<table>
<thead>
<tr>
<th>CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction</strong> 03</td>
</tr>
<tr>
<td><strong>Proceeds of crime</strong> 04</td>
</tr>
<tr>
<td>• What is money laundering? 04</td>
</tr>
<tr>
<td>• The UK’s anti-money laundering strategy 05</td>
</tr>
<tr>
<td>• The legal and regulatory framework – <em>Proceeds of Crime Act 2002</em> 06</td>
</tr>
<tr>
<td>• Principal offences under POCA 06</td>
</tr>
<tr>
<td>• <em>Terrorism Act 2000 and Anti-terrorism, Crime and Security Act 2001</em> 06</td>
</tr>
<tr>
<td>• What might a suspicious transaction look like? 07</td>
</tr>
<tr>
<td>• What should intermediaries do to protect themselves? 09</td>
</tr>
<tr>
<td>• Handling cash 09</td>
</tr>
<tr>
<td>• The Suspicious Activity Reporting (SAR) regime 10</td>
</tr>
<tr>
<td>• What to do when suspicions are aroused? 10</td>
</tr>
<tr>
<td>• Penalties 11</td>
</tr>
<tr>
<td><strong>Bribery and corruption</strong> 12</td>
</tr>
<tr>
<td>• What is it? 12</td>
</tr>
<tr>
<td>• The UK’s legal and regulatory framework 12</td>
</tr>
<tr>
<td>• Protecting your business 13</td>
</tr>
<tr>
<td><strong>Sanctions</strong> 14</td>
</tr>
<tr>
<td>• What are they? 14</td>
</tr>
<tr>
<td>• Who issues sanctions? 14</td>
</tr>
<tr>
<td>• Sanctions administration in the UK 14</td>
</tr>
<tr>
<td>• What should general insurance intermediaries be doing? 14</td>
</tr>
<tr>
<td><strong>Information security</strong> 15</td>
</tr>
<tr>
<td>• Personal data is big money for the criminal 15</td>
</tr>
<tr>
<td>• Staying safe online 16</td>
</tr>
<tr>
<td>• The wider picture for information security 17</td>
</tr>
<tr>
<td><strong>Fraud</strong> 18</td>
</tr>
<tr>
<td>• How big is the problem? 18</td>
</tr>
<tr>
<td>• Types of fraud 19</td>
</tr>
<tr>
<td>• <em>The Fraud Act 2006</em> – new hope? 19</td>
</tr>
<tr>
<td>• The response to fraud 20</td>
</tr>
<tr>
<td>• Reporting fraud 21</td>
</tr>
<tr>
<td>• The internal threat – employee risks 22</td>
</tr>
<tr>
<td><strong>Useful links for further information</strong> 23</td>
</tr>
</tbody>
</table>
The repercussions of financial crime are far-reaching, ranging from the highly visible economic losses that businesses may suffer as a result of being targeted, through to the less tangible, but often as important, damage to reputation and adverse effects on staff morale and recruitment. The time and additional costs associated with having to investigate or recover from an incident can also be very high.

There are no reliable figures about the scale of financial crime, but it is estimated to cost billions of pounds every year, damaging both business and consumers in the process. The general perception among industry practitioners in all sectors is that financial crime is on the increase, although how much of this is due to better detection methods and raised awareness of the issue, as opposed to an actual rise in the number of crimes being committed, is open for debate. What is without doubt is that criminals are becoming increasingly organised and using ever more sophisticated techniques to commit financial crime.

The Financial Services Authority (FSA) has a statutory objective to reduce financial crime. Section 6 of the Financial Services and Markets Act 2000 requires the FSA to aim to reduce the extent to which regulated persons and unauthorised businesses can be ‘used for a purpose connected with financial crime’. This financial crime objective is very broad in scope, as it encompasses not only money laundering (which includes terrorist financing) and fraud in its many guises, but also market misconduct and other crimes, such as corruption and breaking sanctions.

The FSA, in pursuing its financial crime objective, focuses on firms’ risk management, systems and controls. The emphasis is on the senior management of firms to ensure that their businesses are sufficiently well-controlled and structured so as to prevent them being used by criminals or terrorists.

This publication is not intended to provide prescriptive guidance for your firm and should not be seen as a substitute for seeking your own professional advice, if needed. The guide aims to raise awareness among BIBA members about the internal and external risks that may expose their businesses to financial crime and some of the steps they can take to protect themselves.

Any measures put in place to tackle financial crime should always be risk-based and proportionate – taking into account the size, complexity and structure of the firm implementing them.
Financial institutions view payments originating from insurance companies as commonplace, the money is assumed to be clean and does not attract attention. If money launderers can place criminal funds into an insurance policy, then they will have made significant steps in layering and integrating funds into the international financial system.

Historically, there has been the perception that general insurance products offer criminals little opportunity to launder money. Unfortunately, this view has led to insurance being seen as a soft target for criminals and complacency among some firms in developing robust policies to deter and detect money laundering in their businesses.

The perception that the general insurance sector presents a low risk of being used by criminals for money laundering is now fading. The size, structure and global nature of the insurance industry, combined with the easy availability and diversity of its products means that it is clearly vulnerable. Criminals will look for opportunities in insurance products to launder their proceeds, often using the knowledge of insiders within the industry to assist them.

What is money laundering?

Money laundering is the term used to describe the techniques, procedures and processes used to convert the proceeds of crime into other assets in an effort to disguise their true origin. Once these proceeds are successfully laundered, the criminal may enjoy their use without revealing the original illegal source of the money.

