MARSH

MARSH INSIGHTS:

FRAUDS AND SCAMS — INCREASING AWARENESS

Many of us, and many businesses, have a tendency to under-estimate the risk of being affected by fraud. The unhappy reality is that more and more of us are being affected personally, whether by identity theft, cloning of a credit card, or a telephone scam. Businesses are also being targeted by fraudsters.

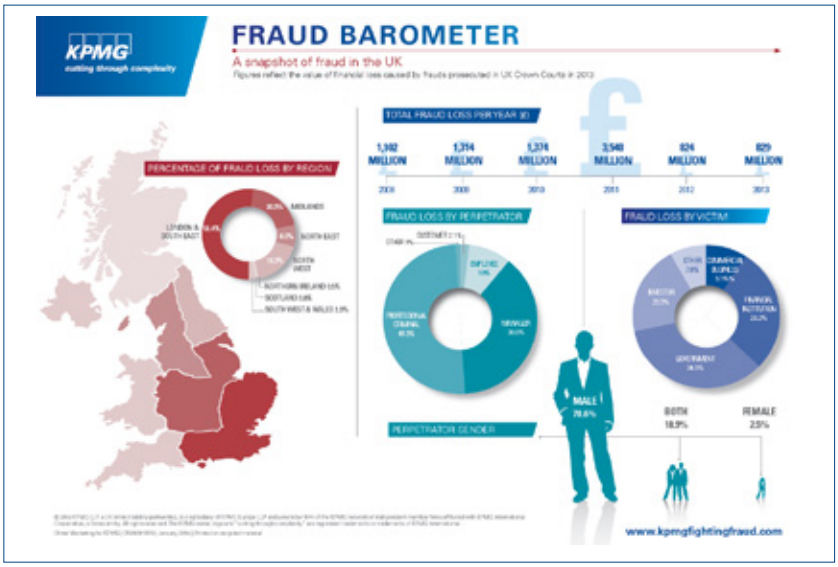
This extended newsletter aims to raise awareness and help reduce risk. It contains self-assessment questions and scenarios to consider, helping you assess your own processes and exposure.

This communication is not about internal fraud on the part of colleagues. It focuses on exposure to external frauds and scams; dishonesty and criminality on the part of clients and other third parties.

KPMG's 2013 Fraud Barometer, a snapshot of fraud in the UK, indicated that more than half of all frauds committed in the UK in 2013 were perpetrated by a combination of professional criminals, customers, and other third parties.

In the past few years solicitors have been exposed to the threat, the reality, and the financial and reputational consequences of external frauds and scams. Awareness of the threats is a key component of minimising the risk of exposure to these frauds and scams and their consequences.

This extended newsletter is aimed at raising awareness of external frauds and scams already experienced by the profession and to alert the profession to frauds and scams which have afflicted solicitors in other parts of the world.



Report reproduced with the permission of KPMG LLP

1. INTRODUCTION

Many of us, and many businesses, have a tendency to under-estimate the risk of being affected by fraud. Some are inclined to assume that the people they deal with in their personal lives and in business will behave honestly and are not capable of behaving dishonestly towards them. When the risk of exposure to client dishonesty is raised with them, the reaction of many is to protest — "If I can't trust my clients.....!".

CAN'T WE TRUST OUR CLIENTS?

The experience of a growing number of businesses, including law firms, provides support for a view that it is prudent to recognise and act upon the difference between:

- Not trusting those you deal with in business/practice.
- Behaving as if you have no reason to make any assumption about their honesty and trustworthiness.

In this newsletter, we will consider a number of case studies based on real life examples of frauds and scams perpetrated by third parties where solicitors, or solicitors' clients, have been the victims and the solicitors concerned have suffered losses as a result.

But first, it's interesting to consider some facts and figures which throw some light on human behaviour and dishonesty.

2. REALITY CHECK — FACTS, FIGURES, AND THE 10-80-10 PRINCIPLE

This section considers facts and figures relevant to understanding the risk of exposure to fraud. The figures we're going to start with are the figures 10, 80, and 10, which have a particular significance in the context of financial crime risks.

THE 10-80-10 PRINCIPLE

The "10-80-10 principle" is a general rule of thumb in criminology circles. It reveals that in any given population, 10% of people will never steal and 10% of people are predisposed to stealing if they are given the opportunity.

What do you think the 10-80-10 principle says about the remaining 80%?

