

**The Fraud
Advisory
Panel**

the fraud Cybercrime and
advisory the Proceeds
panel of Crime Act

CYBERCRIME AND THE PROCEEDS OF CRIME ACT

A practical guide for business

1. Introduction

The Proceeds of Crime Act 2002 (POCA) came into force in Spring 2003. The Money Laundering Regulations 2003 were laid before Parliament on 28 November 2003 and have the effect of expanding the number of organisations who are included in the regulated sector and therefore subject to the additional reporting requirements of POCA and the systems requirements of the Money Laundering Regulations.

The Money Laundering Regulations 2003 (the Regulations) come into force on 1 March 2004⁽¹⁾ and have the effect of revoking the Money Laundering Regulations 1993 and the Financial Services and Markets Act 2000 (Regulations Relating to Money Laundering) Regulations 2001.

1.1 Which Industries will be Subject to POCA?

Any business or individual which launders the proceeds of crime risks a criminal prosecution. POCA widened the definition of money laundering to include the possession of the proceeds of an offender's own crime, as well as more obvious money laundering offences such as entering into an arrangement which facilitates the acquisition, retention or use of another's criminal proceeds, or concealing, disguising, converting or transferring them. Aiding, abetting, counselling or procuring money laundering are also included in the definition, as is attempting, conspiring or incitement to commit a money laundering offence. One of the key defences to a charge of any of these offences is to make a report to the National Criminal Intelligence Service (NCIS).

Duties of disclosure regarding suspicions of money laundering are also imposed upon the regulated sector with criminal penalties for failure to report to NCIS.

A number of industries will be included in the regulated sector. These include:

- Banks and financial services, including Internet banks
- Solicitors (when acting in relation to a financial or real estate property transaction)
- Accountants

⁽¹⁾ With the exception of Regulation 10 which requires high-value dealers to register with the Commissioner of Customs & Excise which must be done by 1 April 2004. Regulation 2(3) (h) & (l) relate to regulated activities of advising and arranging investments relating to rights under regulated mortgage contracts and contracts of insurance. These regulations come into force on 31 October 2004 and 14 January 2005 respectively.

- Casinos
- Estate agents
- Money service businesses which include:
 - Bureaux de Change operators
 - Those whose business involves the transmission of money
 - Those whose business involves cashing cheques
- Insolvency practitioners
- Tax and financial advisers
- Those operating company or trust formation and administration companies
- Dealers in high-value goods for **cash** over 15,000 Euro, including:
 - Auctioneers
 - Car dealers
 - Jewellers and those dealing in gemstones and precious metals, and
 - Art and antique dealers

These industries will need to comply not only with the POCA sections of general applicability but also those aimed at the regulated sector.

The Regulations have two aims. Firstly, to enable suspicious transactions to be recognised and reported to law enforcement agencies and secondly to ensure that if a client comes under investigation in the future a firm can provide its part of the audit trail.

1.2 What do the Regulations Cover?

The Regulations cover the following:

- Internal controls and communication of policies
- Identification procedures
- Recognition of suspicious transactions and reporting procedures
- Education and training of partners and staff
- Record keeping procedures

1.2.1 Cyber concerns

Cybercrime embraces many forms of computer-related criminality, most but not all of which will give rise to criminal proceeds. The use of computer-based records as distinct from books and ledgers adds no new points of principle to money laundering. The use of the Internet does introduce new factors. The Internet does permit anonymity, and the ability to adopt another's identity or to disguise the origin of a message. It provides a readily available means to communicate and conduct transactions from outside the jurisdiction, with less dependency on professionals as

intermediaries. For professionals, there is a danger in assuming that electronically transferred funds must have passed through the regulated sector and as such there is no reason to check the source. This may not be the case.

