quickly arranged to agree the imposition, enforcement and monitoring of new international standards to combat terrorist finance. [209] A special set of FATF recommendations has now been issued. [210] The Basle Committee on Banking Supervision [211] has also revisited the issue of terrorist finance. The FATF will undoubtedly be used as one of the organisations to put pressure on countries to introduce money laundering reform, following on from the considerable success it has had with its report on non-co-operative countries and territories report. Such reform may, however, be general money laundering reform rather than reform relating to terrorist finances specifically.

7.25.3 The issue of terrorist finance is now much closer to the top of many political agendas compared to the position prior to 11 September, when the United Nations Convention on the Suppression of the Financing of Terrorism had only been ratified by four countries. Indeed, the process of introducing uniform international standards on money laundering has now been described as unstoppable. [212] Nevertheless the influence of financial sector represents a powerful lobbying force which may yet frustrate reform, particularly when US politicians seek fundraising for re-election campaigns. [213]

7.25.4 Other political issues arise. Gulf States may resent Western insistence on greater regulation of matters which touch on traditional attitudes to religion and business methods. [214] The USA has acknowledged that tackling possible terrorist fundraising through Islamic charities, particularly those in Saudi Arabia, involves difficult political issues. [215]

7.25.5 There are particular implications for jurisdictions which permit bank secrecy. Following the 11 September attacks, the Chancellor of the Exchequer urged that countries such as Switzerland which have traditionally valued bank secrecy must

---

[209] *Hansard*, House of Commons, Vol 372, No 29, 15 October 2001.
[210] 'Guidance for Financial Institutions in Detecting Terrorist Financing', FATF, Paris, April 2002.
[211] 'Banks urged to step up anti-money laundering efforts', *The Financial Times*, 4 October 2001.
[212] 'Cleaning up', *The Financial Times*, 21 September 2001
[213] 'The war on special interests', *Salon*, 4 October 2001.
www.salon.com/tech/feature/2001/10/4/banking_lobby/index.html
[214] 'Arabia bridles at Americans' insistence on al-Qaeda cash', *The Financial Times*, 21 February 2002.
[215] 'Complex finances defy global policing', *The Financial Times*, 21 February 2002.

now accept the need 'to report suspicious transactions involving what may be terrorist activities.' [216]

[216] 'Swiss are urged to lift bank secrecy', *The Times*, 20 September 2001.

WORKING GROUP MEMBERS*

CRITICAL REVIEW OF TERRORIST-RELATED LEGISLATION AND THE MONITORING OF NEW LEGISLATION

Chair: Sir Ivan Lawrence QC
Barrister, 2 Paper Buildings

Convenor: Dr Kern Alexander
Butterworths Senior Research Fellow, Institute of Advanced Legal Studies, University of London

Members: Mr Enrique Hernandez Sierra
Embassy of Uruguay

Mr M Khawar Qureshi
Barrister, Serle Court

IMPACT OF THE INITIATIVES AGAINST TERRORIST PROPERTY ON BANKS AND FINANCIAL INSTITUTIONS

Chair: Mr Richard Jones QC
Barrister, 3 Hare Court

Convenors: Miss Caroline Foster
Compliance Officer – Technical, Edward Jones Limited

Dr Chizu Nakajima
Director, Centre for Financial Regulation, City University Business School

Members: Mr Mark Anderson
KPMG

Dr Ilias Bantekas
Senior Lecturer & Director, International Law Unit, University of Westminster School of Law

Mr Aidan Casey
3 Hare Court

Mr Richard Collins
Group Compliance Director, Lloyds TSB

Mr Chris Cook
Business Consultant, Enfocast

Mr Jason Haines
Research Fellow in Financial Services Law
Insitute of Advanced Legal Studies

Mr James Ingmire
Solicitor, Allen & Overy

Mr Sebastian Mansfield-Steer
Business Information Group - Legal Department, Goldman Sachs International

Mr David McCluskey
Solicitor, Peters & Peters

Mr Sidney Myers
Partner, Allen & Overy

Ms Emmanouela Mylonaki
Birkbeck College

Ms Yoko Nishida
University of Westminster

Ms Helen Parry
Senior Lecturer, London Guildhall University

Mr Arun Srivastava
Solicitor, Baker & McKenzie

IMPLICATIONS OF INVESTIGATIONS AND ENFORCEMENT: INTERNATIONAL COOPERATION ASPECTS

Chair: Detective Superintendent Nicholas O'Brien
SO12, Metropolitan Police

Convenors: Mr Tarrant Green FCA
Institute of Advanced Legal Studies

Mr Jason Haines
Research Fellow in Financial Services Law
Insitute of Advanced Legal Studies

Members: Dr Robert Evan Bell
Senior Legal Adviser, Office of the Director of Public Prosecutions of Northern Ireland

The Hon Justice Evans-Lombe
Royal Courts of Justice

Mr Edwin Jefferson
Police Service of Northern Ireland

Detective Inspector Cliff Knuckey
Anti Money Laundering Unit, Metropolitan Police

Professor Mike Levi
Professor of Criminology, Cardiff University

Mr Alistair Munro
Deloitte & Touche

Detective Chief Inspector Stephen Ratcliffe
Head, National Terrorist Financial Investigation Unit

Mr Michael Reynolds
Hakluyt & Co

Mr Graham Saltmarsh
Senior Partner, The Charles Hill Partnership

Dr Paul Swallow
SO12, Metropolitan Police

Mr William Tupman
Senior Lecturer, Department of Politics, University of Exeter

IMPACT OF THE INITIATIVES ON OTHER AREAS OF THE LAW

Chair: The Hon Judge Diana Faber
Wood Green Crown Court

Convenors: Dr Charles Mitchell
King's College London

Dr Cheong Ann Png
Associate, Herbert Smith

Members: Mr Richard Earle
Senior Lecturer, University of Westminster

Mr Joseph Lee
Institute of Advanced Legal Studies, University of London

Mr Paul Marshall
Barrister, 3 Hare Court

*These lists are as provided by each Subgroup Convenor at August 30th 2002

The Society for Advanced Legal Studies
17 Russell Square
London WC1B 5DR

Tel: 020 7862 5865 Fax: 020 7862 5855 Email: sals@sas.ac.uk