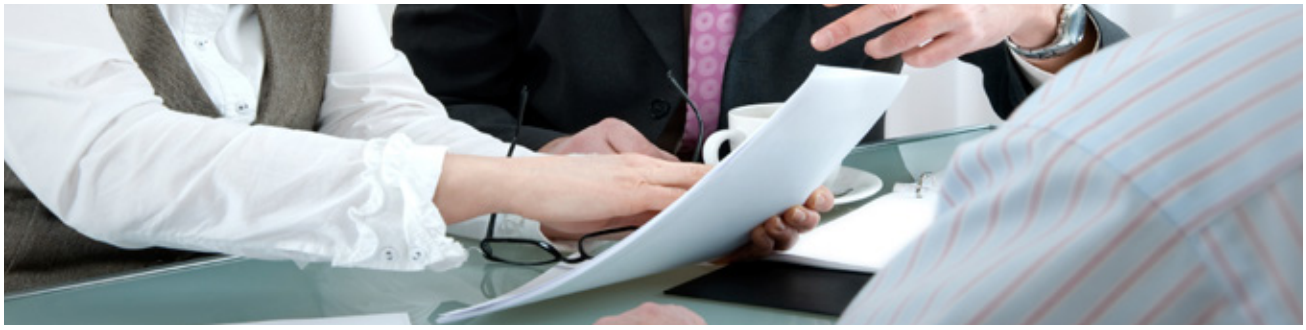
a) They wouldn't know how to go about stealing money?

b) They probably have no need to even consider stealing?

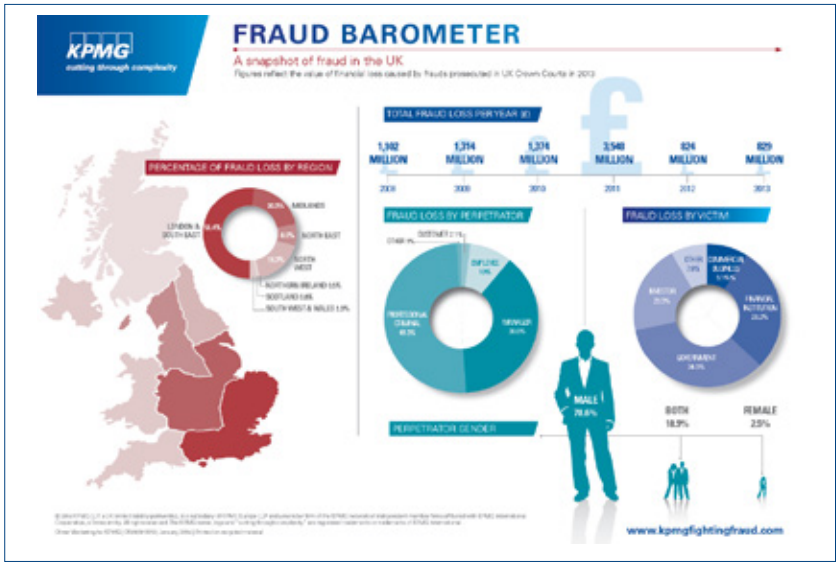
c) They can move in either direction depending on the pressures they are under and how they rationalise a particular opportunity?

The correct answer is c) and the history of the claims experience of solicitors tends to bear that out. The claims history, including the scenarios which follow later in this module, include situations where solicitors have been exposed to claims as a result of:

- Dishonesty on the part of colleagues who were highly regarded and respected, and in a position of trust.
- Clients using their solicitors to facilitate frauds and scams.
- Clients pretending to be other people.
- Fraudsters pretending to be clients.



Let's look again at KPMG's 2013 Fraud Barometer.



Experience of UK:

Across the UK as a whole, the *Fraud Barometer* provided a view of the extent of losses resulting from fraud in 2013 by category of perpetrator:

Percentage of financial crime	Perpetrator
48.3%	Professional criminal
38.6%	Manager
10%	Employee
2.1%	Customer
1%	Other

Experience of Solicitors:

Regrettably, internal fraud involving misappropriation of client funds, or firms' own money, does occur, sometimes involving partners or other solicitors, cashroom staff or other members of the practice's personnel. However, the controls which the profession has in place by virtue of the financial compliance regime mean these occurrences are relatively rare.

Turning to external frauds, that is frauds and scams perpetrated by third parties, including clients and professional criminals, it is an unhappy fact that the profession has been exposed to a number of frauds committed by clients and by professional criminals. Raising awareness of the known and potential exposures is the objective of this newsletter.

3. FRAUD AND THE ECONOMIC CYCLE

Based on their experience of claims trends over many economic cycles, insurers are very familiar with the correlation between adverse economic conditions and increased frequency of claims involving fraud and dishonesty.

Consider the following statement:

Risk and insurance experts warn that, in an adverse economic climate, there are far greater opportunities for fraud to be perpetrated on businesses.

Do you think this statement is true or false?

False. It's not really the opportunities to perpetrate fraud that are greater. It's the motivation factor that is likely to be heightened in times of economic hardship because people are facing financial challenges (because of redundancy, because businesses are struggling, etc.). If someone's business is failing, they may be more likely to contemplate a course of action they would never have resorted to if their business was busy and prospering.

Going back to the 10-80-10 principle, what was said about the 80%? According to the research, for 80% of any given population, their propensity to steal or act dishonestly depends on the pressures they are under and how they rationalise a particular opportunity. That means, for instance, that someone who would otherwise behave honestly could be tempted or pressured to steal if they are suffering severe financial hardship, putting their business or family home at risk. They are capable of rationalising their actions if they take the view that the money they "need" wouldn't be missed by the organisation.

