CIMA

Fraud and money laundering

Topic Gateway Series No. 31

Prepared by Martin Nimmo and Technical Information Service

June 2007

About Topic Gateways

Topic Gateways are intended as a refresher or introduction to topics of interest to CIMA members. They include a basic definition, a brief overview and a fuller explanation of practical application. Finally they signpost some further resources for detailed understanding and research.

Topic Gateways are available electronically to CIMA members only in the CPD Centre on the CIMA website, along with a number of electronic resources.

About the Technical Information Service

CIMA supports its members and students with its Technical Information Service (TIS) for their work and CPD needs.

Our information specialists and accounting specialists work closely together to identify or create authoritative resources to help members resolve their work related information needs. Additionally, our accounting specialists can help CIMA members and students with the interpretation of guidance on financial reporting, financial management and performance management, as defined in the *CIMA Official Terminology* 2005 edition.

CIMA members and students should sign into My CIMA to access these services and resources.

The Chartered Institute of
of Management Accountants
26 Chapter Street
London SW1P 4NP
United Kingdom

T. +44 (0)20 7663 5441
F. +44 (0)20 7663 5442
E. tis@cimaglobal.com
www.cimaglobal.com

Definition

Money laundering is defined as:

'The funnelling of cash or other funds generated from illegal activities through legitimate financial institutions and businesses to conceal the source of the funds.'

Anti-Money Laundering, 2nd ed., IFAC, 2004

Fraud is a general term for deliberate misrepresentation and may include money laundering.

The problems of fraud and especially money laundering are increasing at an unprecedented rate. Governments worldwide are introducing new legislation and penalties for such white collar crimes. However, the huge amounts of money involved in these illegal activities ensure that criminals continue to exploit ways of increasing their activities. They clearly weigh up the potentially vast profits against their chances of being caught and the subsequent penalties.

Context

It is a fact that legitimate financial institutions and businesses may be involved in fraud and money laundering. It is therefore crucial that CIMA members, whether in practice or in business, are fully aware of this possibility and are alert to the signs of money laundering which can affect their business.

Examination candidates should be aware of the risks involved, especially at strategic and TOPCIMA level. They should ensure that they know the signs of possible money laundering and the steps they must take to report it.

Overview

There are a number of ways in which criminals commit financial fraud. Very often this involves stealing another person's identity.

Identify theft

Identity theft (including e-fraud and 'phishing') is a modern day fraud and much is publicised about people whose assets have been stripped by personal identity theft. It is advisable for individuals to check their own personal credit reports regularly. However, there are increasing numbers of reported cases where the identities of companies have been hi-jacked. This occurs through unauthorised changes to the registered address of the company or to directorships.

These crimes are not just a financial risk to the companies concerned, but a reputational risk which may damage the business for an appreciable amount of time.

The Fraud Act 2006 came into force on 15 January 2007. This created a new offence of fraud, which can be committed in three ways:

- by making a false representation (with intent to make a gain, cause loss or risk of loss to another)
- by failing to disclose information
- by abuse of position.

It also became an offence to obtain services dishonestly, to possess equipment to commit frauds, and to make or supply articles for use in frauds. The Identity Cards Act 2006 created offences relating to the possession, control and intent to use false identity documents, including genuine documents that relate to another person.

Phishing

The objective of 'phishing' is to obtain and use personal banking details. Potential victims receive an email purporting to be from a bank or building society, or these days commonly from eBay or PayPal. The email may state that there has been a breach of security or the person concerned needs to update their details.

Alternatively, people may be told that they have made a purchase although they have not. They are then directed to a website that appears to be legitimate where they are asked to disclose their bank or personal details. If you receive any such message:

- do not reply to it
- do not pass any personal information by email or complete any forms asking for personal information
- delete the message.

Concerned individuals should contact the real company or organisation by post or telephone at a genuine address or number. Many companies that deal exclusively on the internet also have a help section which explains what you should do if you receive one of these emails. Examples of 'phishing' letters are also given.

