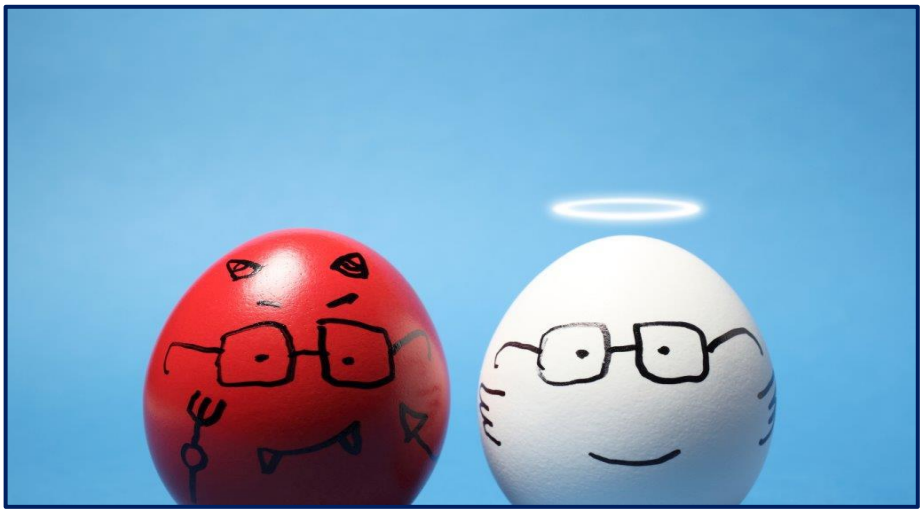
CCAB case studies



Helping professional accountants recognise and fight economic crime

OCTOBER 2016

FOREWORD by Anthony Harbinson, Chairman, CCAB Anti-Money Laundering Task Force, and Director of Safer Communities, Northern Ireland Department of Justice

The threat from economic crime has never been more pressing. Enormous sums of money are lost to fraud and corruption every year, but these crimes also cripple lives as well as livelihoods. Economic criminals – especially the organised variety – are ruthless and determined. Many of them possess great skill, ingenuity and cunning.

The UK bodies who represent the professions have recently come together to renew their commitment to the fight against economic crime. Our joint statement can be found on page 36. A key part of this commitment is to support our members with the tools, skills, insights and knowledge they need both to protect themselves from the ravages of economic crime and, in so doing, to safeguard the wider economy.

These case studies and supporting commentaries, developed by the UK and Ireland's Consultative Committee of Accountancy Bodies (CCAB), are part of that support. They have been designed to illuminate some of the many and varied ways in which professional accountants might unwittingly enable an economic crime or come into close professional contact with people who are knowingly complicit. Ten scenarios cover a range of situations. Each outlines the key areas in which offences might have been committed as well as highlighting the issues that would need to be considered when trying to identify and assess the risks. I hope you will find them useful.

Because we are among the 'gatekeepers' of legitimate finance we are very much in the frontline of the fight against economic crime. Deceiving or corrupting trusted professionals is a feature of many a criminal scheme and frequently a prerequisite of its success. This is a fact of modern commercial life that places a great burden of responsibility on us all. Nonetheless, armoured by our strong ethics and equipped with the right knowledge and skills, we can be equal to the challenge.

About CCAB

The combined membership of the five CCAB bodies – ICAEW, ACCA, CIPFA, ICAS and Chartered Accountants Ireland – amounts to 260,000 professional accountants in the UK and the Republic of Ireland (380,000 worldwide).

CCAB provides a forum for these bodies to work together in the public interest on matters affecting the profession and the wider economy.

CCAB's credibility stems from its insight into all areas of finance and accounting: from finance directors and audit partners to management accountants, professional advisers, public sector finance leaders and entrepreneurs. CCAB's members are active as key decision makers and business leaders throughout the financial value chain, in all sectors, both within the UK and around the world.

Contact

Sharon Grant

Manager, CCAB

sharon.grant@ccab.org.uk
+44 (0)20 7920 8494
Further copies of this report can be downloaded at
http://www.ccab.org.uk/documents/Economiccrimemanifesto2016

Published by CCAB Ltd
PO Box 433 Moorgate Place London EC2P 2BJ
United Kingdom
www.ccab.org.uk

INTRODUCTION

The (un)professional enabler

The term 'professional enabler' is often misused to describe someone who does not necessarily belong to one of the professions but who does work in the regulated sector[1] and has in some way helped an economic crime succeed.

The actions (or inactions) of many of these enablers are anything but professional. A more useful distinction can be draw between two different types of enabler:

- the complicit or negligent; and
- the unwitting.

Members of the first group are by definition always acting in an unprofessional manner because they intentionally give criminals access to the legitimate financial system.

Members of the second group learn the hard way how easy it is for even a conscientious professional to be sucked into a criminal transaction. If we doubt this we underestimate the enemy. And if we become complacent about the threats that economic crime and criminals pose for accounting professionals then we do some of the criminals' work for them and we magnify the already significant risks we face.

Whilst it is not inconceivable that accounting professionals might find themselves unwittingly embroiled in, say, the trafficking of drugs or the theft of physical property, it is in economic crime that we are uniquely well-placed to contribute to crime fighting.

Even so, there are many economic crimes which in no way rely on the involvement of an accounting professional for their success; in other words, where the contribution they could make would be no more significant than an unqualified individual because the exercise of their professional skill is not integral to the crime.

This means that there is another important distinction to be drawn here: between a level of involvement that is almost incidental and, on the other hand, true 'enabling', which implies a degree of involvement in events that is so fundamental as to make the crime impossible without it.

The unwitting enabler

Accountants are a key part of that select group of professionals within the regulated sector who collectively act as gatekeepers of the legitimate economy. While a courier may assist a drug manufacturer in trafficking (see the recent indictment of FedEx for conspiracies to traffic in controlled substances and misbranded prescription drugs) or a hacker might be employed by a company to acquire the restricted content of a competitor's IT systems, lawyers and accountants are in a position to provide access to the very financial system itself.

[1] For the purposes of anti-money laundering, the UK regulated sector includes credit institutions, financial institutions, auditors, insolvency practitioners, external accountants, tax advisers, independent legal professionals, trust or company service providers, estate agents, high value dealers and casinos.

Money launderers often need the advice and services of specialised professionals to facilitate their illegal financial operations. By creating corporate vehicles, making available client money accounts, transferring proceeds, filing fraudulent tax returns, advising on transactions or even providing tax planning advice, those professionals (unwittingly or otherwise) simply unlock the gates they are supposed to be guarding.

Inevitably the accountancy profession can be let down from time to time by a small minority of rogue members. These are the complicit and negligent ones we mentioned above; people willing to act as knowing enablers and purposeful facilitators of economic crime, or else simply to turn a blind eye.