This analysis doesn't really apply to organised crime/professional criminals, whose activities are part of the subject of this newsletter. However, it is as well to be aware that the risk of exposure to frauds and scams is not necessarily constant and that the risks tend to be heightened in adverse economic conditions.

It is also important to realise that the way frauds and scams are perpetrated is not a constant either, as the following excerpt from the KPMG Fraud Barometer 2013 notes. Indeed it is limited only by the resourcefulness and ingenuity of fraudsters. Our individual risk awareness and the risk controls of our businesses need to acknowledge that.

KPMG *Fraud Barometer* 2013

KPMG's bi-annual Fraud Barometer for 2013 showed that fraudsters are at the cutting edge of technology — attacking banks in the virtual world, for example. At the same time, some fraudsters have reverted to "paper and pen" as organisations focus risk management efforts on technology-driven defences.

Hitesh Patel, UK Forensic Partner at KPMG, says:

"It is certainly the case that we have seen fraudsters using very clever high tech frauds to attack banks, businesses and local authorities, but we have also seen some of the biggest frauds in more low tech scams. As old forms of transactions, such as cheques, are phased out, organisations are focussing on developing sophisticated lines of defence. Yet, rather than putting criminals off, many fraudsters are ignoring the challenge of triumphing over technology in favour of using simpler methods of deception."

4. EXTERNAL FRAUD AND SCAMS

Sadly, we are all exposed to frauds and scams in our business and personal lives. On its website, ActionFraud lists a large number of types of frauds and scams, including the following:

ACCOUNT TAKEOVER	An account takeover can happen when a fraudster or computer criminal poses as a genuine customer, gains control of an account and then makes unauthorised transactions.
CHEQUE FRAUD	Cheque fraud relates to any illegal use of cheques to acquire or borrow funds. Types of cheque fraud include counterfeiting, forged cheques, fraudulently altered cheques, bad cheque writing, cheque washing, and using disappearing ink on cheques.
INVOICE SCAMS	Fake invoice scams happen when fraudsters send an invoice or bill to a company, requesting payment for goods or services. The invoice might say that the due date for the payment has passed, or threaten that non-payment will affect credit rating. In fact, the invoice is fake and is for goods and services that haven't been ordered or received.
OFFICE SUPPLY SCAMS	Office supply scams happen when telemarketers trick employees into ordering or paying for stationery. The caller might mislead a company's employees into thinking that an order for office supplies has already been placed, either by an existing or former colleague, and that they are calling to chase up a signature for the order form to help them keep complete records. The company is then sent an invoice for unwanted, and often overpriced, stationery and office supplies.
TELECOMMUNICATIONS	Telecommunications frauds involve the misuse of airtime by fraudsters who have no intention of paying any bills. Telecommunications frauds can include: • Mobile phone fraud. • Fixed line fraud.

These are all types of fraud/scam which have afflicted businesses of every type.

The range and variety of frauds and scams demonstrates fraudsters' ingenuity, creativity and determination and the need to keep our risk awareness and risk controls up to date.

5. FOCUS ON SOLICITORS

The role solicitors play in transactions of all sorts, and the fact that solicitors are often responsible for safekeeping and custody of substantial sums of client money, may make the profession a particularly attractive target for the activities of fraudsters. Some of these fraudsters may be opportunists but the fraudsters who target the profession, the client funds they are responsible for, and their client bank accounts, also include organised criminal gangs; some of them very sophisticated cyber criminals.

The intelligence and capabilities these criminals have is considerable, enabling them to engage in "social engineering" (described later) and to commit "confidence tricks" to overcome barriers and risk controls which might otherwise be considered more than adequate.

Consider the following hypothetical scenarios which suggest ways in which frauds might be perpetrated on firms of solicitors. Consider whether the sorts of procedures and risk controls which law firms require to have in place would prevent these hypothetical scenarios ever becoming a reality and resulting in claims.

Theft from solicitor's client bank account

Firm A had GBP1,000,000 stolen from its client account after a member of the firm's finance team was persuaded to disclose password/PIN information. With the password/PIN information, a fraudster was able to transfer client funds using the bank's automated bank transfer facility. Transfers of funds were effected overnight and only discovered the following day.

Fraudulent commercial loan transaction

Firm B was engaged to act for a lender in a commercial property/loan transaction involving commercial property in England. Firm B arranged a direct transfer of the loan funds to the borrower's bank account.