The term laundering comes from the process of turning ‘dirty’ money into ‘clean’ money. There are three basic stages in the money laundering process, which are as follows:

**Placement**

The proceeds of a crime normally take the form of cash and the aim of the criminal at this stage is to move the cash into the non-cash economy.

E.g. the money launderer makes a cash payment to a broker to purchase an insurance policy.

**Layering**

Once cash has been placed in the financial system, a variety of methods are used to confuse the audit trail, often by passing transactions through several stages (layering), each one making it more difficult to trace the true origin of the funds and appear more legitimate.

**Integration**

This is the final stage in the process which is to introduce the now apparently ‘legitimate’ money back into the mainstream economy in a way that makes it appear as if they were legitimate funds.

E.g. the money launderer using the money received from an insurance claim to buy property.
The UK’s anti-money laundering strategy

The UK’s approach to anti-money laundering aims to be risk-based and proportionate; which essentially means directing resources where the risk is greatest.

The Serious Organised Crime Agency (SOCA) is at the forefront of the fight against serious organised crime including money laundering. The agency was established by the Serious Organised Crime and Police Act 2005 (SOCPA) and amalgamated the National Crime Squad, National Criminal Intelligence Service and parts of HM Customs and Excise and the Immigration Service.

The Financial Action Task Force (FATF) is an inter-governmental body which aims to develop and promote national and international policies to combat money laundering and terrorist financing. It sets international standards for anti-money laundering and counter terrorist financing (CTF) controls through a number of recommendations that require countries to establish laws to combat, control and investigate money laundering, terrorist financing and asset recovery.

Countries must establish a Financial Intelligence Unit (FIU) to receive, analyse and disseminate suspicious activity reports (SARs) relating to money laundering and terrorist financing and provide a link between the reporting sector and investigating agencies.

The UK Financial Intelligence Unit sits within SOCA and strives to protect the UK from money laundering and terrorist financing. It also provides opportunities for the authorities to recover criminal and terrorist property and thereby to reduce the harm to the UK caused by criminality and terrorism.

Countries must establish a Financial Intelligence Unit (FIU) to receive, analyse and disseminate suspicious activity reports (SARs) relating to money laundering and terrorist financing and provide a link between the reporting sector and investigating agencies.
Legal and regulatory framework – Proceeds of Crime Act 2002

The current legislation that criminalises money laundering in the UK is the Proceeds of Crime Act 2002 (POCA) (sections 327-340). The Money Laundering Regulations 2007 also define and impose requirements on those conducting ‘relevant business’ to have systems and controls in place to obtain evidence of the identity of their clients, keep records, train staff, make internal reports and appoint a ‘nominated officer’ to whom knowledge or suspicion of money laundering should be reported and who will make reports to the necessary authorities. The FSA is responsible for monitoring firms’ compliance with the Money Laundering Regulations.

The Joint Money Laundering Steering Group, which is made up of a number of trade associations from the UK’s financial services industry, gives practical assistance in how to interpret the Money Laundering Regulations in the form of guidance.

Principal offences under POCA

The relevant provisions of POCA set out the three principal money laundering offences, which are all concerned with the actual use of, or dealing with criminal property:

- **Section 327** concealing, disguising, converting, transferring or removing from the jurisdiction (defined as England and Wales, Scotland or Northern Ireland) criminal property.
- **Section 328** entering into or becoming concerned in an arrangement that you know or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another.
- **Section 329** the acquisition, use or possession of criminal property unless for an adequate consideration.

Criminal property is widely defined as any property that constitutes a person’s benefit from criminal conduct, or represents such a benefit and a person knows or suspects it constitutes or represents such a benefit. Criminal conduct includes tax evasion and benefit fraud.

Insurers, brokers and intermediaries working exclusively in the general insurance market are not covered by the Money Laundering Regulations. This does not, however, mean that they are free from any regulatory obligations where money laundering is concerned.

They could commit money laundering offences contrary to POCA where they know, or suspect, that one of their clients is engaged in money laundering. Making a timely report to the relevant authority where it is known or suspected that another person is engaged in money laundering and receiving consent to proceed with the suspicious transaction could give a firm or an individual a full defence to a potential money laundering charge.


The **Terrorism Act** establishes a series of offences related to involvement in arrangements for facilitating, raising or using funds for terrorism purposes.

The Act:
- makes it a criminal offence for any person not to report the existence of terrorist property where there are reasonable grounds for knowing or suspecting its existence
- makes it a criminal offence for anyone to take any action likely to prejudice an investigation by informing (i.e. ‘tipping off’) the person who has been made the subject of a suspicion report, or anybody else, that a disclosure has been made to a nominated officer or to SOCA, or that the police or customs authorities are carrying out or intending to carry out a terrorist financing investigation
- grants powers to the law enforcement agencies, similar in scope to that introduced under POCA.

The **Anti-terrorism, Crime and Security Act 2001** gives the authorities power to:
- seize terrorist cash,
- to freeze terrorist assets and
- direct firms in the regulated sector to provide the authorities with specified information on customers and their (terrorism-related) activities.
What might a suspicious transaction look like?

FATF produced a report in 2005, chapter two of which was devoted to money laundering vulnerabilities in the insurance sector. The report set out nine common ways in which the insurance sector and its products can be used for money laundering purposes. These typologies were drawn from a collection of real-life incidents of money laundering from various jurisdictions around the world.

It also produced a broad set of indicators which, if present in a transaction, might give rise to money laundering in the insurance sector. These indicators are divided into four broad areas:

- indicators not unique to the insurance industry
- policyholder characteristics and behaviours
- policy characteristics and policy maintenance
- other indicators.