The vast majority of accountants take their gatekeeping responsibilities very seriously indeed and seek, to the best of their ability, to use their professional skills to thwart economic crime. But that does not mean our professional training somehow inoculates us against deception. Criminal schemes are often very sophisticated, with complicated structures designed to disguise the true source and ownership of money and other assets even from expert eyes. Simple schemes too can be accompanied by genuinely persuasive explanations and convincing documentation, all carefully contrived to lend legitimacy and to hide the truth beneath a thick blanket of plausibility.

In other words, for professional accountants to avoid becoming unknowingly embroiled in a criminal scheme they need to remain vigilant at all times, of course, and to make good use of their professional skills. But more than that they must lean heavily on the strong defences provided by the profession's ethical guidance and procedures.

Professional ethics also protect the professionals

Breaches of the law and regulations should not be considered in isolation from breaches of professional ethical codes. Many jurisdictions have complex systems regulating a range of activities thought to be vulnerabilities in the economy at large. Various regulatory and professional bodies are thus empowered to impose on their regulated populations (individuals and businesses) general and specific standards and disciplines. Regulatory infringements are typically punished by administrative means, with severe criminal penalties reserved for the more serious or persistent breaches.

All CCAB accountants are required to follow a formal code of ethics. In many situations in which an accountant has committed a serious regulatory infringement or criminal act, that ethical code is likely to have been breached first. In this way the code of ethics can be seen as a first line of ethical defence for accounting professionals who find themselves in difficult situations.

- If professional accountants knowingly enter into relationships with criminals, and become knowingly involved in transactions likely to involve the proceeds of crime, they are displaying a lack of integrity and behaving unprofessionally because their very involvement is likely to bring discredit to the profession.

- Financial crimes are often preceded by ethical breaches. The unethical behaviour then provides the foundations for subsequent breaches of the law and regulations.

- If the risk assessment procedures of professional accountants are entirely inadequate then even before there is complicity in any crime their lack of client due diligence is a breach of the fundamental ethical principles of professional diligence, competence and due care.

- And if professional accountants turn a blind eye to certain irregular behaviours or transactions simply because of the potential for financial reward (as happened in a number of recent, high profile money laundering cases) then how can they be said to have acted objectively or (therefore) ethically?

Ethics and compliance

Well-rooted ethics can make an important contribution to compliance. If a compliance culture lacks strong and explicit ethical foundations it tends to become purely rule-based. In other words, the rules themselves become the last word on a given decision, inviting overly-legalistic thinking in which obedience to the letter of the law becomes the prime objective.

By contrast an ethical culture is values-based and it is those values that underpin each rule or policy. Here employees are expected to know and follow the rules and policies, but they are also expected to exercise good faith and sound judgement in seeking to honour the spirit (the intended purpose) of those rules. Ethics can also guide the 'how' of our decision-making (the way we think, our motives), not merely the actions or inactions which are the final outcomes.

Professional accountants should be well-equipped in this regard. They will have received formal training in ethical analysis. They should be able to draw on long experience of following and applying an ethical code. Their sense of professional scepticism will have been keenly honed over the years. But there is no room for complacency.

Fraudsters too have their own, often sophisticated, toolkit with which they pursue their objectives, one of which is to hoodwink otherwise conscientious professionals. We must expect them to bring their A-game to the criminal job-at-hand and we must never underestimate them as manipulators and adversaries. To this end, these case studies are intended to:

- highlight the key areas of risk;
- help to identify some of the ethical issues;
- outline the kinds of economic crimes professional accountants can most commonly help combat; and
- draw attention to the challenges posed by a commercial accounting environment in which criminals are often one step ahead.

However, they are not part of the formal guidance of CCAB member organisations. You may find it useful to seek further information from the advisory services and websites of your own individual CCAB body. The IFAC website is another useful source of information.

As ever we welcome feedback both on the issues raised by this document and what might be done to improve or expand its contents. To get in touch please e-mail admin@ccab.org.uk

Economic Crime

The term ‘economic crime’ can be difficult to define but it is generally accepted as an umbrella term for a group of all too familiar offences. Over time new financial crimes will emerge and criminals will adopt new technologies and strategies. But today, generally-speaking, there are six main types.

Bribery and corruption

Corruption is the misuse of one’s position or office to commit crimes which can include theft, extortion and the soliciting of bribes. Bribery is the paying or offering of an illegal inducement, usually in exchange for an unfair and illegitimate advantage. An organisation commits an offence of enabling if it consents to a bribe being paid on its behalf. But it would also have committed an offence (of omission) if someone committed bribery on its behalf and the organisation could not show that its procedures for preventing bribery were adequate nonetheless.

Money laundering

This is the illegal handling of the proceeds of one or more criminal offences with the intention of obscuring the true origins of the money so that it can be enjoyed by the criminals openly or used to commit further crimes. Professionals enable money laundering, whether knowingly or unknowingly, whenever they help criminals gain access to the systems used by legitimate finance.

Fraud

Fraud is the act of gaining an illicit advantage through deception, in particular by manipulating financial information or accounting records. One of the most famous cases of corporate fraud was Enron, where the CFO was himself actively involved in overstating earnings and concealing debt. The Enron case is a prime example of how specialist knowledge and a trained intellect can be used criminally to muddy the waters of corporate reporting.

Tax evasion

When the law is broken in order that taxes legally due are not paid then businesses and individuals have evaded, rather than avoided, taxation. In 2014 an accountant with no formal accounting qualifications and no membership of a professional body was jailed for tax fraud. He had understated his clients' earnings and overstated their expenses in order to reduce their tax liabilities, then kept the tax refunds for himself. HMRC launched an investigation after a number of his clients complained.

Intellectual property theft and other information breaches

An intellectual property violation is generally the unauthorised use of privately-owned information. The information itself can take many forms, including scientific or technological developments, original designs and works of art or performance. The violations can include industrial espionage (including the illegal accessing or hacking of computer systems), copyright piracy and the sale of counterfeit goods.

Cybercrime

This is a very broad category because any crime committed using a computer or network is a cybercrime; criminals make extensive use of e-mail, internet banking, online systems and mobile technology just like everyone else. Cybercrime typically involves the intent to cause harm – whether to individuals, organisations or infrastructure – or to commit financial or identity theft. Hacking; the development and distribution of malicious software; the use of false identities to open accounts and obtain credit or cash: these are all cybercrimes. The swift, invisible and often remote manner of these crimes means that individuals or organisations can easily become unwitting enablers simply by ignoring a warning sign or having inadequate controls to protect their own systems.

Case study 1

Money laundering

While carrying out work for a convicted criminal, accountant S allowed £50,000 to pass through his firm's client money account. Initially he did not realise the cash had come from a criminal source but he continued to work for the client even after he became sufficiently concerned to file a suspicious activity report (SAR) with the National Crime Agency (NCA). The court accepted that he had been a naive victim of a sophisticated criminal.

(Suggested discussion points can be found on the pages following.)

Case study 1: **Money laundering** *(continued)*

1. Which money laundering offences might have been committed by this accountant?

Part seven of the *Proceeds of Crime Act 2002* (POCA) includes the following money laundering offences:

Section 327 – concealing, etc.
Concealing, converting, transferring or disguising criminal property, or removing it from the UK.