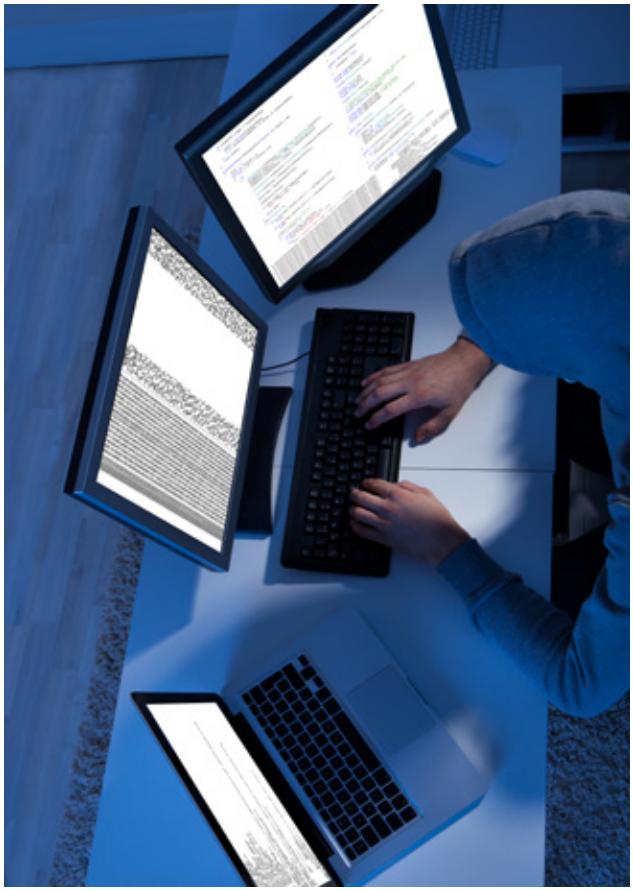
After settlement, it emerged that the law firm was not a genuine law firm; that the transaction was a scam; the security/charge created over the property was void and the lenders had no security for the substantial loan advanced to the fraudster. The bank account to which the loan money had been transferred was the fraudster's own bank account and the lenders made a claim against the firm in respect of their substantial loss.

REALITY CHECK

Actually, the facts of the two scenarios are not hypothetical. They really happened.

It's an uncomfortable fact that a number of firms have had client funds stolen from their client bank accounts in the way described. In each case, a member of the firm's cashroom team was convinced and persuaded by a very clever "confidence trick". They were all convinced the caller was legitimate, a genuine member of the bank's staff legitimately responding to a real fraud involving the firm's client bank account and helping the firm to put things right.

In all of these cases, the fraudster posed as a member of the bank's fraud investigation team contacting the firm under the pretext of suspicious activity identified by the bank on the solicitor's client account. In all cases, the caller's "cover story" was evidently convincing and the firm's employee complied with the request for details of password/PIN or insertion of card in card reader.



6. HOW CAN SOLICITORS AVOID EXPOSURE TO THESE EXTERNAL FRAUDS?

Consider this excerpt from a firm's risk assessment and risk prevention plan. Would this work? How effective do you think these measures would be in addressing exposure of law firms to the fraud scenarios we've just been looking at?

Risk assessment (excerpt)

IDENTIFIED RISK	RISK CONTROL
Fraud risk — external Exposure to third party frauds and scams. Recent third party/client frauds and scams illustrate the increased importance of client vetting and other controls to minimise the risk of exposure to unwitting involvement in frauds/scams and resulting liability (and possible other sanctions).	Review client vetting criteria and, if found necessary, amend/tighten client vetting. Check that colleagues are applying client vetting criteria consistently.

These measures are entirely prudent and worthwhile. However would they have been effective in reducing the risk of exposure to the types of fraud in the scenarios we've just been considering?

Fraud on Firm A — analysis

In addition to apparent penetration of IT systems, this form of client bank account theft has relied on persuading staff in the firms' cashroom/finance teams to reveal security information (or otherwise comply with the fraudster's instructions) and thereby to facilitate access to client bank accounts via online banking.

Fraud on Firm B — analysis

In the transaction involving the fake law firm, the fraudsters relied on solicitors failing to detect that they were corresponding with a non-existent law firm and, crucially, failing to spot an irregularity in the bank account details provided in the bank transfer instruction.

Conclusion

These real life examples demonstrate the diverse nature of the external fraud risks to which law firms are exposed and prove that a methodical approach to risk avoidance or, perhaps more realistically, risk reduction is called for. This requires a range of measures starting, importantly, with risk awareness and including a set of targeted risk controls.

A number of points emerge from the activity that has been seen:

- The profession is exposed to a range of different types of external fraud/scam.
- A "con trick" to induce disclosure of security information is one of the methods used by fraudsters to gain access to systems and bank accounts.
- Fraudsters are capable of breaching IT security by hacking and penetrating computers and computer networks with malware, including trojans.
- Fraudsters are determined and persistent.

The risk alerts also highlight a number of important risk management points:

- The need to maintain awareness of current frauds and scams by reading risk alerts and tapping in to other sources of warnings.
- The importance of ensuring that all colleagues (including cashroom/finance team colleagues) are fully aware too – a weak link in the practice's risk awareness and risk controls can undermine the best efforts of everyone else in the practice.
- Never disclose password, PIN, or other security information.
- Don't allow yourself to be persuaded or tricked in to believing someone is bound to be genuine just because they have private information about you, your practice, your bank account, bank account transactions, or your clients.