The FATF list of indicators are summarised as follows:

**Indicators not unique to the insurance industry**
- large one-off cash transactions
- use of a false address or post office boxes
- overseas business from higher risk jurisdictions.

**Policyholder characteristics and behaviours**
- where the policyholder is a known criminal, or a relative or an associate of a known criminal
- erratic or abnormal behaviour by the policyholder
- high premium payments compared to verifiable legitimate income
- lack of concern by the policyholder over charges/early redemption costs
- the policyholder’s undue interest in early payout options
- change of beneficiary
- general insurance coverage for assets of a value that appears inconsistent with the customer’s economic profile
- early or suspicious claims in general insurance.

**Policy characteristics and policy maintenance**
- policy payments made by third parties
- multiple sources of funds to pay premiums
- significant premium top-ups to a policy
- overpayment of premium, particularly where followed by a request for repayment to be made to a third party and/or another jurisdiction
- using an insurer like a bank to move funds around
- early redemption of the policy.

**Other indicators**
- unusually high commission charges
- involvement of recently established insurance or reinsurance companies or companies whose background does not appear particularly transparent.
Brokers and intermediaries are often perceived as a weak link in the insurance industry’s anti-money laundering efforts, as they often lack knowledge or fail to take money laundering seriously.
What should intermediaries do to protect themselves?

As the Money Laundering Regulations become more effective and those within the regulated sector become more proficient at protecting their organisations against such activities, criminals are increasingly turning their attention to those in the business community who are outside the money laundering regulations.

Brokers and intermediaries are often perceived as a weak link in the insurance industry’s anti-money laundering efforts, as they often lack knowledge or fail to take money laundering seriously; they could also be unduly influenced by the pressures of competition or approaches from criminals.

Firms may adopt measures to identify and prevent money laundering by:

- establishing and implementing policies and controls to guard against products being used by clients to launder funds
- ensuring the source of a client’s funds is identifiable
- being able to verify the customer’s identity using reliable, independent source documents, data or information and understand their normal activities. This is referred to as Customer Due Diligence (CDD), it is also known as Know Your Customer (KYC). Intermediaries always need to consider the complete relationship that they have with the customer to detect any ‘unusual activity’; do not look at individual actions in isolation
- ensuring staff understanding and awareness of money laundering and the risks of committing a criminal offence. BrokerASSESS has a module to help staff improve their knowledge of what constitutes money laundering and how intermediaries may be targeted
- training staff to recognise suspicious activity and know who to report these matters to within the organisation. Training should be on a regular basis to ensure that staff are made aware of any changes in their responsibilities
- having procedures in place to record suspicious activity and report it to SOCA.

Handling cash

A customer paying a premium in cash provides potential for the intermediary to be used as a vehicle for money laundering. Criminals can deposit ‘dirty’ money along with a firm’s legitimate deposits thereby completing the first step of the money laundering process. The most obvious response to the threat would be for the intermediary to stop taking cash from clients and only allow payment by cheque, debit/credit card or direct debit/standing order, as money arriving through these types of transactions will already have had some form of vetting by the financial institution providing them.

However, ceasing to accept cash is not always feasible. Intermediaries may wish to consider setting up procedures for accepting cash payment from clients in order to minimise the threat from money laundering. They may want to set a level of cash payment by the customer below which staff need not take any action and a maximum level above which no cash payments will be accepted. In between those two levels firms may want to apply particular vetting requirements to customers, for example:

All new private customers
- obtain a photocopy of original ID such as a passport or photo driving licence and a current utility, council tax or credit card bill (again they must be originals, not copies printed off from the internet).

All new commercial customers
- details of the full name of the company, its activities and business address
- the registered number, registered office of country or incorporation, the business address for corporate firms
- names of directors (or equivalent) and names of beneficial owners holding more than 25 per cent for private firms/unlisted companies.
It is important to remember existing customers could be just as likely to be engaged in suspicious activities as new ones if their background has not been checked. Just because a certain function, process or behaviour is longstanding, does not necessarily mean that is correct, lawful or above suspicion. Firms should remain vigilant and may want to carry out regular checks during the course of a business relationship to ensure that the customer remains the sort that they want to retain.

Suspicious Activity Reporting (SAR) regime
The Suspicious Activity Reporting (SAR) regime is a central element in the UK’s anti-money laundering offensive; it provides individuals and businesses with a defence to the principal money laundering offences if they report instances of money laundering and suspicious activity to the authorities.

POCA establishes two distinct regimes for suspicious activity reporting (ss.330-338). In the first, section 330 of POCA requires institutions in the regulated sectors (those subject to the Money Laundering Regulations) to disclose information (in the form of a SAR) where they know or suspect or have reasonable grounds to know or suspect money laundering. Those involved in the life, pensions and investment side of the insurance industry are part of the regulated sector.

The second regime allows persons and businesses generally – not just those in the regulated sectors – to avail themselves of a defence against money laundering charges by making an authorised disclosure to SOCA.

The Act states that a firm should make a disclosure before an act of money laundering takes place and that the consent of the authorities to undertake an activity including completing a transaction (a ‘prohibited act’), about which they have concerns should be sought. A disclosure can be made after the prohibited act provided there was good reason for the failure to disclose before the act took place and the disclosure was made on the reporter’s own initiative as soon as practicable.

What to do when suspicions are aroused?
Suspicions or unease about a transaction should be reported immediately. Full details should be reported to the central point of contact within the firm who may well be the money laundering reporting officer. The person making the initial report within the firm must be careful not to discuss their suspicions with anyone else as this could ‘tip off’ (POCA sections 333 and 342) the individual or business that they are under investigation, which is a criminal offence.