Section 328 – entering into an arrangement
Entering into an arrangement, or becoming involved in one, which you know or suspect facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.

Section 330 – failure to disclose (regulated sector)
Knowing or suspecting (or having reasonable grounds for either) on the basis of information acquired in the course of regulated business that someone is engaged in money laundering and yet failing to disclose those facts as soon as possible.

2. What are the penalties for these offences?

Offences under s.327 and s.328 (as well as s.329)

- Summary conviction – a maximum of six months' imprisonment and/or a fine not exceeding the statutory maximum.
- Conviction on indictment – a maximum of 14 years' imprisonment and/or a fine.

Offences under s.330 (as well as s.331 and s.332)

- Summary conviction – a maximum of six months' imprisonment and/or a fine not exceeding the statutory maximum.
- Conviction on indictment – a maximum of five years' imprisonment and/or a fine.

3. How might he have reduced the risks or defused them altogether?

Perfectly straightforward examples of good practice could easily have protected him from much of what he did wrong.

- Better know-your-client procedures might have identified the criminal connection earlier.
- Continuing due diligence procedures – particularly where unusual transactions fall outside the normal run of business – are an essential part of anti-money laundering compliance.

Case study 1: **Money laundering** *(continued)*

- The firm's professional body most likely has strict regulations governing the operation of a client money account. In any case the firm should have had its own strict control procedures including scrutiny of the purposes to which the account is being put.

- Wilful blindness, fear and simple ignorance of the Money Laundering Regulations (including the duty to report and seek consent for disclosures) are all suggested by this accountant's decision to continue working after suspicions arose. Adequate training might at least have remedied his AML ignorance.

4. What should he have done about his suspicions?

He could simply have made the commercial decision to end the relationship before the transaction was processed. As a professional he has every right to choose for whom he will work as well as to resign without explanation (as long as he takes care not to reveal his suspicions – this would constitute tipping-off in the eyes of the law).

Once suspicions had arisen his decision to make a SAR was the right one. But in circumstances like this, where there is a risk that any unexplained or unexpected actions might inadvertently alert the suspect to your suspicions, it is advisable first to seek legal advice. When making the SAR he should also have sought the NCA's permission to proceed (a so-called consent request) so that law enforcement could follow the money, gather valuable intelligence and bring the criminal to justice more quickly. In transferring what turned out to be criminal property the accountant had himself committed an offence; a successful consent request would have protected him from prosecution under s.327 of POCA.

Case study 2

Money laundering

G was a solicitor whose client asked him to transfer a property (valued at £150,000) to a professional contact who ran an estate agency. The consideration for the transfer was just £43,000 (the value of the outstanding mortgage). The solicitor received a fee of £399 for his work.

Later it emerged that the sellers were drug dealers who had originally purchased the property for £83,000 (£40,000 in cash, the rest borrowed). They had since been convicted and imprisoned. The property – viewed by the Crown as criminal proceeds – was now the subject of confiscation proceedings.

G was arrested and put on trial alongside the estate agent. According to the prosecution the transfer was intended primarily to frustrate the confiscation proceedings and the solicitor and estate agent should have realised proceeds of crime were involved when the property was so grossly undervalued.

The solicitor claimed he had no knowledge or suspicion that the property was a criminal asset; the co-defendant (the estate agent) had told him the sale was to help some friends in financial difficulties.

The solicitor was convicted of failure to report, contrary to s.330 of POCA, and sentenced to 15 months' imprisonment.

The estate agent was convicted of entering into an arrangement contrary to s.328 of POCA and of acquiring criminal property contrary to s.329. He was sentenced to a total of three years' imprisonment.

(Suggested discussion points can be found on the next page.)

Case study 2: **Money laundering** *(continued)*

1. Where are the red flags?

Proper due diligence might have identified a money laundering risk attached to the original source of income.

The sale of the property at significantly below market value should also have sounded alarm bells.

A property purchase with an estate agent as principal might be thought to represent a transaction outside the run of normal business practice. Even moderate levels of professional scepticism might have led the solicitor to question the adequacy of the explanation he'd been given.

All of this should have taken place before any client identification procedures. A practitioner cannot ascertain what sources and quality of evidence are required without first carrying out an adequate risk assessment, which should include the sources of income/property and the circumstances of the relationship/transaction.

2. Beyond the legal penalties, what are the wider consequences of a money laundering conviction for the practitioner?

Knowing involvement in crimes of this sort strikes at the very heart of who we are and how others see us. The consequential harm of a conviction can go wide and deep: damaging marriages and family life; tarnishing professional and personal reputations; destroying jobs and careers; undermining assets and future financial security; ruining health.

Indeed, these were the very terms in which the solicitor appealed against what he believed was a 'manifestly excessive' sentence. He submitted that the offences had involved a lapse in the high standards expected of a solicitor rather than a desire to engage in criminal activity; in spite of his previous good character, and even though he had made no financial gain besides the conveyancing fee, the consequences of his conviction and imprisonment had been catastrophic – his practice lost, struck off as a solicitor, and with dramatic consequences for his finances, personal life and health. The period of imprisonment was, therefore, reduced.

Case study 3

Money laundering

M is the UK money laundering reporting officer (MLRO) for Xavier LLP, an accounting firm which is now an international operation having recently acquired a number of overseas offices. Aggressive foreign expansion has been expensive and the firm is now expected to focus on winning new business and keeping costs as low as possible for the next two years.

Xavier LLP's customary risk assessment system operates on a points basis. Potential customers are awarded scores according to just two factors: whether they are located in a high-risk country, and the nature of the work on offer. The majority of risk points are derived from location so most customers, who are not based in high-risk countries, tend to be classified as normal risk. The firm categorises high-risk countries using a well-known index published by an independent non-profit organisation. Even so, all work referred to the UK by its new international offices is also treated as normal risk because the firm now has a single set of customer due diligence (CDD) policies and procedures for its worldwide operations and is part of a network of what it considers to be trusted referrers.

It is clear to M that the international business development plan has been successful; an overseas member of the network recently referred some work to the office in Erehwon (a high-risk country) part of which (some UK tax planning advice) was then passed to the UK firm in which M is located. The services in question – which will involve the purchase of various UK assets – are to be provided to an individual and to a newly-established company (of which the same person is a director).

The new customer was not physically present for identification purposes (not unusual in Erehwon) but the points system assessed the risk as normal because he and his company are not based in a high-risk country. The funding source for the asset purchases has been recorded as an asset disposal. On paper the company's business seems relatively uncontroversial.

The documentation received by M was sent by a junior member of the Erehwon office; the engagement partner has been unavailable for several weeks, enjoying the hospitality of the new client's luxury yacht. The UK deputy MLRO, whose job it is to review the documentation, has already raised concerns about the due diligence of the Erehwon client acceptance procedures, but his concerns were deemed 'inconsistent with strategic objectives'.