- *Identity procedures* – ‘know your client’. Although checks are in place to verify identities the Internet has given rise to identity theft and caution is advised.
- *Identity procedures* – ‘companies/partnerships’. Again, the Internet has heightened the amount of fake or stolen identities for companies and partnerships. Stringent checks are recommended.
- *Trusts* – There are specialist identification requirements that have to be met for trusts, local authorities, operational pension schemes and charities. As with new clients or companies, stringent ID checks are required to eliminate the chance of fake or stolen identities. Trusts created in jurisdictions without money laundering procedures in place will warrant additional enquiries. It should be remembered that these are potentially very high risk from a money laundering viewpoint and you should be careful to ensure that you are happy with, for example, the source of funds, the reason for the trust, and the reason for any business connected with the trust.
- *Reporting suspicious transactions* – The advent of e-commerce means that many transactions do not require any human intervention by the provider of the service. However, this lack of human intervention will not provide a defence to a charge under POCA. Therefore, any automated transactions must be carefully monitored and the following questions should be asked:
 - Is the transaction or activity normal for this customer?
 - Does the transaction or business make sense from a business/personal point of view?
 - Has the pattern of transactions changed?
 - Where the transaction is with an entity in another country, is there a good business reason for this?
- *Record keeping procedures* – This is of utmost importance if there is an investigation. Records need to be kept for at least five years for relevant business. Again there are concerns with data being infiltrated either through an external force such as hacking or internally through a disgruntled employee.

1.3 When Should an Individual or Business Report Money Laundering?

A person who handles relevant business must report:

- (a) Actual knowledge or suspicion, or
- (b) Reasonable grounds for knowing or suspecting that another person is engaged in money laundering.

A person who knows or suspects that they may have been caught up in money laundering also needs to report, as a defence to a charge of money laundering.

Third parties outside the regulated sector may also report, as a matter of public interest, as they are covered by the confidentiality over-ride provisions in Section 337 of POCA.

Section 340(11) of POCA defines money laundering as an act which:

- (a) Constitutes an offence under section 327, 328 or 329;
- (b) Constitutes an attempt, conspiracy or incitement to commit an offence specified in paragraph (a);
- (c) Constitutes aiding, abetting, counselling or procuring the commission of an offence specified in paragraph (a), or
- (d) Would constitute an offence specified in paragraph (a), (b) or (c) if done in the United Kingdom.

Sections 327, 328 and 329 define which activities constitute a money laundering offence under the Act:

Section 327 Concealing, etc

(1) A person commits an offence if he:

- (a) Conceals criminal property;
- (b) Disguises criminal property;
- (c) Converts criminal property;
- (d) Transfers criminal property;
- (e) Removes criminal property from England and Wales or from Scotland or from Northern Ireland.

(2) But a person does not commit such an offence if:

- (a) He makes an authorised disclosure under section 338 and (if the disclosure is made before he does the act mentioned in subsection (1)) he has the appropriate consent;
- (b) He intended to make such a disclosure but had a reasonable excuse for not doing so;
- (c) The act he does is done in carrying out a function he has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct.

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

Section 328 Arrangements

- (1) A person commits an offence if he enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.
- (2) But a person does not commit such an offence if:
 - (a) He makes an authorised disclosure under section 338 and (if the disclosure is made before he does the act mentioned in subsection (1)) he has the appropriate consent;
 - (b) He intended to make such a disclosure but had a reasonable excuse for not doing so;
 - (c) The act he does is done in carrying out a function he has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct.

Section 329 Acquisition, Use and Possession

- (1) A person commits an offence if he:
 - (a) Acquires criminal property;
 - (b) Uses criminal property;
 - (c) Has possession of criminal property.
- (2) But a person does not commit such an offence if:
 - (a) He makes an authorised disclosure under section 338 and (if the disclosure is made before he does the act mentioned in subsection (1)) he has the appropriate consent;
 - (b) He intended to make such a disclosure but had a reasonable excuse for not doing so;
 - (c) He acquired or used or had possession of the property for adequate consideration;
 - (d) The act he does is done in carrying out a function he has relating to the enforcement of any provision of this Act or of any other enactment relating to criminal conduct or benefit from criminal conduct.
- (3) For the purposes of this section:
 - (a) A person acquires property for inadequate consideration if the value of the consideration is significantly less than the value of the property;

- (b) A person uses or has possession of property for inadequate consideration if the value of the consideration is significantly less than the value of the use or possession;
- (c) The provision by a person of goods or services which he knows or suspects may help another to carry out criminal conduct is not consideration.