KPMG *Fraud Barometer* 2013

"Fraudsters' determination to focus on the so-called old-fashioned scams and avoid elaborate methods of deception is also evident through a resurgence of cases involving tax rebates, loans and mis-selling. ..... It shows that, although the motivation to deceive comes in a variety of forms, many criminals are still prepared to rely on the traditional conman artistry of making financial gain through misplaced trust, attacking people's vulnerabilities and sensibilities."

This takes us on to the topic of "social engineering", which is an aspect of the sorts of frauds and scams we have just been looking at.

7. SOCIAL ENGINEERING AND EXPOSURE TO EXTERNAL FRAUD

Social engineering explained

"Social engineering" describes a kind of intrusion that relies heavily on human interaction and often involves a "con trick" to induce others to depart from standard/normal security procedures.

For example, a criminal using social engineering to break into a computer network might try to gain the confidence of an authorised user and get them to reveal information that compromises network security.

Criminals who engage in social engineering often rely on people's natural helpfulness as well as their weaknesses. They might, for example, call the authorised employee with some kind of urgent problem that requires immediate network access.

These criminals may appeal to vanity, authority, and greed.

They may engage in old-fashioned eavesdropping.

Those who create computer viruses use social engineering tactics to persuade people to open email attachments containing malware. Phishers use social engineering to convince people to divulge sensitive information, and scareware vendors use social engineering to frighten people into running software that is useless at best and dangerous at worst.

Social engineers rely on the fact that people are not aware of the value of information and are careless about protecting it. Consequently, social engineers may:

- Search rubbish for valuable information.
- Gain information by looking over someone's shoulder (shoulder surfing).
- Take advantage of people's natural inclination to choose passwords that are meaningful to them but can be easily guessed.

The greater the dependency on information, the greater the threats posed by social engineering.

Addressing the threats involves a range of measures but education is essential; education about the value of information and the importance of protecting it, increasing people's awareness of how social engineers operate.

Based on this description and some of the examples provided, it certainly appears that the fraudsters who have been stealing, and attempting to steal, from solicitors' client bank accounts have been engaging in social engineering. How else did the fraudsters acquire the information which enabled them to commit the "con trick" and access systems?

RISK CONTROLS

Fake law firms have been a particular concern to the profession and the Solicitors Regulation Authority (SRA). The SRA has issued guidance on the matter and provided fraud warnings on their website highlighting "known" fraudulent firms.

It is suggested that, when dealing with unfamiliar law firms, solicitors should adopt a consistent approach of:

- Using the SRA guidance, or a version of it, as a checklist and having a note (perhaps an annotated copy of the guidance) on file to record the enquiries undertaken in relation to the England and Wales firm.
- Considering/investigating any discrepancies or anything suspicious in bank transfer details – and having this evidenced on the file, again by reference (as a minimum) to checks suggested by the Solicitors Regulation Authority (SRA). A bank account name which bears no relationship to the name of the other firm ought to raise suspicion as should a bank account name which includes "Limited" or "Ltd" when the other firm is not a limited company.

SPOTTING FAKE LAW FIRMS

Watch out for red flags such as:

- Errors in letter heading on letters received (e.g. misspelt solicitor names, named partners, branch offices, and place names).
- No landline telephone number is available.
- Inconsistent telephone and fax numbers to those generally used.
- A firm based in serviced offices.
- Email addresses which use generic email accounts.
- A sudden appearance of a firm in a locality in which there is no obvious connection to the area.

If you are dealing with a firm which is unknown to you, do an internet search to see if it is genuine and if a particular branch office exists/remains open.

If you are dealing with a firm which is unknown to you, check the firms details on the SRA website.

SPOTTING "SUSPICIOUS" BANK TRANSFER DETAILS

Watch out for red flags such as:

- A strange or suspicious bank account name (e.g. the account not being in the name of the firm).
- Inconsistent bank account details to those generally used by another firm.
- A firm based in one part of the country with a bank account in a different area.
- An overseas client account.

CONCLUSION

From 2013 onwards SRA has been issuing over 100 scam alerts a year. The risk of being induced, fraudulently, to transfer funds to a fraudster's bank account in a genuine transaction e.g. by providing bank transfer details late in the day when attention is focused on other pre-completion priorities is high.

So even if you are entirely satisfied regarding the identity of the solicitor/firm you are dealing with, it's still essential to pay due attention to the bank transfer details.

8. OTHER EXAMPLES OF EXTERNAL FRAUDS AND SCAMS

There is a diverse range of other external frauds and scams involving different techniques and arising in different areas of solicitors' practice activities.

When considering each of these frauds and scams, think about the extent to which each incident might have involved any of the factors, following:

- Social engineering.
- A "con trick".
- An information security failure.
- A breach of IT security.
- Reliance on failure to spot or investigate irregularities in identity information/documentation or bank transfer details.

8.1. TRUST AND PROBATE – INTERCEPTION OF EMAIL CORRESPONDENCE

Solicitors handling the administration of an estate contacted a beneficiary overseas to notify him of his entitlement to a quarter share of his late aunt's estate. At intervals thereafter, there were email exchanges between the solicitors and the beneficiary regarding progress with the estate and the beneficiary's prospective entitlement.