For a number of months this fruitful new client relationship continued without incident but then it became apparent that the beneficial owner of the company was a high profile member of a notorious drug trafficking cartel, well known to his own local media. The funds used to set up the company in question had indeed come from an asset disposal – 88 kilos of Trujillo cocaine.

Xavier LLP is now the subject of close regulatory attention and dealing with severe reputational damage. M is facing similar problems, but in a personal capacity.

(Suggested discussion points can be found on the pages following.)

Case study 3: **Money laundering** *(continued)*

1. What deficiencies are there in the firm's AML systems?

The culture of the firm appears to place commerciality over compliance; this is clearly visible in the aggressive approach to expansion and the decision to disregard the concerns of the deputy MLRO ('inconsistent with strategy').

Though there is no explicit reference to cuts in the compliance budget, from the details provided we can infer that resources might be stretched too thinly. The firm has been made especially exposed by its expansion into what appear to be riskier regions. In the Erehwon office itself, for example, we might wonder why there seems to be no-one who isn't either a partner or a junior available to conduct communications with the UK.

It is questionable to rely solely on a public-domain index from a non-profit organisation to assess geographic risk. Multiple sources should be used, including (for example) the Financial Action Task Force (FATF) list of high-risk and non-cooperative jurisdictions. There also appears to be an excessive preoccupation with geography at the expense of other factors such as service, channel and client risks.

It is dangerous to treat all work referred by an international office as normal risk by default, particularly when there is so much evidence to suggest that the firm-wide AML policies are not being enforced (people in Erehwon seem to have their own way of doing things). We might also want to interrogate the reality behind the term 'trusted referrers' and to consider the implications for CDD; Erehwon is itself a high-risk country.

Why was the end-customer classified as normal risk even though he was not present for client identification purposes? This alone should have made him and his company high-risk by default, resulting in enhanced due diligence (EDD). In fact there appears to have been no effort made to carry out any CDD on the beneficial owner and there is no mention of EDD in the scenario at all. Some additional questions were asked about the funding source and the nature of the business but the evidence is simply not detailed enough, pointing to an essential lack of professional scepticism.

When the information provided to the UK firm came from a junior member of the Erehwon team further concerns should have been raised. This suggests either a shortage of resources, or a lack of supervisory control, or both. Since there is no mention of a dedicated AML resource in Erehwon we should expect evidence of at least some direct communication between the engagement partner and the UK MLRO.

The engagement partner's client socialising is, at best, a strong indication that self-interest and personal familiarity are undermining objectivity and professional scepticism. The firm's policies on gifts and hospitality might already have been breached and so too might the anti-bribery legislation. At worst there could even be direct complicity in economic crime.

The legitimate concerns of the UK deputy MLRO were brushed aside even though the criminal connections of the beneficial owner don't seem to have been much of a secret. Just because the news hadn't reached the Erehwon media, never mind the UK's, that is no excuse; basic know-your-client work using internet media searches was not done.

Case study 3: **Money laundering** *(continued)*

2. How culpable was senior management?

This case illustrates a particular problem that is more likely to arise in larger or expanding organisations: complicity or recklessness at ground level coexisting with weak control or naivety higher up. There should be no delegation without supervision, but difficulties also arise if the dividing line between delegation and supervision becomes blurred. It would be reasonable to expect that:

- when shortcomings are highlighted senior management makes sure they are addressed satisfactorily, with suitable new or amended procedures put in place;
- a risk-based approach to anti-money laundering is capable of diverting compliance resources to high-risk areas;
- a consistent group-wide due diligence system not only exists, but is enforced to stop any part of the business acting as a weak link; and
- a culture of openness and transparency is fostered to encourage everyone to raise their concerns internally without fear of reprisals.

3. What qualities does an AML team need to deal effectively with situations like this?

- Individuals should possess strength of character, independence and integrity. The latter is vital in any AML role, but especially in compliance. Team members need to be willing to challenge non-compliance and make sure that policies and procedures are being followed.
- Good communication skills are needed so that the key messages are delivered to the right people, in the right way, and in a timely manner.
- Good 'translation' skills will be required to distil relatively technical subject matter into a plan that can be easily digested by all.
- Alertness and a heightened sensitivity to risk are both vital – along with a healthy dose of professional scepticism.
- Detailed knowledge of the firm's business, as well as its systems, strategy and governance structure.
- Detailed knowledge of the legal frameworks governing the firm's business operations.

4. What is the culpability of the MLRO?

The MLRO exposed the firm to unacceptable risks by failing to take reasonable care to create and maintain adequate AML systems and controls. Similarly, procedures for assessing the risks posed by new customer prospects are inadequate, with no EDD performed in the case of higher-risk customers.

Case study 3: **Money laundering** *(continued)*

Systems and controls to support the firm's expansion (including ongoing review and monitoring procedures) also appear to be either absent or inadequate. Nor is there any evidence that he has acted to address any shortcomings – with, for example, training and/or new mechanisms to make sure senior management had what it needed in terms of information and analysis about the operation and effectiveness of the AML systems and controls.

5. What recommendations might you make to Xavier LLP?

The firm should undertake an urgent review of all its AML procedures and consider enlisting expert help from outside the firm. Where AML deficiencies are reported it must act immediately.

The strategic objectives should be re-examined. Does the firm really want to do business in countries with high corruption risk? If so, then appropriate AML systems and procedures must be introduced throughout global operations. Training for all staff on the key points of the legislation, regulations and codes of conduct (along with assessment to make sure it has been absorbed) is also essential. Depending on the outcome of the strategic assessment the firm should hire additional dedicated AML staff worldwide.

To strengthen AML coordination processes and reduce risks there should be routine information sharing between all of the firm's AML teams. CDD procedures should be strengthened and some of the default 'normal' risk categorisations withdrawn.

Rather than relying on a single third-party index the firm should make proper use of government or FATF guidance as well as the findings on money laundering prevention in particular countries or jurisdictions. More use should also be made of the advisory notices issued by some domestic authorities – in the UK these include HM Treasury and the NCA.

It was a serious mistake not to investigate the origins of the funding and seek sufficient evidence of legitimacy. When a customer's funding source is said to be the proceeds of a property sale evidence of ownership and the sale itself should be obtained.

When a customer is not physically present they should be automatically deemed high-risk. Since the key risk here is identity theft the customer's identity needs to be clearly established with sufficient extra documentary evidence.

Given the recent behaviour of the engagement partner the firm might also benefit from a review of its ethics policies to identify and mitigate threats to objectivity. Records of these matters and the associated discussions they trigger should form part of the client file notes.

In fact the firm's whole culture requires a rethink. An essential part of maintaining adequate firm-wide AML systems is that the importance of AML procedures receives clear and public support right from the very top of the organisation – which is clearly not happening here.

Case study 4

Cybercrime – corporate identity theft

K is an accounting firm employee. She has recently completed her training contract and is now being contacted by recruitment consultants. One of these calls outlines a job that sounds too good to be true. The discussion quickly turns to K's client portfolio and the structure of her firm. The head hunter seems to know (and be on good terms with) a number of K's colleagues. He promises to call back soon with more details of this fantastic opportunity.