To summarise, a person commits an offence under POCA if he or she conceals, disguises, converts, transfers or removes from the jurisdiction any criminal property. This could clearly cover the acts of an individual carrying out transactions in the course of his employment or business. Protection for such a person is achieved by the provisions for authorised disclosures (suspicious transaction reports). An individual has a defence to any of the above offences if he or she makes an authorised disclosure, or intended to make such a disclosure, but has a reasonable excuse for not having done so.

A person also commits an offence if he or she attempts, conspires or incites another to commit a money laundering offence or aids, abets, counsels or procures it.

The definition of criminal property includes property from criminal conduct committed anywhere in the world, provided that the criminal conduct would be an offence if it were committed in this country. This is a very wide jurisdiction and should be useful when prosecuting Internet crime, because for jurisdiction purposes it will not matter where the offence was committed, provided that the conduct constitutes a criminal act in this country.

Brothels and Bullfighters

The duty to report exists in a wide range of circumstances because of the broad definition of money laundering. If it is a crime in the UK, POCA applies even if the act which gives rise to the proceeds of crime occurs outside the jurisdiction and is not a crime in the jurisdiction in which it is committed. The property concerned will still be treated as criminal property. This has given rise to the brothels and bullfighters argument. If a bullfighter from Spain (where the activity is legitimate) were to instruct a solicitor and pay his earnings into the solicitor's client account in the UK (where bullfighting is a criminal offence), the solicitor would be under a duty to report the transaction to the National Criminal Intelligence Service (NCIS) as a suspicious transaction.

2. Cybercrimes which may give rise to a duty to report under POCA

Computer enabled fraud comes in many forms. Examples of such frauds range from get-rich-quick schemes that don't exist to emails that demand an additional fee to be paid by credit card or personal details including passwords and account numbers.

POCA may have implications for any cybercrime which is initially perpetrated to generate value. As mentioned above, money laundering is also covered by the Act. This means that any organisation whose services can be utilised by criminals to launder money will need to be aware of the legislation, for example the betting and gaming industry, Internet payment systems and money transfer organisations.

Examples of money laundering methods include:

- Making payments to reputable institutions with the objective of receiving a clean cheque in return:
 - Financial service clients may buy investments with criminal proceeds and be prepared to suffer a loss (through short-term dealing) in order to receive a clean cheque.
 - Making overpayments to institutions including Government departments in order to obtain a clean cheque in return.
 - A customer may ask to deposit money in the client account of an accountant, solicitor, or other professional adviser to show that he has funds for a proposed business deal. The return of funds might then be requested as the deal “falls through”. The launderer then has a clean cheque from a reputable source.
- Using cash-based businesses in order to “drip-feed” cash from illegal sources into them to disguise them as legitimate business turnover. Suspicions may be aroused where income is disproportionate to outgoings, where the customer base appears inadequate, or where the only Internet banking activity is to transfer funds outside the jurisdiction.
- Transferring high-value items instead of money. The Internet provides an additional way to initiate this. E-cash can be used over the Internet, but the restriction on maximum value may be a disincentive to launderers. As always, a careful watch should be maintained on any changes in the use of these facilities.

There are a number of cybercrimes that may give rise to a duty to report under POCA. These include:

- Cyberlaundering
- Advanced fee frauds
- Computer hacking
- Cyber extortion
- Identity theft
- Sale of stolen or counterfeit goods via the Internet, and
- Credit card fraud

2.1 Cyberlaundering

This refers to any activity that is carried out via the Internet that can be used to launder money. Organisations which are vulnerable can include Internet casinos and online banks.