When the solicitors emailed the beneficiary in connection with an interim payment to account, the beneficiary responded with details of his bank account. However, it transpired that this email wasn't from the beneficiary; it was from a fraudster who had intercepted the email correspondence. The bank details were for the fraudster's bank account.

Fortunately, the solicitor handling the estate was suspicious of the email and made contact with the beneficiary (not by email) to establish whether it was genuine. The solicitor's vigilance meant the fraudster's attempted fraud was thwarted.

This "near miss" arose in the course of the administration of an estate, but could a fraudster commit a similar fraud by intercepting email correspondence between solicitors and their clients in other types of work, for example debt collection or property letting? Arguably it could arise in any situation where clients at some point provide their solicitors with details of their bank account for remittance of funds — proceeds of a property sale or company disposal or a personal injuries award.

However the risk is not just confined to solicitor/beneficiary or solicitor/client communications as the following examples show.

In one case, a firm acting in a house purchase remitted the purchase price at settlement to a bank account believing the account to be the selling solicitors' client account. The bank account details had been provided in an email purporting to come from the responsible fee earner at the selling solicitors.

In another case, the finance team in a small Scottish law firm acted on an internal email instruction to make an immediate bank transfer of a significant sum of the firm's own funds. This email instruction appeared to have been sent by the firm's senior partner.

The emails in both cases were sent by fraudsters masquerading as the selling solicitors and senior partner respectively. The bank account details provided in the emails related to the fraudster's bank account.

RISK CONTROLS

As always, awareness is a crucial element of a solicitor's risk controls — ensuring that colleagues, including cashroom/finance team colleagues, are aware of the risks and the potential exposure to this type fraud. However, other items should be considered too:

- Validation/verification of client bank account details — Whenever a client provides bank account details/instructions for the first time (or changes details/instructions), it's essential that these are verified.
- If the client has provided the (new) details/instructions by email, when contacting the client for confirmation be sure to do this by a different form of communication e.g. by telephone or by letter. This minimises the risk that a fraudster who has provided a fraudulent payment instruction, e.g. by email, is also in a position to provide false validation by intercepting your email request for confirmation.
- Perhaps bank account details should only be provided by email if the email is encrypted.
- Watch out for any change to your client's email address. It may be a subtle change, designed to deceive. For example:

- Joe.bloggs@hotmal.com or Joe.bloggz@hotmail.com

8.2. COMMERCIAL PROPERTY — IDENTITY THEFT

According to CIFAS, the UK's Fraud Prevention Service, "Identity crimes are the fastest growing types of fraud in the UK. They involve criminals making use of details to get past an organisation's security measures: from dates of birth to financial details, passwords and so on."

Identity theft crime may take the form of:

Identity theft, sometimes referred to as impersonation fraud: when a criminal uses the details of a genuine victim to impersonate them and, for example, open new accounts.

Identity fraud, where a criminal makes up an identity — often involving forged documents — in order to get products or services.

Account takeover fraud, where the fraudster has enough details (like passwords) to bypass security on the victim's accounts and take over the running of them.

HOW HAS IDENTITY THEFT AFFECTED SOLICITORS? CONSIDER THIS CASE STUDY

Example

A new client, Graham Phoney, consulted Rachel Quince, a commercial property associate with the firm of Bloggz LLP. The firm also received instructions to act for the lender. Mr Phoney was raising funds for expansion of his micro-brewery by remortgaging the brewery premises. The transaction proceeded smoothly, the security documents were duly executed, and the loan funds released to Mr Phoney.

Some time later Bloggz received a very unwelcome letter from solicitors instructed by the lenders to pursue a claim against the firm following Mr Phoney's default. It turned out that Mr Phoney was a phoney, and that the actual owner knew nothing about the loan.

Mr Phoney's name and the owner's name were very similar — but not the same. Rachel had been prevailed upon to accept an explanation from Mr Phoney which supposedly accounted for the slight difference.

WHAT COULD HAVE BEEN DONE TO AVOID THIS CLAIM ARISING?

SRA risk alerts and this newsletter could have raised awareness of, and suggested risk controls relevant to, situations where fraudsters have masqueraded as:

- **The true owners of residential properties** and engaged solicitors in the sale or mortgaging of "their" properties.
- **Existing clients of solicitors** and, by intercepting email correspondence between solicitors and (genuine) clients/beneficiaries, have given solicitors instructions to remit funds from balances held for the (genuine) client/beneficiary.
- **A genuine law firm** acting on behalf of a party (in reality the fraudsters) to a property/commercial transaction with the ultimate objective of procuring a transfer of funds in to a bank account represented as a solicitor's client bank account (but in reality a bank account set up by or under the control of the fraudsters).

How were the fraudsters in these various situations able to satisfy the vetting procedures and processes of lending institutions, banks and other parties including solicitors? How were they in possession of detailed information about those they were impersonating, about transactions, about banking processes and thereby able to establish credibility and to convince others of their credentials?