In the pub that evening a member of the finance department (who received a recruitment call similar to K's) can be heard bragging to colleagues about a great new career opportunity that is coming his way – that is when he's not complaining noisily about the firm's 'woefully inadequate' IT systems.

Not long after, some of the firm's clients start to receive correspondence from someone purporting to be K telling them that certain transactions on which K's firm has been advising now need to go ahead quickly and that they must make the necessary bank transfers urgently. Some clients have already made their transfers and are now contacting the firm to check on progress.

It soon emerges that the firm's systems, including its customer ledger information, have been hacked over the weekend. The transfers made by clients were in fact diverted into a fake client money account set up by the criminals. The money has now disappeared.

(Suggested discussion points can be found on the pages following.)

Case study 4: **Cybercrime – corporate identity theft** *(continued)*

1. In what ways, if any, was this crime 'enabled' either by the firm or individual employees?

K and her colleague in finance are not only victims. Having been convinced by a fraudster to reveal sensitive information, they have become unwitting enablers. Without the information they provided the criminal plan may well have failed.

Any firm could find itself in a situation like this purely because of simple lapses in IT or information security and a failure to monitor client activity. Many cyber-attacks are launched at the weekend in the knowledge that there will be no-one around to notice the untoward activity. By Monday morning it is often too late.

2. Which fundamental ethical principle is K likely to have breached?

Confidentiality.

3. How would you stop this happening again?

Many cybercrimes include an element of old-fashioned, one-to-one deception (now called 'social engineering'). Professional accountants have skills which are often in high demand and they can receive many, sometimes flattering, calls from recruitment consultants. Of course employers and clients alike are owed a duty of confidentiality. But the sharing of detailed information about the firm and the affairs of its clients, as happened here, can easily become much more than a breach of confidentiality by actively enabling a fraud or cyber-crime that might otherwise have fallen at the first hurdle.

All employees should receive regular training on the ethical requirements of their role, the nature of the fraud risks that threaten the firm and its clients, and what they can do to help prevent these kinds of crime. They should also be actively encouraged to think carefully about what information – especially work information – they share on social media, and to question the professionalism of their motives for doing so.

Meanwhile, the firm should:

- ensure that documents carrying sensitive information are destroyed securely;
- monitor online references to itself – this can help identify imposters;
- carry out a systems health-check – which could include tasking a consultant to attempt unauthorised entry to critical systems – and get professional advice on data security;
- educate staff on IT security and how to spot cybercrime red flags;
- follow the latest expert guidance (from GCHQ) on secure passwords – at least eight characters long, no dictionary words, change them only after a suspected or actual security breach;

Case study 3: **Money laundering** *(continued)*

- ensure that firewall and anti-virus software is up-to-date;
- use data encryption software in correspondence;
- make special efforts to protect access to applications like searchable databases – these can give criminals a way in; and finally
- remember: weak controls make crime possible.

Case study 5

Investment fraud

An investment company is relying on fresh deposits from new investors to pay returns to existing ones. Not only does the company have insufficient assets to back all deposits the assets it does have are not insured, even though investors are promised that they will be.

The investments are primarily being sold to pension investors by an independent financial advisor (IFA) who earns more than half the investment value of each sale as a commission. The same advisor submits false claims for services not rendered, pays the company director to overlook the accounting irregularities, and uses a complex web of offshore companies to disguise his ill-gotten gains.

Drake, the in-house accountant, receives a financial inducement for arranging the processing of these dubious invoices.

(Suggested discussion points can be found on the pages following.)

Case study 5: **Investment fraud** *(continued)*

1. Which economic crimes are being committed?

- Fraudulent trading
- Conspiracy to commit fraud
- Bribery
- Furnishing false information
- Money laundering

2. In what ways are these crimes being enabled by professionals?

The financial advisor is acting criminally on his own behalf as well as helping the investment company commit fraud.

The in-house accountant (naively or otherwise) is also helping by processing the dubious transactions.

3. What part should the professional scepticism of the in-house accountant be playing and which clues should have aroused his suspicion?

Professional scepticism is an attitude of mind that requires a questioning disposition and continuing alertness to the conditions which might point to misstatement, whether by error or fraud.

The clear evidence of bias and self-interest among everyone involved should have prompted a desire to investigate further and informed all decisions about what enquiries were needed to get to the objective truth. It is helpful in situations like this for accountants to put themselves in the shoes of an independent third-party observer and to ask: What questions would they expect me to ask? What matters would they expect me to challenge? What evidence would I require to satisfy those challenges?

Scepticism is also fundamental both to the perception and the reality of professional integrity. Accountants should never associate themselves with information they believe to be misleading – particularly when there are so many indications of management bias. Not that bias is the only cause for suspicion.

- For assets to be recorded in the company's books they would need to meet the basic criteria of existence, valuation and ownership rights and obligations. Closer investigation might well reveal discrepancies in these areas too.

- Such large commissions should sound alarm bells – if not for their suspect legitimacy then, at the very least, their sustainability.

- Duplicate invoices for identical amounts from connected suppliers are always suspicious. The same is true for unnecessarily complicated payment arrangements.

Case study 5: **Investment fraud** *(continued)*

4. What action might the in-house accountant have taken?

When professional accountants believe that others are behaving or acting unethically they should first consider raising the matter internally, either through the organisation's own whistle-blowing procedure (if there is such a thing) or by consulting management or whoever is responsible for governance. Alternatively, they may wish to seek the advice of their professional body and/or a lawyer.

In-house accountants are not usually subject to the UK AML regime with its requirement that suspicious activity reports (SARs) are made in accordance with POCA. However, that does not prevent them from making voluntary SARs or from reporting their concerns through other channels (such as Action Fraud). In this scenario the investment company would be regulated by the Financial Conduct Authority (FCA) and would therefore be required to have an MLRO to which an internal report should be made. And, since this is a situation in which the fundamental principle of confidentiality can be overridden, the conduct of the IFA could be reported to the FCA as well.

If all the available options for reporting and escalation have been exhausted, the in-house accountant might finally conclude that it is appropriate to resign.

5. Is anti-bribery law relevant in this situation?

The relevant law is found in the Bribery Act (2010). This says that a commercial organisation is liable to prosecution if a person associated with it pays a bribe with the intention of obtaining or retaining a commercial advantage. The company has a full defence only if it can show that it had anti-bribery procedures in place which should have been adequate to prevent the crime. These 'adequate procedures' would need to include: risk assessment, top-level commitment, proportionate procedures, due diligence, training and communication, monitoring and reviews. Any corporate lack of understanding or respect for the legislation would represent a substantial weakness in such a defence.

6. Do professional accountants have a role to play in this regard?

Yes they do. Even where such practices have become the norm, accountants can help prevent the paying of bribes by using their expertise and professionalism to act with integrity and by refusing to become associated with practices they know to be unethical or contrary to the law and regulations. They also have a role to play in educating others within the organisation by explaining the risks and potential consequences of bribery.