It is also vital that the customer is not made aware (either directly

"Suspicions or unease about a transaction should be reported immediately. Full details should be reported to the central point of contact within the firm who may well be the money laundering reporting officer"
or indirectly) that suspicions about their activities have been reported. The customer must be allowed to continue their relationship with the firm normally, unless specifically advised otherwise. Failure to maintain confidentiality may leave an individual/firm open to criminal prosecution, resulting in imprisonment and/or a fine.

The nominated person within the firm will then take the necessary action. This could involve them making a Suspicious Activity Report to SOCA. The preferred method of reporting is via SAR Online, SOCA’s web-based reporting mechanism which provides a free secure method of reporting suspicious activity. Reports submitted in this way are acknowledged by an automated email of receipt providing a reporter with the reassurance that their information has been received.

SOCA does not acknowledge receipt of posted or faxed reports. Registration for SAR Online is a simple process and can be accessed from the website www.soca.gov.uk. There is online help with registration and a telephone helpline during office hours.

SOCA has seven days in which to consider a SAR and decide whether to grant consent for a transaction to go ahead (POCA section 336). During this period, a firm should make itself available in case SOCA needs to discuss a report with it. If the person who initially made the report is unavailable the firm should make sure that there is someone else available who is able to discuss the case intelligently with SOCA in their absence.

Records of all disclosures should be made. Where it was decided not to make a disclosure, the nominated person within the firm should make a record of their reasons for not making a report to SOCA.

Penalties
Failure to comply with the requirements under POCA can result in serious consequences (see table below).

<table>
<thead>
<tr>
<th>Breach</th>
<th>Maximum Punishment</th>
</tr>
</thead>
<tbody>
<tr>
<td>General breach of Money Laundering Regulations</td>
<td>2 years’ imprisonment and/or a fine</td>
</tr>
<tr>
<td>Assisting a money launderer to conceal/steal where the person is aware/suspects criminal activity</td>
<td>14 years’ imprisonment and/or a fine</td>
</tr>
<tr>
<td>Tipping off (informing a third party that they are under investigation)</td>
<td>5 years’ imprisonment and/or an unlimited fine</td>
</tr>
<tr>
<td>Failure to report a suspicion or knowledge of money laundering</td>
<td>5 years’ imprisonment and/or an unlimited fine</td>
</tr>
<tr>
<td>Destroying or disposing of relevant documents</td>
<td>5 years’ imprisonment and/or an unlimited fine</td>
</tr>
</tbody>
</table>

*Proceeds of Crime Act 2002: penalties for breach*
What is it?

Bribery and corruption are significant problems worldwide. Bribery and corruption distorts competition and investment, impedes free and fair trade, and places an unacceptable burden on business and society trapping many in poverty.

The UK’s Foreign and Commonwealth Office defines bribery broadly as the receiving or offering/giving of any benefit (in cash or in kind) by or to any public servant or office holder or to a director or employee of a private company in order to induce that person to give improper assistance in breach of their duty to the government or company which has employed or appointed them.

Bribes may also be paid to individuals who, although not holding an appointment in a relevant company or national government, can exert influence over such an appointee by reason of some personal, business or other relationship.

Bribes may be paid in advance as an inducement or once the ‘favour’ has been carried out.

The UK’s legal and regulatory framework

The UK’s legislative framework against bribery and corruption is complex and in addition to common law offences corruption offences are found in at least 12 statutes: The main statutes are the Public Bodies Corrupt Practices Act 1889 and the Prevention of Corruption Act 1906 as supplemented by the Prevention of Corruption Act 1916 and the Anti-terrorism, Crime and Security Act 2001 (which extends jurisdiction to overseas corruption).

The UK is a signatory to a number of international initiatives designed to stamp out corruption. UK law also makes it illegal to bribe foreign public or private officials or office holders. Any UK national or company can be prosecuted in the UK for this crime – even if no part of the offence took place here. Failure to comply is punishable with an unlimited fine and/or up to seven years’ imprisonment.

The FSA takes these matters very seriously, as corruption poses a direct risk to its statutory objectives. Firms which employ corrupt practices are also in breach of PRIN 2.1.1 and are liable to regulatory action. The FSA’s Wholesale and Institutional Markets team wrote to a number of firms in November 2007, expecting them to review their business practices and controls to minimise the risk that the firm makes, or will make, illicit payments either directly or indirectly to, or on behalf of, third parties and to bring to the FSA’s attention anything relating to such a review of which they would reasonably expect notice.
Protecting your business

The failure to put in place adequate anti-bribery controls exposes firms to significant legal and regulatory risks.

The Department of Business, Enterprise & Regulatory Reform suggest a number of steps that businesses can take to combat bribery and corruption:

• identify the jurisdictions and business sectors which pose the greater threat to your operations
• draw up an anti-corruption and anti-bribery policy
• communicate anti-bribery policy to staff and make breaching that policy a disciplinary matter
• detail the procedures that staff should follow during business transactions and what to do in the event that they should be offered a bribe or asked to make one
• prohibit the offer, giving or acceptance of bribes, gifts, hospitality or expenses by employees or other parties involved that could influence the outcome of a business transaction
• prohibit all donations to charities or political parties to obtain a business advantage
• report any evidence of a foreign rival company acting corruptly to the local judicial authorities and/or the authorities of the country where the company is registered
• always keep accurate records of business transactions in order to be able to show that they have been carried out fairly and within the law.