At least part of the answer in some of these scenarios may be down to the fact that information had been compiled from public sources, overcoming information security, and taking advantage of information security lapses.

RISK CONTROLS

- Complete anti-money laundering (AML)/identity checks thoroughly — don't be persuaded to cut corners.
- Don't be persuaded to disregard anomalies.
- Consider asking for sight of documents (not title documents) relating to the property purchase.
- Ensure that any unusual aspects of the transaction are fully reported to the lender.

8.3. RESIDENTIAL PROPERTY — FRAUD ON LENDERS

Residential property solicitors have been targeted by fraudsters to act in relation to unoccupied property. The solicitors, who were, along with lending institutions and house owners, the victims of the frauds, and are often completely vindicated in relation to claims against them by the lending institutions. It is nevertheless worthwhile reviewing the facts of these cases for risk management points that can be taken from them.

These frauds involved identity theft. The perpetrators identified properties which were not occupied by their owners and which had no securities in place. They then assumed the identity of the owners, obtained substantial loans over the properties and disappeared with the loan funds. To carry out this scam the fraudsters needed to involve a solicitor to carry out the security work and draw down the loan.

Following default on the loans the lenders contacted the true owners who were completely unaware of the situation.

RISK CONTROLS:

Claims made by the lenders based on allegations of breach of warranty of authority in such scenarios are often unsuccessful and the solicitors completely vindicated. However, the situation was extremely concerning for the firms involved and the risk remains of solicitors being exposed to other forms of identity theft. It is therefore as well for solicitors to be aware of this particular fraud and of the guidance which was issued to the profession at the time:

- Be on alert in situations where you are approached by individuals for whom you have not previously acted, who claim to be the owner of a property which is currently security-free and ask you to handle a substantial new loan over it. There is a considerable risk that they may not be genuine.
- Consider taking the following steps:
  - Ask those instructing you to explain why they have not instructed the solicitors who acted in the original purchase (and who would already be familiar with the title).
  - Check their proof of identity very carefully and ask for sight of documents relating to their purchase.
  - Enquire as to the purpose of the loan. Even where you are offered a plausible explanation (e.g. purchase of a second home or property abroad) obtain independent verification from a reliable source.
  - If the property has been let out, contact the letting agents and ask them when the landlords were last in touch.
- If you decide that it is safe to proceed make sure that any unusual aspects of the transaction are fully reported to the lender.
- Finally, under no circumstances accept a mandate to remit any funds to a third party (e.g. a company or non-solicitor agents) but insist that they are sent direct to the client's own bank account.

The final point in this guidance is a risk control which should be considered as a matter of course. Any situation in which clients are requesting payment to a third party rather than themselves could be a "red flag" i.e. a flag to consider the possibility of an identity theft fraud being committed.

8.4. IDENTITY FRAUD "CON TRICK"

An example of an identity fraud resulting in a claim against solicitors has been highlighted to solicitors in New South Wales, Australia.

This involved a couple making an appointment to see a solicitor regarding urgent completion of a certificate relating to a mortgage transaction. The "husband" had brought suitable ID with him but the "wife" had forgotten to bring hers with her. The "wife's" ID was later brought to the solicitor's office by the "husband" and the solicitor signed the required certificate.

The reality was:

- The "wife" wasn't the wife at all. She was the husband's new partner.
- The husband and girlfriend disappeared with the mortgage advance.
- The solicitor faced a claim.

RISK CONTROLS

This scenario makes the case for:

- Insisting on following proper procedures.
- For not being pressurised in to cutting corners.
- For adhering to strict compliance with client/transaction vetting/AML compliance.

8.5. RESIDENTIAL PROPERTY – MORTGAGE FRAUD

A very large number of claims have been made by lending institutions arising out of "opportunistic mortgage fraud". Opportunistic fraudsters provide untrue or misleading information or fail to disclose required information in order to secure loans (or loan amounts) they wouldn't otherwise be entitled to.

These situations expose solicitors to the risk of claims by lenders where solicitors have failed to comply fully with the lenders' reporting requirements. In a large number of such transactions, lenders have argued that they would not have proceeded to lend had the solicitor reported certain key facts concerning the transaction.

In some cases, the misleading of lenders into lending (or lending more than they would have otherwise) has amounted to fraud and the borrowers have been prosecuted accordingly. In many cases, there may be no prosecution and perhaps the conduct of the borrowers doesn't constitute fraud.

CLAIMS AGAINST SOLICITORS

There have been very large numbers of claims by lenders against solicitors arising out of scenarios very similar to this. The lenders base their claims on (alleged) non-compliance with the terms of The Council of Mortgage Lenders (CML) Handbook requiring solicitors to report to them:

- If the buyer is acquiring from a party who has owned the property for less than six months.
- If the full purchase price is not passing through the solicitors' hands at settlement/if the solicitors do not have control of the full purchase price.
- If the price being paid at settlement is not in accordance with the offer of loan.
- If there are any other material facts which might influence the lender's decision to lend, e.g. the fact that the transaction is not at arm's length/is between connected parties.