On 2 November 2005 the Times recorded that a fraudster who duped almost £200,000 from eBay customers using a 'phishing' scam had been jailed by Preston Crown Court. David Levi of Lytham, Lancashire, led a gang that amassed a fortune by stealing account details from users and assuming their identities. It is believed to have been the first successful prosecution for 'phishing'.

Individuals should purchase appropriate computer software to protect them from this type of attack. Anti-spyware and personal firewalls are ideal, and anti-virus software will give a measure of protection against 'phishing'.

Cash back fraud

Cash back fraud may result when an individual offers something for sale on the internet, Exchange and Mart or even the small ads in a local paper. They may be contacted by a 'buyer' who wants to purchase the advertised item without wanting to see it.

The seller then receives a cheque for considerably more than the asking price, and is asked to send some or all of the difference to the buyer or shipping agent by money transfer (usually Western Union). The cheque will either be forged or stolen. Even if it is cleared by the bank, it can be recalled and the seller will not be reimbursed for this loss.

Research has established that many people put themselves at risk of fraud through a failure to take basic precautions. For example, one in eight people fail to log out after shopping online, leaving their financial details visible to others. One in four people do not check if a website is secure (the padlock symbol to the bottom right of your screen will usually indicate this).

People are also urged to sign up to security schemes such as Verified by Visa and MasterCard SecureCode. The simple step of typing in a password or security code when buying online makes it less likely for fraudsters to use stolen card details.

The Isle of Man Financial Services Commission adds a security point applicable in the case of emails; If you want to save a copy of a document, do not open it. Right click on the name of the document you require and a dialog box will appear which will give you the option to save the target or to print it.

'419' letters

There continues to be a steady flow of letters either in hard copy, by fax or by email, appealing to CIMA members to assist the originator(s) with moving money out of the respective country by bank transfer. These letters are known to the Police in the UK as '419' letters (after Section 419 of the Nigerian Penal Code).

In a typical '419' (advance fee fraud) letter, the author claims to be a senior government, company or bank official who has managed to over inflate a contract, generating a huge personal profit. In return for help in smuggling money out of the country, the recipient is offered a percentage, usually between 10% and 30% (which can apparently amount to several million pounds).

At first no money is requested, but once a victim has been drawn in, requests will be made for legal and administrative payments. Victims have lost hundreds of thousands of pounds in some cases, not to mention the loss of business and reputation.

Interpol strongly recommends that people:

- do not reply to these letters
- do not surrender bank account details
- do not surrender company details
- do not send or hand over ID documents and letters with personal or official letterheads and logos, not even copies.

Companies that have sent polite letters of refusal have had their letterheads abused. Under no circumstances should such approaches be responded to. CIMA members or students should send any letter of this type on to their local police force immediately.

Overview of money laundering

The fight against financial crime worldwide is largely based on the 40 principles of the international Financial Action Task Force (FATF) set up by the G7 nations. In the UK, HM Treasury recently issued the draft Money Laundering Regulations 2007, which will implement the EU 3rd Money Laundering Directive.

This is only the latest of many measures. The Money Laundering Regulations 2003 (in force until 15 December 2007 when they will be replaced with the new Regulations) have been supplemented by the Proceeds of Crime Act and the Serious Organised Crime Act, as well as other primary legislation. Similar regulation applies in all EU member states (currently based on the EU 2nd Money Laundering Directive) and compatible measures apply in most countries worldwide.

The EU Third Money Laundering Directive

The EU third Money Laundering Directive and the new Money Laundering Regulations include changes to the obligations related to customer due diligence. This is the requirement for financial institutions, including 'external accountants', to identify their customers and verify their identity. They also need to maintain full records.

It is vital that CIMA members understand that this not only relates to accountants offering audit, insolvency services or financial advice. It applies to all CIMA Members in Practice, and to all their new or existing clients, whether individuals or companies. The Third Money Laundering Directive will be adopted in UK law as the Money Laundering Regulations 2007.