Transparency International, a global civil society organisation leading the fight against corruption, has developed a series of publications aimed at helping businesses develop an anti-bribery policy. It has produced a six-step programme for small and medium sized business, which can be found at the link: www.transparency.org/content/download/29197/443933/file/BusinessPrinciples_SME30Jan2008.pdf

The guide may also assist larger businesses in encouraging SMEs in their supply chain to implement no-bribes policies and practices.
**What are they?**

Economic, trade and financial sanctions are normally used by the international community for one or more of the following reasons:

- to bring about a change in the behaviour of a target country or regime
- as an enforcement tool in cases where international peace and security has been threatened and diplomatic efforts have failed
- to prevent and suppress the financing of terrorists and terrorist acts.

The range of sanctions that can be applied include comprehensive economic and trade sanctions and/or more targeted measures such as arms embargoes, bans on targeted individuals travelling, and financial or diplomatic restrictions. Financial sanction measures can vary from the comprehensive – prohibiting the transfer of funds to a sanctioned country and freezing the assets of a government, the corporate entities and residents of the target country – to targeted asset freezes on individuals/entities. Funds and assets are very widely defined and can include the benefits flowing from insurance policies, returned premiums or claims payments.

**Who issues sanctions?**

The increasing emphasis on sanctions, both at home and abroad, is likely to result in governments looking more closely at what financial services firms are doing to comply with them. The sanctions that BIBA members are most likely to be affected by are those imposed by the HM Treasury, the European Union, and the United Nations. Those doing business in America will have the US Treasury Department’s Office of Foreign Assets Control (OFAC) to contend with.

**Sanctions administration in the UK**

In the UK, the Foreign & Commonwealth Office is responsible for overall policy on international sanctions, including the scope and content of international sanction regimes.

The Department for Business, Enterprise and Regulatory Reform is the UK department responsible for trade sanctions. Responsibility for administering financial sanctions in the UK lies with HM Treasury.

The UK sanctions regime applies to any person or entity within the UK and to UK citizens and entities abroad. Breaching those rules is a criminal offence and can result in imprisonment (up to seven years) and/or a fine.

The Asset Freezing Unit at the Treasury acts as the single point of contact on financial sanctions. The Treasury maintains a consolidated list of targets listed by the UN, European Union and UK under legislation relating to current financial sanctions regimes. This list includes all individuals and entities that are subject to financial sanctions in the UK and can be found at: [www.hm-treasury.gov.uk/documents/financial_services/sanctions/sanctions_index.cfm](http://www.hm-treasury.gov.uk/documents/financial_services/sanctions/sanctions_index.cfm)

Firms can sign up to a free subscription service to receive an email alert as soon as a new financial sanction has been added to the Treasury’s website. This can be done by sending an email to:

**Firms can sign up to a free subscription service to receive an email alert as soon as a new financial sanction has been added to the Treasury’s website. This can be done by sending an email to:**

AFUsubscribe@hm-treasury.gov.uk with the words **SUBSCRIBE SANCTIONS** in the subject field.

**What should general insurance intermediaries be doing?**

There are no specific statutory or regulatory obligations for general insurance intermediaries to check their customers’ names against the Treasury sanctions lists. However, one look at the ostensibly ordinary lifestyles of those individuals involved in the London bombings in July 2005 should be sufficient to counter the argument that an intermediary conducting business solely in the UK with local residents cannot be aiding terrorism.

Intermediaries would do well to check customers against the lists in order to avoid committing an offence of non-disclosure. In the event that a customer is found to be the target of financial sanctions then the account must be frozen and a report made to the Asset Freezing Unit at the Treasury. All enquiries regarding financial sanctions should be made to the following address:

**Asset Freezing Unit**

**HM Treasury**

**1 Horse Guards Road**

**London**

**SW1A 2HQ**

**Telephone:** 020 7270 5454

**Email:** assetfreezingunit@hm-treasury.gov.uk

Be aware that some of the names on the sanctions lists are fairly generic, the Asset Freezing Unit will be able to provide guidance in the event of a possible match.
The advent of mass digital communication through the internet has been a huge boon to business, allowing it to manipulate information and reach customers in ways never imagined 20 or 30 years ago. Unfortunately, criminals have also been quick to embrace this technology in order to gain access to confidential customer information.

Personal data is big money for the criminal

Individuals are becoming more careful about disclosing their personal information online so as to avoid becoming the victims of identity theft and they are increasingly keen to know how their data is being used by the financial services community.

Taking care of personal confidential information held in relation to customers has never been more important. The FSA fined Norwich Union £1.26m in December 2007 for information security lapses, demonstrating the importance of keeping customer data safe.

Financial services companies have a duty to protect personal information under the Data Protection Act 1998 (DPA). The Criminal Justice and Immigration Act 2008 gives the Information Commissioner’s Office, the privacy regulator, powers to impose substantial fines on organisations that deliberately or recklessly commit serious breaches of the DPA.

The FSA also requires firms to take reasonable care to put in place and maintain robust systems and controls to ensure that their customers’ data do not fall into the wrong hands and are used for financial crime purposes (SYSC 3.2.6R). Data security also forms an important part of any firm’s treating customers fairly programme.

In April 2008, the FSA published the results of a major thematic work looking at firms’ systems and controls around personal customer data. The review found that many firms still had yet to fully appreciate just how damaging data loss and fraud is to their businesses and especially their customers. This included senior management at firms not recognising the value of their customers’ data to fraudsters or that staff could pose as big a threat to data security as computer hackers and burglars.