It is clear from the Bribery Act that to claim ignorance of your agent's activities would not constitute an adequate defence. Invoices and expenses claims should, in all likelihood, have required approval and processing in the accounts department. Invoices for round sums, or with bland descriptions such as 'hospitality' or 'client entertainment', should always be probed further (it can help to request itemised invoices). Reviews of expense categories (perhaps while preparing financial statements or tax returns) can offer extra opportunities to highlight additional areas of concern, which can then be followed-up through the appropriate internal channels.

Case study 6

Terrorist financing

Mr X, a customer of LoganBank, receives large cash deposits into his account. He says they are his wages from an employer in Iran.

Some of the money is used by Mr X to rent property in his country of residence. These transactions arouse sufficient concern for a LoganBank official to submit a suspicious activity report (SAR).

Mr X also owns a Syrian company and this also receives substantial transfers from Iran. Further enquiries reveal that the manager of this company has already been convicted of terrorism and that the company itself is caught up in an on-going anti-terrorism investigation. The cash deposits in Mr X's personal account do indeed prove to be linked to the financing of terror.

(Suggested discussion points can be found on the next page.)

Case study 6: **Terrorist financing** *(continued)*

1. Why can terrorist financing be considerably more difficult to spot than money laundering?

The main difficulty is that the money itself might be 'clean' right up to the moment it is used to finance a terrorist attack. There may be no typical trail of dirty or suspicious money to follow. This case is a good example of how by exercising due diligence a professional can avoid unwittingly enabling crime and instead help in the investigation and apprehension of the criminal.

2. Where are the red flags?

Again, we see the importance of adequate risk assessment as the first step in undertaking client due diligence. It is unlikely that simply obtaining documentary evidence of Mr X's identity would have brought the fundamental issue to light. A better, more secure approach would have been to make enquiries about the individual's business and the source of his income, both of which actions are an integral part of all good AML risk assessment.

The Financial Action Task Force (FATF) publishes this helpful list of the main red flags associated with terrorist financing.

- Unusual business activity.
- Inability to identify funding sources.
- Wire transfers made soon after cash deposits.
- International transfers of money from and/or to locations of specific concern (it helps to keep an eye on the list of high-risk jurisdictions maintained by HM Treasury and the Office of Financial Sanctions Implementation).
- Commercial or account behaviour that is atypical.
- Transactions with links to charities or relief organisations.
- Big cash transactions, particularly in areas with frequent terrorist and criminal activity.
- Media coverage of the account holder's activities.
- Large sums transferred between the accounts of people or newly-established companies with no apparent business relationship.
- Frequent cash deposits or withdrawals from charity accounts involving people with no apparent relationship.
- Unexplained transfers into the accounts of individuals and companies from foreign jurisdictions with a reputation for terrorist activity.
- Either the identity of an account holder or the destination of the transfer is supported by little, incomplete or unverifiable information.
- Frequent international transfers into and out of the accounts of companies created by the nationals of terror-prone countries.

Case study 7

Money laundering

A police operation identifies an in-house accountant who is believed to be part of a criminal organisation laundering the proceeds of drug trafficking.

He is an expert in financial instruments and his job is to make the sources of the criminal proceeds appear legitimate. He makes short-term investments which are quickly liquidated so that the proceeds can be reinvested. By primarily using electronic transfers he is able to spread the investments over numerous geographical areas, equities markets and overseas financial institutions. As far as possible he is also expected to make a profit.

(Suggested discussion points can be found on the next page.)

Case study 7: **Money laundering** *(continued)*

1. What red flags might an outsider notice?

Unnecessarily complex group structures and investments in areas with no obvious geographical connection can both be indications of money laundering. The absence of any obvious explanation for the structure of these transactions could be a sign that they are being deliberately set up to confuse and obscure. The use of complex financial instruments by a business with no obvious reason to do so can be a sign of the layering and integration stages of money laundering.

2. What can professionals do to combat non-professional enablers? What tools do they have at their disposal?

Professional accountants are well-placed to help law enforcement root out unprofessional enablers. Any given transaction or series of transactions often requires the involvement of several advisors; if you have suspicions it may be that one of the other professionals involved in the transactions is either complicit or an unwitting enabler.

Professional accountants have a duty under the money laundering regime to make a suspicious activity report (SAR) whenever they suspect a crime with proceeds. SARs include details of all parties to the suspicious transaction or arrangement. Similarly, all CCAB bodies require their members to report the misconduct of fellow members. There is no comparable duty to report a member of another body but that does not prevent a voluntary report being made. No offence of tipping-off is committed when the disclosure is made in this way to a professional organisation identified as an anti-money laundering supervisory body under schedule three of the money laundering regulations.

3. What obligations can we place on an 'in-house accountant'?

The accountant in this case is not bound by a duty to report, but their direct involvement in the money laundering process means that they are themselves breaking the law.

Professional codes of ethics also have a fundamental role to play here. By promoting professional integrity we help safeguard against complicity in economic crime and thin the ranks of the (un)professional enablers. Meanwhile, in taking due care we also thin the ranks of the professional enablers by protecting against unwitting participation in economic crime. The accountant here is surely in breach of their professional body's code of ethics because they are operating with complete disregard for scepticism and alertness (key qualities of a true professional) and without respect for the fundamental principles of integrity and due care.

Case study 8

Investment fraud

A firm which claims to offer 'investment management services' approaches you to help prepare its books. It has an online presence and a very well-designed website. Among the many stock pictures of professionals looking 'professional' is a photo of its premises in the shadow of an iconic City landmark. You are aware that the firm rents these offices.

The firm trades in gold, palladium and other precious metals. It has numerous skilled advisors on the payroll such that a large part of revenues is paid as salaries.

The managing director is professionally qualified but his previous business (which had a strikingly similar name) failed recently when the commodity markets collapsed. The first filing deadline for that business was missed and the company collapsed shortly after. Unfortunately previous accountants are unavailable to tell you any more about what happened.

(A suggested discussion point can be found on the next page.)

Case study 8: **Investment fraud** *(continued)*

How can your risk assessment procedures protect you?

For the purposes of this exercise put yourself in the position not of an objective assessor with the benefit of hindsight, but a sole practitioner who has just been approached to do some work. You will need to consider the effectiveness of your risk assessment systems carefully and honestly.

This scenario describes a fairly typical London investment fraud. These often have no permanent office space, preferring rented physical or 'virtual' offices instead. Their business name may refer to accountancy or finance services in order to conjure up in the investor's mind something of the prestige of the professions. They favour images and references to iconic buildings or street names for similar reasons, and the website is likely to reflect this. Another common ruse is to purport to trade in precious commodities. High salary costs as a proportion of turnover is yet another sign of an investment scam. ESCROW services may also be offered – to facilitate money laundering.

The individuals involved in this fraud may be professionally qualified in some way, though not necessarily as accountants. They are likely to have had previous involvement in similar scams with similar names. Year-end accounts may not exist – the businesses were probably wound up before they were required – but the explanations for previous closures will doubtless sound perfectly plausible.