2.2 Advanced Fee Fraud

Advanced fee fraud involves requests for assistance in removing large sums of money often from West African jurisdictions. Victims are promised a share of the money in return. Contact is usually made with the victim by email or post.

If a business becomes aware that it has become implicated or involved in an advanced fee scam then it may have a duty to report. For example, a business may need to report if it becomes aware that its name and/or stationery is being used to add credibility to a scam, or that its website has been copied for the purposes of carrying out an advanced fee fraud. It has arguably become concerned (even indirectly) in an arrangement which facilitates the acquisition, use, retention or control of criminal property.

2.3 Hackers

There are two main groups of hackers – internal and external. The aim of the hacker may be to steal corporate information, carry out an e-theft, plant malicious computer programs, disrupt the target's computer system, highlight a lack of security or deface the company's website causing damage to its corporate reputation.

Businesses that become a victim of a hacker who steals corporate (including customer) information may be required to report under POCA, particularly when the purpose of the hacking has been to obtain funds or the credit card details of customers. In such circumstances the victim could arguably be seen to have become concerned in an arrangement which facilitates (by whatever means) the acquisition of criminal property.

2.4 Cyber Extortion

Recently there have been reports of cyber extortion involving threats to bring down websites with denial of service attacks unless payments are made to third parties. One of these cases has been linked to organised gangs of criminals including the Russian Mafia. These transactions involve money laundering because the third party will be in possession of criminal property that are the proceeds of extortion.

2.5 Identity Theft

Identity theft refers to the using of another person or business's identifying details without their permission for commercial gain. This information can then be used to open bank accounts; obtain payments, credit or other forms of identification (such as passport or driving licence); fraudulently obtain social security benefits (in the case of individuals); or obtain goods and services.

Recently a number of High Street banks have been targeted by online fraudsters who send emails to customers inviting them to log on to bogus bank websites to verify their account details. These details are then used to steal funds from a person's account or to carry out other forms of identity theft. This is commonly known as "phishing". There is no obligation to report an attack relating to phishing activity where no theft of funds has yet actually taken place; the obligation exists when the information obtained from a phishing attack is subsequently used to transfer funds from one account to another.

2.6 Sale of Stolen or Counterfeit Goods via the Internet

Internet auctions may also find that they are under a duty to report suspicious transactions. For example, if they suspect (or indeed know) that a user is selling stolen or counterfeit goods through the service the organisation provides then it has

arguably become concerned in an arrangement facilitating the acquisition, control or use of criminal property. The organisation may have a duty to report the user.

2.7 Credit Card Fraud

Credit card companies, NCIS and the Home Office have reached an agreement on the reporting of card fraud. Under this agreement, credit card companies are obliged to report card frauds that fit **all** the following criteria:

- A fraud was committed using a payment card, and
- The proceeds of the crime can be located, ie. goods/services that are delivered can be attributed to a fraudster, and
- The fraudster can be located and identified as having committed the crime.

At Risk Jurisdictions

The Financial Action Task Force on Money Laundering (FATF) is an inter-governmental body which aims to combat money laundering and terrorist financing. The FATF maintains a list of non-co-operative countries and territories which identifies jurisdictions with deficiencies in their anti-money laundering systems or that have a demonstrated unwillingness to co-operate in anti-money laundering efforts (the 'FATF List'). This list is available from the FATF website (www.fatf-gafi.org).

3. Trades and Professions that may be affected by duties to report

Members of these trades and professions should make themselves aware of any anti-money laundering guidance issued by their trade or professional body, and follow it where appropriate.

3.1 Solicitors

Solicitors who carry out web-based legal services would need to be aware of cyberlaundering, credit card and identity fraud.

3.1.1 Credit Card and Identity Fraud

Some solicitors accept payment by credit card. Credit cards may be applied for in a false name. This is known as application fraud. If the client then makes payments from the credit cards into the client account and that payment is used to pay the solicitor's firm itself or is passed through the firm's accounts for the purposes of a transaction, the firm has potentially committed a money laundering offence. This is because it is arguably in possession of stolen funds; the firm has transferred or disguised criminal property albeit unwittingly. If a solicitor knows or suspects that a money laundering offence has been committed using the office client account he or she is under a duty to report it, regardless of whether it is engaged in relevant business.