The report includes 16 pages of examples of both good and bad practice against which members
could benchmark their own systems and controls and take steps to improve them where necessary. The report can be accessed at: www.fsa.gov.uk/pubs/other/data_security.pdf

The FSA has also produced a fact sheet on the subject aimed at small firms, which can be found at: www.fsa.gov.uk/pages/Doing/small_firms/general/PDF/data_security.pdf

Staying safe online
Firms should protect the integrity of their computer systems to ensure that they are not subject to the effects of viruses, Trojans, denial of service and phishing attacks. The cost of protecting a computer system against malicious attack and being used for financial crime purposes may appear prohibitive, but the consequences of not doing so can be even more damaging.

The National Cyber Security Alliance recommends small businesses should consider the following key security principles:

Use passwords
• ensure that all employees use effective passwords, and when possible, stronger authentication technology.
• encourage the use of passwords that comprise a mix of upper and lower case letters characters and numbers and change them regularly.
• encourage staff not to share these passwords, make them too obvious, or write them down where they can be found if they are a bit forgetful. Individuals should also ensure that colleagues and/or customers are not able to observe them when they are entering their passwords.

Protect your computer system
All firms should install and use anti-virus programs, anti-spyware programs, and firewalls on their computer systems. The introduction of CDs, memory sticks and other portable devices from external sources that have not been virus checked should be prohibited.

Keep all software up-to-date
Ensure that all computer software is current and contains the most recent patches (i.e. operating system, anti-virus, anti-spyware, anti-adware, firewall and office automation software). Most security and operating systems contain automatic updates, make sure that this function is switched on and sign up for security notifications from the software company.

Create back-ups
Make regular back-up copies of all important data/information. Store a secured copy offsite away from the office and use encryption to protect any sensitive information about the company and customers.

What happens in the event of an emergency?
Create a contingency plan for the business to allow recovery in the event of an emergency. Include plans to continue business operations at an alternate location when necessary. The BIBA website contains useful information on the kind of things that a contingency plan should include (see link below).

The wider picture for data security
Data security goes beyond a firm’s IT system, encompassing areas of the business such as the physical security of the building, staff recruitment, training, disposal of data and updating hardware. All these areas should be considered when putting together policy and procedures designed to protect and secure data.

Physical security
It is vital to know who has access to your office and, more importantly, customer data files. Firms responsible for security at their own premises might want to think about carrying out a risk assessment which should give consideration to:
• identifying areas of weakness in the physical security of the building which may allow unauthorised access and securing those routes, e.g. fitting alarms and CCTV
• introducing security procedures for monitoring the activities of staff and visitors
• restricting access to sensitive areas within the building, e.g. server rooms and accounts departments
• securing paper and electronic files when not in use.

Firms occupying serviced offices should check what procedures their landlord undertakes to ensure the suitability and integrity of the staff they employ to secure, maintain and clean their premises.

Make sure that the plan is tested regularly to ensure that it remains up to date and effective.
Disposal of data

There have been well-publicised cases of sensitive paper-based customer data files ending up in rubbish bins outside the offices of financial services firms for all to see.

All customer data, whether it is held on paper or electronically, must be disposed of securely. This may entail the shredding of confidential paper documents in-house by the firm itself, or through the use of an external company which specialises in the secure disposal of confidential information. If a third-party company is used to dispose of customer data, firms should satisfy themselves that their data is being disposed of in a secure manner and that staff carrying out these duties have been properly vetted to ensure their integrity.

Firms throwing away computers, giving them to staff or charity, selling on or sending machines to be recycled should always make sure that the data on the hard drive is wiped.

Who is using your IT system and for what purpose?

It might have involved a disparaging remark about a competitor or obscene comments about a colleague, but we have all received emails at work which should never have been sent through the office computer network. Then there are those embarrassing pictures of drunken antics at the office Christmas party, which colleagues have posted on Facebook.

Whether these communications are sent accidentally to a much wider audience than originally intended, or deliberately released with malicious intent, they serve to highlight the speed and ease with which information spreads in the digital age. The uncontrolled use of the internet and emails not only damages a firm’s reputation and exposes it to litigation, but also increases the risk of data loss or theft.

The internet and email are vital business tools, however. Firms should consider implementing a policy about acceptable internet and email use, restricting the use of those facilities to members of staff who have a legitimate business need for them, while blocking access to internet sites deemed unacceptable. Particular thought should be given to the risks associated with staff using web-based communication facilities, such as Hotmail and Facebook, particularly if they have access to customer data. Firms may also wish to carry out ongoing monitoring of staff and their use of the internet, the content of their emails as well as what information they are accessing and why.

Some firms have gone so far as to ban the use of mobile phones, MP3 players, PDAs and other electronic devices in the office because of the ease with which they can be used to steal information.

Use of data outside the office

The ease with which laptops and other portable devices such as memory sticks and CDs can be lost or stolen presents firms with a huge potential financial crime risk. The Ministry of Defence, Marks & Spencer and the Nationwide Building Society are just a few of the household names that have faced a firestorm of media attention because customer data stored on laptops has either been lost or stolen.

The Information Commissioner’s Office has recently declared that it is not appropriate for customer data to be taken out of the office on laptops or other portable devices unless it is encrypted. The FSA supports this view. Firms should therefore use encryption for laptops and other portable devices and put in place policies and procedures restricting the removal of customer data offsite.

Firms must also ensure that the systems and procedures designed to protect their customer data are regularly tested to ensure that they remain robust and that staff are fully trained and understand the importance of following procedures.
How big is the problem?