Requirements of CIMA members

All CIMA members, but especially registered Members in Practice, must observe the requirements of regulations and relevant legislation, as failure to do so could lead to prosecution. They could also face both substantial fines and imprisonment if found guilty. Members and students will also be subject to the Institute's own conduct procedures.

Attention should be drawn to the Fraud Act 2006 and to anti-terrorism legislation. The UK Government's view is that terrorism is largely financed by fraud and money laundering. It also considers that money laundering covers a wide range of offences ranging from drugs dealing to VAT fraud, robbery and disposing of the proceeds of crime.

Application

There are three sources of sector specific guidance, namely IFAC, the CCAB and CIMA. Both IFAC and the CCAB have issued online guidelines. CIMA has published its own summary as *Anti-Money Laundering: what every accountant must know*. This is available as a downloadable PDF document from this website, or in hard copy from Professional Standards. A new edition, incorporating guidance on the Money Laundering Regulations 2007, will be available later in 2007.

Customer due diligence (CDD)

CIMA registered Members in Practice must perform CDD when taking on a new client, or when starting a possible contract or transaction with a person or company. CDD should eventually be extended to relationships with an established supplier. CIMA Members in Practice (described as 'external accountants' in the draft Money Laundering Regulations 2007) are required to perform CDD, and CDD should be considered for use by all members, not just those in practice, as a routine means of establishing identity for business activity. This is risk based to an extent; in some circumstances simplified CDD is acceptable, and in others enhanced CDD may be required.

CDD was formerly known as KYC (know your client) but the regulations are now quite specific about the requirements. Essentially, CIMA members must demonstrate to their supervisory authority that they have taken the proper measures in line with the risks. If necessary, they must involve the Serious Organised Crime Agency (SOCA), the Police or the Crown Prosecution Service. CDD is now an essential part of the client business relationship.

CDD means:

- identifying and verifying the customer's identity using documents, data or information obtained from a reliable and independent source
- where applicable, identifying the beneficial owner and taking risk based and adequate measures to verify their identity
- obtaining information on the purpose and intended nature of the business relationship
- conducting ongoing monitoring of the business relationship.

This ongoing monitoring should include:

- Scrutiny of transactions undertaken throughout the business relationship. This is to ensure that transactions are consistent with the accountant's knowledge of the client, the business and risk profile.
- Ensuring that documentation, data or information held is kept up to date, and carefully filed in hard copy.

Enhanced customer due diligence

Enhanced due diligence must be performed where the situation clearly represents a higher risk of money laundering, for example, when the client is not present. This is covered in Regulation 10 of MLR 2007. Enhanced due diligence is particularly important when the client is a 'politically exposed person'.

Client not present

Where the customer has not been physically present for identification purposes, specific measures must be taken to compensate for the higher risk. At least one of the following measures should be applied.

- Ensuring that the customer's identity is established by additional documents, data or information.
- Taking supplementary measures to verify or certify the documents supplied. Alternatively, confirmatory certification by a credit or financial institution which is subject to the money laundering directive, may be required.
- Ensuring that the first operational payment is carried out through an account opened in the customer's name with a credit institution.

Politically Exposed Persons (PEP)

A PEP is an individual who is or has, at any time in the preceding year, been entrusted with prominent public functions. PEP status also applies to an immediate family member or a known close associate of such a person.

This is particularly important for people outside the UK, or for those entrusted with a prominent public function by a state other than the UK, the European Union or an international body, at any time in the preceding year. CIMA members are responsible for deciding whether a person is a known close associate of a PEP. They should pay attention to any information they have or which is publicly known.

In respect of a business relationship or occasional transaction with a PEP, CIMA members are classed as a 'relevant person' and must:

- have appropriate risk based procedures to determine whether the customer is a PEP
- have senior management approval for establishing a business relationship with such a person
- take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction
- conduct enhanced ongoing monitoring of the business relationship.

Simplified due diligence

Regulation nine of the new regulations essentially says that Simplified Due Diligence (SDD) may be used where the client is:

- a credit or financial institution subject to the money laundering directive requirements
- a listed company in the European Economic Area
- the beneficial owner of a pooled account held by a notary or other independent legal professional
- a public authority in the United Kingdom.