Solicitors need to take particular care when dealing with long distance clients (i.e. clients who only contact the solicitor through telephone, e-mail or post and with

whom there is no face-to-face contact). Thorough identity checks need to be made before accepting such payments in order to ensure that a firm knows its clients.

3.1.2 Cyberlaundering

One well-known money laundering scam is where a client instructs a solicitor, pays money into the client account and then changes his or her mind and asks for money to be returned. Solicitors should be particularly wary where the client is from an “at risk” jurisdiction. Solicitors should also take care where a client offers to pay (or does pay) a greater figure on account of costs that the solicitor has requested. Solicitors offering web-based services need to be even more careful when identifying clients due to the anonymity offered by the Internet.

3.2 Estate Agents

Many estate agents now operate over the Internet. Estate agents should take care to properly identify clients and to keep good records particularly where they are dealing with long distance clients. This is important when dealing with clients from “at risk” jurisdictions such as those which appear on the FATF List.

Estate agents may find that they are also used to facilitate mortgage frauds. It is an offence to be concerned with an arrangement that facilitates the acquisition of criminal property. Knowledge or suspicion that a mortgage fraud is being carried out may mean that the estate agent is concerned with such an arrangement as well as having a duty to report under Section 330 of the Act. For example it might be necessary to report a suspicion that a client applying for a self certified mortgage has fraudulently inflated his or her earnings on the application form.

3.3 Casinos

Online casinos and betting agencies can become the victims of cyber extortion. Any instance of cyberlaundering that a casino worker became aware of, or suspected, would need to be reported.

Money laundering through any Internet casino works in the same way as through non-virtual casinos:

- The launderer buys chips with which to gamble.
- Inevitably the launderer will lose a percentage of the funds but this is a price that he or she is willing to pay in order to clean the money.
- At the end of the gaming session the launderer cashes in his or her remaining chips and takes payment by means of a draft (or a transfer from the casino in the case of an Internet casino), which can be paid into the launderer’s account.
- The payment will appear to come from a legitimate source – the casino.

The lack of identity checks and the nature of Internet gambling means that the opportunity for this type of crime is high and the opportunity for detection is low.

3.4 Art Dealers, Auctioneers, Precious Stone and Metal Dealers

Art dealers and auctioneers may find that high-value goods are traded through their businesses in order to facilitate the movement of dirty money. Art dealers,

auctioneers, precious stone and metal dealers may all carry out relevant business, if they undertake high-value cash transactions.

Under the terms of the Money Laundering Regulations 2003 transactions which involve cash payments of 15,000 Euro or where there are linked transactions that total 15,000 Euro should be recorded. Where there is a suspicion or actual knowledge of money laundering this should be reported. Relevant business is defined under the Money Laundering Regulations 2003 to include:

(n) the activity of dealing in goods of any description by way of business (including dealing as an auctioneer) whenever a transaction involves accepting a total cash payment of 15,000 Euro or more.

In addition, there is always a duty to report, regardless of value, if there is a risk of entering into an arrangement involving money laundering.

The potential for money laundering may increase for online and/or telephone auctions, though such businesses will not be relevant business, where payments in cash are not possible. However, the risk of entering into a money laundering arrangement may be greater because the identity of the purchaser may be concealed. Two examples where this may arise are:

3.4.1 Online Auction Fraud

If the auction is aware that counterfeit or stolen goods are being sold on its site or through its business it may be under a duty to report. Again, the business has arguably become concerned in an arrangement that facilitates money laundering.

3.4.2 Stolen or Counterfeit Goods

For some individuals, the online auction is an ideal place to sell stolen goods or pirated software. Before the advent of the Internet many goods were – and probably still are today – fenced at pawnshops and auctions.