Our initial risk assessment and ongoing client due diligence will clearly need to be well up-to-scratch here. A number of indications are mentioned which we can feed into an overall risk-based approach. It will also be important to maintain our professional scepticism and questioning mind at all times: just how likely is it that we have been given legitimate explanations?

An organisation with lots of money to pay staff might also have lots of money for professional fees – especially to pay an accountant whose work will lend legitimacy to dubious activities. We will need to make sure that offers of generous remuneration do not impair our objectivity, due care or diligence.

Case study 9

Mortgage fraud

You are a sole practitioner approached by an overseas client prospect who has been running a successful import/export business in his home country and would now like to expand into the UK.

In spite of a relatively short credit history the evidence obtained during the client due diligence process does check out. You are able to obtain a notarised copy of a passport from the client's local legal representative.

After a year or so of preparing accounts and tax returns for the business the client informs you that he plans to make a significant personal property purchase in the UK. The deposit will be paid by an overseas business associate. You are asked to provide an accountants' report to support the mortgage application.

In addition to your existing book-keeping and tax work the client now wants to use your client money account to receive direct payments of UK rental income and to pay the property management expenses. The balance remaining after settlement of taxes is to be remitted to the client's overseas business bank account.

The anticipated rental receipts look somewhat higher than you would have expected but the client describes the property's superior fixtures and furnishings while referring to impressive pictures in a number of brochures. Heavy hints are dropped that there could be more of this kind of work in the future.

(Suggested discussion points can be found on the pages following.)

Case study 9: **Mortgage fraud** *(continued)*

1. The importance of ongoing client due diligence

It would be difficult to claim that this client appeared low risk from the outset.

There is little evidence of any face-to-face contact and we learn of a relatively short credit history. Initial client due diligence should certainly include careful probing of his reasons for choosing our firm; are we in the habit of accepting long distance instruction from our clients?

We also need to be confident that the third party who notarised the identity evidence is indeed reliable. The *CCAB's Anti-Money Laundering Guidance for the Accountancy Sector* says the following:

> *'Businesses should have regard to the standing of the person certifying and may wish to consider specifying from whom certification may be accepted …'*

The guidance further suggests that such an acceptable person would be an '*independent legal professional'* located in an EU or other country which has equivalent AML law and supervision of compliance.

In a situation like this many of the documents or valuation reports could be excellent forgeries. Given that many accountants are not experts in this field, these could be difficult for even an experienced professional to spot.

Ongoing client due diligence would be particularly valuable in protecting us here as well as in any situation in which (as the CCAB AML guide suggests):

- a previously stalled engagement restarts;
- there is a change of control and/or ownership of the client;
- there is a material change in the level, type or conduct of business; or
- any other cause for concern or suspicion has arisen (in which case care must be taken to avoid making any disclosure that could constitute tipping off*)*.

2. What kind of client due diligence questions should we be asking?

Q: Why this sudden diversification into property investment, especially when the deposit will be paid by a third-party and the funds are destined for an overseas import/export business?

Ongoing client due diligence might lead you to contact the local lawyer who notarised the passport. In doing so you should use publicly available contact details taken from (for example) a public website. You could also visit the local company registry (if one exists) to check for changes in the company information. And if the planned purchaser is not the overseas business (ie, the recipient of the rent), then this too should raise further concerns about the nature of the client's business model.

Case study 9: **Mortgage fraud** *(continued)*

Q: Why the desire to use our client money account? Have there been difficulties in obtaining a UK bank account? If so, why?

Overseas individuals can sometimes find it difficult to obtain a UK bank account. They may have insufficient history or financial institutions might be reducing their exposure to risk. But there can also be more worrying reasons and it would be worth investigating further why it is so important that your client money account be used instead. Revisit the initial client due diligence and examine the bank records used for preparing the business accounts; you might find things that provide a springboard for further enquiries.

Consider conducting your own independent research into the true gap, if any, between the expected rental income and the market norm. And can you obtain any more information about the depositor or the proposed tenants?

Q: We are being told that this could be the first of several lucrative transactions. Is this the client's way of derailing your objectivity and professional scepticism by appealing to material self-interest?

You should perform and document a threats and safeguards analysis. Do this in addition to your ongoing due diligence considerations. You might also want to consider at this point documenting any suspicions you might have about money laundering. (It is also interesting to note that from this scenario money launderers do not always appear to mind paying taxes!)

3. Indicators of mortgage fraud?

There are plenty. All the main boxes are ticked by this scenario.

- The client or property is located far from your firm.
- The business or individual has no previous involvement in property investment.
- Any credit history is short.
- The deposit is to be paid by a third-party.
- The rental arrangements are not arms-length.
- There are subsequent, similar transactions in the pipeline (generally speaking: the more frequent they are, the more suspicious you should be).

When accountants sign-off on a mortgage application it is problematic for them to try to claim that they knew little about their client's identity and funding source. Not only are we required to carry out due diligence before starting a business relationship, that relationship may also (as in this case) include business advice and tax services which would theoretically require us to possess knowledge of the client's income sources.

Case study 9: **Mortgage fraud** *(continued)*

4. What other professional regulations might be relevant here?

Most professional bodies have regulations regarding the operation of client money accounts. However, whether or not activities like those outlined here are permitted, it is always worth asking whether it is strictly appropriate for your practice to provide its clients with what are, in effect, banking facilities.

Case study 10
Fraud

McCoy is a junior member of an in-house finance team who receives this email purporting to be from the CEO.

From: Frost (mailto:e.Frost@outlook.com)
To: McCoy@outlook.com
Subject: Project Blackbird

I have assigned you to manage Project Blackbird.

This is a strictly confidential financial operation which takes priority over other tasks.

Have you already been contacted by Marko from BOEM LLP?

This is very sensitive. We must make sure not to infringe FCA regulations.

Regards,

Frost

Soon after, McCoy receives a call from 'Marko' instructing him to make a funds transfer to a particular account. A follow-up email contains the destination account details and asks McCoy to send confirmation of the transfer by return email.

McCoy does as he is instructed. When he sends the confirmation Marko responds with a lengthy sequence of emails providing McCoy with details of several more bank accounts and instructions to make a number of further payments.

All of the domain names associated with Marko's emails appear as if they belong to BOEM LLP. McCoy suspects nothing.

(A suggested discussion point can be found on the next page.)

Case study 10: **Fraud** *(continued)*

What could have been done to prevent this fraud?

In most organisations it would probably be somewhat unusual for the CEO to make direct contact with a junior member of the finance team. However, the junior would doubtless be flattered by the attention and eager to please – which is one of the reasons deceptions like this succeed. All staff should be left in no doubt that they would never be criticised for responding with great caution in an unusual situation like this.

Finance team members should always take extra steps to verify the identity of anyone who purports to be contacting them from a professional services firm; a simple web search to confirm contact details and then a follow-up call could suffice. In addition the true origin of an email can sometimes be revealed by hovering over the sender's name.