SDD may also be used where the product is:

- a life insurance policy (subject to limitations of premium)
- an insurance policy for a pension scheme (if there is no surrender clause and if the policy cannot be used as collateral)
- a pension, superannuation or similar scheme which provides retirement benefits to employees (subject to conditions)
- electronic money (see Article 1(3)(b) of the electronic money directive), where:

  If the device cannot be recharged, the maximum amount stored in the device is 150 Euro
  or

  If the device can be recharged, a limit of 2,500 Euro is imposed on total transactions in a calendar year. This is unless the bearer redeems an amount of 1,000 Euro or more in the same calendar year.

A credit or financial institution situated in a non European Economic Area State, which imposes requirements equivalent to those laid down in the money laundering directive, and is supervised for compliance with those requirements.

It is highly advisable to read Regulation 9 before proceeding. There are other limited circumstances where SDD may be used. SDD does not require CIMA members to apply the normal CDD measures if there are reasonable grounds to believe that the client, product or transaction is covered by the above instances.

Suspicious activities and suspicious activity reports

It is difficult to describe exactly what constitutes suspicious activity, to some extent this is a gut feeling that something is wrong. An individual may feel that a client has funds that are unaccounted for, a dubious background or that the character of the business relationship has changed.

A suspicious situation must be reported to SOCA without delay. It is possible to report electronically using the SOCA website or to download faxable forms. A sole trader or a small partnership will probably do this themselves, but a larger firm must designate a specific person as the Money Laundering Reporting Officer who is responsible for liaison with SOCA.
www.soca.gov.uk/financialIntel/disclosure.html#forms
[Accessed 20 May 2008]

The purpose of filing a suspicious activity report (SAR) is for CIMA members to obtain consent to proceed with the transaction. Even where consent is not given, the form allows members to provide SOCA with as much information as possible.

Consent typically takes up to a week. The larger the sum of money involved, the more likely it is that SOCA will take an interest. It is important to avoid tipping off the client or prospective client, as tipping off is an offence under the Proceeds of Crime Act. It may result in fines and prison sentences for compromising an investigation. Sometimes the client may perceive a delay in dealing with his or her account. This leads to difficulties, and it may be as well to prepare appropriate 'excuses' for such delays. Here it would be unwise either to lie or to suggest to the client that the process would be brief.

There have been real life situations which can involve threats of kidnapping or bodily harm, despite the legal sanctions. Criminals have little compunction about the lives of unwitting intermediaries who may get in their way. It is best to refuse business if a client is deemed to be suspicious.

Legal professional privilege

Under the UK's Proceeds of Crime Act (POCA) and Money Laundering Regulations (MLR), the courts regard the client's right to confidentiality with a legal adviser under so called professional privilege as fundamental to the right of access to legal advice. Apart from lawyers, only patent agents, trademark agents and licensed conveyancers had previously been granted such privilege.

After representation, this right of professional privilege was extended to accountants (not just auditors) and tax advisers with regard to money laundering only. To qualify, tax advisers must be members of appropriate professional bodies, referred to as 'relevant professional advisers'. These advisers now include members of the CCAB bodies, including CIMA.

'Professional privilege relates to information communicated by a client or his representative in connection with the giving of legal advice or in connection with legal proceedings or contemplated legal proceedings, but does not apply to information communicated with the intention of furthering a criminal purpose (including laundering money).'

Law Society of England and Wales

The following information is covered under legal professional privilege:

- advice on the interpretation or application of any element of tax law
- advice on the legal aspects of a takeover bid, for example, the Companies Act legislation
- advice on duties of directors under the Companies Act
- advice to directors on legal issues relating to the Insolvency Act 1986, for example, on the legal aspects of wrongful trading (not applicable to CIMA members). Advice on employment law
- legal Professional Privilege normally applies when a client is either unwittingly involved or not directly involved in money laundering, and requires advice from a legal adviser in an accounting or taxation context. Advice may be given and the accountant is not required to report to SOCA about the client
- exemption from making a money laundering report does not apply where the services provided will be used to further a criminal purpose. However this exception is complex and further legal advice should be sought before a decision is made.