Reported fraud has been estimated to cost the UK’s economy at least £20 billion a year, making its impact second only to drug trafficking, according to the Economic Crime Department of the City of London Police.
Insurance fraud is probably the one area of financial crime that most intermediaries will have had some experience of. Unfortunately, many people perceive insurance fraud to be socially acceptable. Research from the Association of British Insurers has found that false and inflated insurance claims cost the industry more than £1.6 billion a year, increasing the premiums paid by honest policyholders by five per cent.

Types of fraud
Fraudsters may use many different methods to obtain cash or information from their intended victims and these methods are constantly evolving, some of the more familiar ones include:

- use of cloned/stolen credit cards
- advance fee frauds (or 419 frauds) – the targeted individual pays a small fee to claim a free holiday or a prize which is never received, or is asked to help someone transfer millions to their bank account for which they will receive commission
- pyramid selling schemes
- internet phishing attacks (e.g. emails apparently from your bank requiring you to verify your personal details)
- fraudulent use of a firm’s branding
- fake websites
- identity theft.

The Fraud Act – new hope?
The Fraud Act 2006 came into effect at the beginning of 2007 and introduced an entirely new approach toward fraud. The new Act simplifies the law and makes the prosecution process more effective by providing a clear definition of fraud. The focus is now on the dishonest behaviour of the suspect and their intent to make a gain or cause a loss.

A common complaint within the insurance industry is that the authorities have no appetite to pursue fraudulent cases. It is hoped that the Fraud Act will now make it easier to prosecute fraudsters as under the new legislation it is no longer necessary to prove that a person has been deceived.

The Fraud Act 2006 came into effect at the beginning of 2007 and introduced an entirely new approach toward fraud. The new Act simplifies the law and makes the prosecution process more effective by providing a clear definition of fraud.
A National Fraud Reporting Centre and its associated intelligence bureau will also be created. Individuals and businesses will be able to report fraud to the centre either by telephone or online.

Section 1 of the Act
This introduces a new offence of fraud which can be committed in three ways:

- **Fraud by false representation (section 2)**
  Lying about something using any means, e.g. by words or actions, sending a 'phishing' email or appropriating a brand name to set up a false website.

- **Fraud by failing to disclose information (section 3)**
  Keeping quiet when you have a legal duty to say something, e.g. not declaring information on a tax return.

- **Fraud by abuse of position (section 4)**
  Abusing a position where there is an expectation to safeguard the financial interests of another person or organisation. A person may be regarded as having abused their position even if their conduct consisted of an omission rather than an act.

The Act also introduces a series of new offences to consider, which are:

- **Possession of articles intended for use in frauds (section 6)**
  This applies anywhere and includes any article found that could be used to carry out a fraud e.g. cloned credit cards, electronic data.

- **Making or supplying articles for use in frauds (section 7)**
  The person must know or intend the article to be used to commit or assist fraud.

- **Participating in fraudulent business carried on by a sole trader, etc (section 9)**
  This now extends to individuals, partnerships and trusts.

- **Obtaining services dishonestly (section 11)**
  For example, using a stolen credit card to purchase services or products on the internet.

The response to fraud
BIBA and the ABI have a working party which intends to create industry guidelines for brokers and insurers to support the Insurance Fraud Bureau in reducing fraud. As a first step this anti-fraud working party has created a 'single point of contact' list for brokers to report suspected fraud to insurers which can be found on the BIBA website. The IFB is also seeing some success in its efforts to reduce the impact of organised crime within the industry particularly on the staged motor accident front.

Financial services firms will undoubtedly feel the effects of the Government’s efforts to curb the fraud economy. A new National Fraud Strategic Authority will act as a coordinating body, providing a national and international focus for public and private sector anti-fraud policies or activities already underway with the overall aim of reducing such crime in the UK. The new authority is expected to begin its operations in October 2008.

A National Fraud Reporting Centre and its associated intelligence bureau will also be created. Individuals and businesses will be able to report fraud to the centre either by telephone or online. This information will be analysed to help give a better focus to police and investigative agencies’ activities.

A National Fraud Lead Force is also being set up which will provide some central functions and strengthen the support available to police in England and Wales. The City of London Police’s Economic Crime Department will provide the nucleus for this new lead force. It will also act as a centre of excellence for fraud investigations. Hopefully, these actions combined will have a significant impact on reducing fraud in the UK.
Reporting fraud

Firms have a duty to report significant frauds to the FSA. They also have a duty to report their suspicions that other intermediaries or insurers are involved in criminal and fraudulent activity. Examples of possible financial crime involving insurance fraud could entail:

- misappropriation of client money or money held under risk transfer agreements
- falsifying customer details to obtain insurance business that would otherwise be rejected or more costly
- falsifying rates in order to select an insurer which would give the highest level of commission.

The FSA has a streamlined system for reporting financial crime in the insurance sector, which can be found at the following link:


The FSA will need the following information:

- the name of the intermediary and/or insurer suspected
- details of any individuals involved
- details and evidence of the suspected and/or proven fraud or financial crime
- the names of the customers involved
- summary of investigations.

Members may also contact the compliance team at BIBA to report their concerns about a particular intermediary or insurer, which will be passed on anonymously to the FSA, should that route be preferred.

The Insurance Fraud Bureau operates a free and confidential helpline for anyone who wishes to report suspected insurance fraud.

Contact the Cheatline on tel: 0800 328 2550.
The internal threat – employee risks

A focus on reducing the threat of financial crime to a business from external sources can mean that risks from within the firm are overlooked.

Disgruntled employees, those with money worries, the soon-to-be redundant or those moving on to take up a new job with a competitor can all seriously damage a business should they choose to because of the access they have to confidential information and intellectual property.