There should also be an internal mechanism to make sure the finance team is kept aware of all scams of this sort. Any suspected incidents should be reported to Action Fraud (www.actionfraud.police.uk).

Final exercise

The CDD 'plea' word search

Hidden in the grid of letters below are several phrases commonly used in the kind of communications to MLROs that usually include a request to speed-up the client due diligence process. The sample phrases have been taken from real conversations with MLROs or published cases in which inadequate AML procedures figured prominently.

Some of the phrases were found in the email correspondence between Barclays employees in 2011 and 2012 when, in circumstances of strict secrecy, Barclays executed a number of risky transactions for high net-worth 'politically exposed persons' (or PEPs). Responsibility for the bank's financial crime risk assessment was confused and Barclays failed to respond to a number of indicators of high risk. The client identities were kept so confidential that the bank's own staff were prevented from carrying out the necessary client due diligence (CDD); instead of performing the extra checks that the situation required, they followed a less rigorous process than normal. As a result the CDD documentation was inadequate and the source-of-funds evidence was insufficient.

How many phrases can you find?

H	S	M	E	B	D	S	T	R	E	A	F	U	W	D	A	B	T	I	C	A	I	T	J	S
I	E	P	S	O	B	I	L	P	H	G	B	T	Y	E	F	N	P	Q	U	V	S	A	U	N
T	G	E	T	P	A	S	T	C	O	M	P	L	I	A	N	C	E	W	K	L	C	I	S	T
A	H	O	A	T	D	K	W	T	A	D	A	T	O	L	T	B	E	N	G	D	S	R	T	U
G	U	N	I	Q	U	E	B	U	S	I	N	E	S	S	B	I	C	H	D	F	N	A	A	Y
R	V	E	L	J	O	S	Q	C	D	E	A	U	O	P	V	R	B	X	O	E	G	F	F	E
E	F	C	K	A	Y	S	T	J	I	D	Z	A	E	C	V	A	B	M	N	D	S	K	O	H
A	V	X	S	B	E	K	B	N	T	U	C	M	I	S	D	C	I	Y	T	A	J	P	R	G
T	H	Z	A	E	S	D	E	A	L	O	F	T	H	E	C	E	N	T	U	R	Y	G	M	O
O	L	I	R	G	O	L	W	V	J	H	A	X	Y	M	A	T	S	H	P	J	E	H	A	R
P	R	F	G	H	E	I	C	J	S	M	T	B	C	D	E	H	L	A	S	S	F	U	L	P
P	K	U	M	B	S	C	E	D	G	G	T	O	R	Y	T	I	Z	M	E	Y	J	V	I	W
O	J	O	I	O	S	N	H	A	X	A	U	I	H	S	D	S	R	P	T	Q	F	O	T	E
R	V	A	E	P	D	F	R	B	M	F	D	W	C	Q	L	T	I	Y	C	C	X	O	Y	N
T	H	M	X	N	Z	P	B	A	S	Y	E	K	A	K	R	H	E	S	L	W	Q	U	D	F
U	E	A	F	R	A	B	W	O	I	X	Q	Z	N	M	B	R	E	U	I	A	I	L	R	C
N	G	G	R	E	M	L	B	S	U	T	A	U	A	C	H	O	M	A	E	R	P	N	F	R
I	R	L	K	U	N	C	O	M	M	E	R	C	I	A	L	U	X	P	N	R	B	F	G	N
T	D	A	I	B	A	E	G	I	K	S	U	T	R	I	P	G	U	E	T	A	C	S	G	G
Y	T	A	B	C	G	I	D	Z	S	H	L	B	A	U	W	H	Q	U	S	I	R	U	X	E

ALWAYS REMEMBER:

- The role of gatekeeper to the legitimate financial system is a very important one.
- Special care should be exercised when operating a client money account.
- Never ignore the need for ongoing client due diligence.
- Accountants should remain specially alert to scam emails and telephone calls.
- Risk assessment is an important part of the client due diligence process and should not be overlooked or cut short.
- Risk assessment should come before verification – first think about things like this:
    - why they chose you;
    - the practicality of working together (including across borders);
    - the sense or logic of the client's story; and
    - whether the background information adds up.
- A professional-looking website is very easy to create or clone – it tells you very little on its own.
- Risk assessment procedures should be in proportion to the size and activities of your organisation.
- Accounting firms should perform firm-wide risk assessments as well as assessing client-specific risks.
- Terrorism is not necessarily an expensive business – small amounts of money can pay for a lot of human suffering.
- Suspicious activity should be reported to the UK Financial Intelligence Unit (UKFIU – which is part of the NCA) as soon as a suspicion arises. That would also be the moment to carefully consider whether you should continue to act for this client.

WORD SEARCH ANSWERS

Just a formality
Unique business
Be lenient
Tick boxes
Get past compliance
A great opportunity
Don't upset client
Take a pragmatic view
Race this through
Deal of the century
Uncommercial

JOINT ANTI-CORRUPTION STATEMENT BY PROFESSIONAL BODIES
11 MAY 2016

Bribery and corruption represent serious threats to economic growth, individual livelihoods and civil society across the world.

For many years, professional bodies have worked alongside government, regulators, law enforcement and international bodies and supported our members to combat bribery, corruption, tax-evasion, money laundering and the financing of international terrorism. We will continue this work and provide support to facilitate national and international cooperation and to improve monitoring and enforcement systems.

We deplore corruption and the significant harm it causes; we play a vital role in training, educating and supporting our professions to uphold the highest levels of integrity and ethical standards.

We know criminals seek to abuse the services provided by our members to launder the proceeds of corruption and we are committed to ensuring the professions we serve are armed with the tools to thwart this abuse.

We stand united in the fight against corruption in all its forms and are committed to sharing knowledge, skills and intelligence with our fellow professionals and with all agencies fighting this cause. The co-signatories to this statement are as follows:

The Law Society of England and Wales; The Institute of Chartered Accountants in England and Wales, The Society of Trust and Estate Practitioners; The Law Society of Northern Ireland; The Law Society of Scotland; The International Federation of Accountants; The Association of Chartered Certified Accountants; The Chartered Institute of Public Finance and Accountancy; The Institute of Chartered Accountants of Scotland; Chartered Accountants Ireland, The Chartered Institute of Management Accountants; The Association of Taxation Technicians; The Association of International Accountants; The Chartered Institute of Taxation; The International Association of Bookkeepers; The Institute of Certified Bookkeepers; The Institute of Financial Accountants; UK200; The Association of Accounting Technicians.

Consultative Committee of Accountancy Bodies

ICAEW | ACCA | CIPFA | ICAS |
Chartered Accountants Ireland

tel: +44 (0)20 7920 8100
fax: +44 (0)20 7920 8783
email: admin@ccab.org.uk
web: www.ccab.org.uk

PO Box 433
Chartered Accountants' Hall
Moorgate Place
London EC2P 2BJ

Registered Address: CCAB Ltd | Chartered Accountants' Hall Moorgate Place London EC2P 2BJ | Registered in England and Wales No.1864508