In addition, art dealers and auctioneers should be wary of transactions where the purchaser is prepared to pay way over the estimated value for a particular item.

Any online sales of fake or stolen goods counts as money laundering, since they involve the transfer of criminal property. Knowledge or suspicion of any involvement in such transactions would need to be reported.

3.5 Money Service Businesses

These include Bureaux de Change, cheque cashing businesses, and any other businesses involving the transfer of money.

3.5.1 Cyberlaundering

Any attempt to launder funds electronically will need to be reported in the same way as knowledge of, or a suspicion that, an individual was attempting to launder cash.

3.6 Internet Banks

Part 5 of POCA 2002 introduced new investigatory powers, which allow a court to order a bank to disclose whether it holds an account for a defendant and if so, to monitor that account. This would include Internet banks.

3.7 Accountants

Anyone providing accounting services is within the scope of relevant business, as are those providing the related services of audit, insolvency or tax advice.

3.7.1 Indications of Money Laundering⁽²⁾

The risk factors associated with money laundering are often the same for any fraud and the appendix to SAS 110 provides a list of potential factors. In addition, the list below summarises some of the key factors to be wary of in a business:

- The presence of a dominant owner
- Management appears to have little knowledge of the business
- Anyone dealing in large amounts of cash
- Poor record keeping
- Trading with countries with weak legislation
- Complex corporate structures with offshore jurisdictions with no apparent business reason
- Large transactions between bank accounts
- Reported turnover of an organisation that does not equate with its apparent size
- Foreign travel which appears unnecessary or expensive
- Odd patterns of trading with a customer
- Transactions with companies whose identity is difficult to establish
- Long delays in production of accounts, and
- Unusual trading terms being offered

Dealing with clients over the Internet where face-to-face contact is not always possible is a factor which is likely to increase the opportunities for money launderers to use accountants to disguise the proceeds of crime.

The Fraud Advisory Panel would like to thank Steven Philippsohn, Chairman of the Fraud Advisory Panel Cybercrime Working Group and the Fraud Litigation Team at Philippsohn Crawford Berwald together with Esther George, Riten Gohil, Stephen Hill, Ian Hodges, Jon Merrett, and Alice Rigby for their assistance in the preparation of this publication.

⁽²⁾ Excerpts from the following documents are reproduced with the kind permission of the Auditing Practices Board Limited: SAS 110 Fraud and Error, and PN 12 Money Laundering.

Useful Links

Association for Payment Clearing Services (APACS)
www.apacs.org.uk

Association of Chartered Certified Accountants (ACCA)
www.acca.org.uk

British Bankers' Association
www.bba.org.uk

Chantrey Vellacott DFK
www.cvdffk.com

City of London Police
www.cityoflondon.police.uk

Crimestoppers
www.crimestoppers.co.uk

Department of Trade & Industry
www.dti.gov.uk

Financial Services Authority
www.fsa.gov.uk

Home Office
www.homeoffice.gov.uk

HM Customs & Excise
www.hmce.gov.uk

HM Treasury
www.hm-treasury.gov.uk

Philippsohn Crawfords Berwald
www.pcbllitigation.com

Inland Revenue
www.inlandrevenue.gov.uk

Institute of Chartered Accountants in England & Wales
www.icaew.co.uk

Institute of Chartered Accountants of Scotland
www.icas.org.uk

Interactive Gambling, Gaming & Betting Association
www.iggba.org.uk

Law Society
www.lawsociety.org.uk

Metropolitan Police
www.met.police.uk

National Association of Real Estate Agents
www.naea.co.uk

National Audit Office
www.nao.gov.uk

National Criminal Intelligence Service (NCIS)
www.ncis.gov.uk

National Hi-Tech Crime Unit
www.nhtcu.org

Serious Fraud Office
www.sfo.gov.uk

Small Business Service
www.businesslink.org

The Fraud Advisory Panel

Chartered Accountants' Hall PO Box 433 Moorgate Place London EC2P 2BJ www.fraudadvisorypanel.org