The downright dishonest employee may also be thrown into the equation. There is evidence that organised crime groups deliberately target firms in the financial services sector in order to place staff to commit financial crime, in particular identity theft.

It is important for a business to know its employees as well as they know their customers. Firms should have a comprehensive vetting policy to determine the integrity of their employees and follow it when recruiting.

Firms can use a variety of online databases and information sources to check the credentials of staff, these might include:
- verification of complete school, university and employment history
- references
- credit, address and telephone number checks
- treasury sanctions list check
- County Court Judgment checks
- electoral roll
- police records
- professional association disciplinary records
- FSA Register
- international media sources.

Firms may wish to introduce tiered vetting according to the sensitivity and seniority of a job role. They may also wish to put in place service level agreements with agreed vetting standards when using recruitment agencies to ensure the quality of recruits coming into the business through that route.

Remember that nothing stays the same. Just because a member of staff passed background checks when first employed does not mean that they will continue to do so. Annual risk assessments for all staff should be carried out to ensure that their records are up to date and that they remain the kind of individual that you wish to employ. Checks could also extend to random audits of recruitment agency vetted staff.
### USEFUL LINKS FOR FURTHER INFORMATION

#### UK sites

<table>
<thead>
<tr>
<th>Service</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>HM Treasury</td>
<td><a href="http://www.hm-treasury.gov.uk">www.hm-treasury.gov.uk</a></td>
</tr>
<tr>
<td>HM Treasury sanctions pages</td>
<td><a href="http://www.hm-treasury.gov.uk/documents/financial_services/sanctions/fin_sanctions_index.cfm">www.hm-treasury.gov.uk/documents/financial_services/sanctions/fin_sanctions_index.cfm</a></td>
</tr>
<tr>
<td>Home Office</td>
<td><a href="http://www.homeoffice.gov.uk">www.homeoffice.gov.uk</a></td>
</tr>
<tr>
<td>Home Office Identity Fraud Strategy Group</td>
<td><a href="http://www.identity-theft.org.uk">www.identity-theft.org.uk</a></td>
</tr>
<tr>
<td>Foreign &amp; Commonwealth Office</td>
<td><a href="http://www.fco.gov.uk">www.fco.gov.uk</a></td>
</tr>
<tr>
<td>Department of Business, Enterprise &amp; Regulatory Reform</td>
<td><a href="http://www.berr.gov.uk">www.berr.gov.uk</a></td>
</tr>
<tr>
<td>Financial Services Authority</td>
<td><a href="http://www.fsa.gov.uk">www.fsa.gov.uk</a></td>
</tr>
<tr>
<td>Serious Organised Crime Agency</td>
<td><a href="http://www.soca.gov.uk">www.soca.gov.uk</a></td>
</tr>
<tr>
<td>Serious Fraud Office</td>
<td><a href="http://www.sfo.gov.uk">www.sfo.gov.uk</a></td>
</tr>
<tr>
<td>Economic Crime Department, City of London Police</td>
<td><a href="http://www.cityoflondon.police.uk">www.cityoflondon.police.uk</a></td>
</tr>
<tr>
<td>Metropolitan Police Fraud Alert</td>
<td><a href="http://www.met.police.uk/fraudalert">www.met.police.uk/fraudalert</a></td>
</tr>
<tr>
<td>Joint Money Laundering Steering Group</td>
<td><a href="http://www.jmlsg.org.uk">www.jmlsg.org.uk</a></td>
</tr>
<tr>
<td>Institute of Money Laundering Prevention Officers</td>
<td><a href="http://www.implo.com">www.implo.com</a></td>
</tr>
<tr>
<td>Insurance Fraud Bureau</td>
<td><a href="http://www.insurancefraudbureau.org">www.insurancefraudbureau.org</a></td>
</tr>
<tr>
<td>CIFAS – the UK’s Fraud Prevention Service</td>
<td><a href="http://www.cifas.org.uk">www.cifas.org.uk</a></td>
</tr>
<tr>
<td>The Fraud Advisory Panel</td>
<td><a href="http://www.fraudadvisorypanel.org">www.fraudadvisorypanel.org</a></td>
</tr>
</tbody>
</table>

#### US sites

<table>
<thead>
<tr>
<th>Service</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Treasury</td>
<td><a href="http://www.treas.gov">www.treas.gov</a></td>
</tr>
<tr>
<td>Office of Foreign Assets Control</td>
<td><a href="http://www.treas.gov/offices/enforcement/ofac/index.shtml">www.treas.gov/offices/enforcement/ofac/index.shtml</a></td>
</tr>
<tr>
<td>Coalition Against Insurance Fraud</td>
<td><a href="http://www.insurancefraud.org">www.insurancefraud.org</a></td>
</tr>
<tr>
<td>National Cyber Security Alliance</td>
<td><a href="http://www.staysafeonline.info">www.staysafeonline.info</a></td>
</tr>
</tbody>
</table>

#### International sites

<table>
<thead>
<tr>
<th>Service</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Action Task Force (FATF)</td>
<td><a href="http://www.fatf-gafi.org">www.fatf-gafi.org</a></td>
</tr>
<tr>
<td>International Association of Insurance Supervisors</td>
<td><a href="http://www.iaisweb.org">www.iaisweb.org</a></td>
</tr>
<tr>
<td>United Nations</td>
<td><a href="http://www.un.org/sc/committees">www.un.org/sc/committees</a></td>
</tr>
<tr>
<td>European Union</td>
<td><a href="http://www.ec.europa.eu/external_relations/cfsp/sanctions">www.ec.europa.eu/external_relations/cfsp/sanctions</a></td>
</tr>
</tbody>
</table>