Further information

CIMA Articles

Nimmo, M. *Government targets fraud with tougher legislation.* Insight, March 2007. Available from: **www.cimaglobal.com/insight**
[Accessed 20 May 2008]

Nimmo, M. *Professional privilege puts accountants in the legal spotlight*. Insight, August 2006. Available from: **www.cimaglobal.com/insight**
[Accessed 20 May 2008]

Nimmo, M. *Money laundering laws force new 'know your client' procedure.* Insight, June 2006. Available from: **www.cimaglobal.com/insight** [Accessed 20 May 2008]

Nimmo, M. *How to beat charity fraudsters* in 'Come hell or high water.' Financial Management, February 2006, pp14-17. Available from: **www.cimaglobal.com/insight** [Accessed 20 May 2008]

Nimmo, M. *Money laundering: financial crime and terrorism are global issues.* (PDF 496KB). Financial Management, November 2005, pp28-29. Available from: **www.cimaglobal.com/financialmanagement** [Accessed 20 May 2008]

Articles

Abstract only from Business Source Corporate available from: **www.cimaglobal.com/mycima** [Accessed 20 May 2008]

Choudhury, C. *Safety first*. Accountancy Age, 05/10/2006, p. 16-17

Council approves rules on the tracing of fund transfers in order to better combat terrorist financing. Accountancy Ireland, December 2006, Volume 38, Issue 6, p. 34

Solicitor group's role more than sticking to the rules. Accountancy, November 2006, Volume 138, Issue 1359, p. 108

AccountancyAge: damned if you do, damned if you don't. Accountancy Age, 28/09/2006, p. 15

Cycle of crime. Accountancy, September 2006, Volume 138, Issue 1357, p. 43-44

Whistleblower. Accountancy, August 2006, Volume 138, Issue 1356, p. 21

ICAEW issues money laundering tips. Accountancy, April 2006, Volume 137, Issue 1352, p. 109

Books

Graham, T., Bell, E. and Elliott, N. (2006). *Money laundering.* London: LexisNexis Butterworths Tolley. (Butterworth's Compliance Series)

Lilley, P. (2006). Dirty dealing: the untold truth about global money laundering, international crime and terrorism. London: Kogan Page

Muller, W., H., Kalin, C. and Goldsworth, J. (2007). *Anti-money laundering: international law and practice.* Chichester: John Wiley and Sons

Reuter, P. and Truman, E. (2004). *Chasing dirty money: progress on anti-money laundering.* Washington D.C: Institute for International Economics

Schott, P. (2006). *Reference guide to anti-money laundering and combating the financing of terrorism.* Washington D.C.: The International Bank for Reconstruction and Development/The World Bank/The International Monetary Fund

CIMA Mastercourses

Money laundering: dispelling the myths. To book via
www.cimamastercourses.com
please go to Find and key in the course code MOLA.

Websites

Money laundering: how it is done and what is being done about it
A guide to sources **http://digbig.com/4wxry**
[Accessed 20 May 2008]

Institute of Chartered Accountants in England and Wales
Money laundering web page
http://digbig.com/4wxsa
[Accessed 20 May 2008]

Web resources for money laundering regulations
Selected by solicitor Delia Venables
http://digbig.com/4wxsb
[Accessed 20 May 2008]

Other information

How SMEs can reduce the risk of fraud (2005) Brussels: FEE. (Free download)
http://digbig.com/4wxsc
[Accessed 20 May 2008]

Fraud Risk Management bibliography on CIMA website
http://digbig.com/4wxsd
[Accessed 20 May 2008]

First published in 2006 by:

The Chartered Institute of Management Accountants
26 Chapter Street
London SW1P 4NP
United Kingdom

Printed in Great Britain