RISK CONTROLS

- Ensure that you are fully aware of all the requirements of the CML Handbook/the lenders' instructions.
- Ensure full compliance with the requirements of the CML Handbook/lenders' instructions.
- Consider adopting the Law Society's CML Handbook Compliance Checklist.
- If there is any doubt regarding the requirement to report a matter to the lender, adopt the approach "If in doubt report".
- Await instructions from the lender before proceeding (that is an explicit requirement of the CML Handbook).

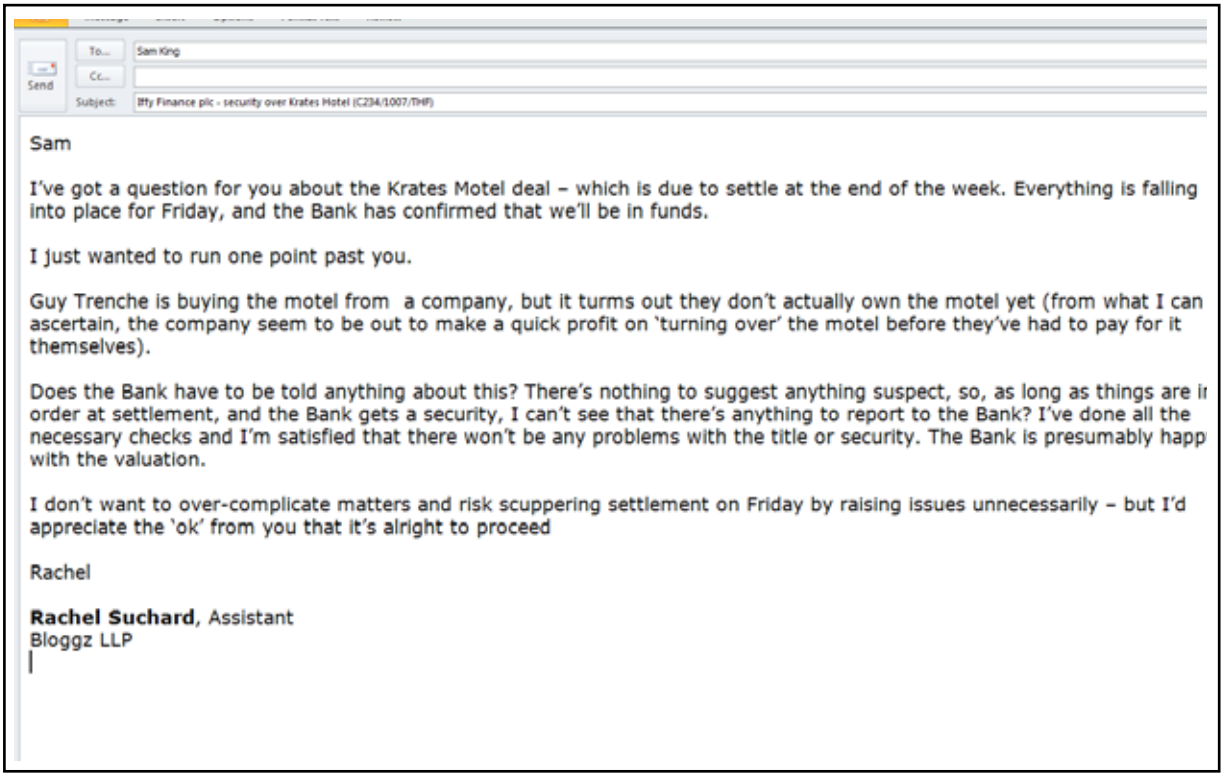
In discussions at workshops and seminars, when similar scenarios are discussed, some solicitors have expressed the concern that they would be hesitant about reporting to the lender, matters which might result in the buyer's transaction not proceeding. It's crucial to remember that in these transactions solicitors are almost always acting for two clients – the buyer/borrower and the lender. In such cases solicitors owe duties (contractual duties) to report in accordance with the requirements of the CML Handbook, and:

- Buyers/borrowers must understand the solicitor's duty to report certain matters to the lender.
- If the buyer/borrower wishes their solicitor not to report certain matters to the lender, the solicitor must consider his/her position and whether it is possible to continue to act.

8.6. COMMERCIAL PROPERTY — FRAUD ON LENDER

The risk of exposure to a claim by a lender as a consequence of a borrower's dishonesty is not confined to residential property only.

Let's consider a case study which illustrates a commercial property-related fraud. Imagine you are a commercial property partner receiving the following email from an assistant:



To... Sam King

Cc...

Send

Subject: Iffy Finance plc - security over Krates Hotel (C234/1007/THF)

Sam

I've got a question for you about the Krates Motel deal – which is due to settle at the end of the week. Everything is falling into place for Friday, and the Bank has confirmed that we'll be in funds.

I just wanted to run one point past you.

Guy Trenche is buying the motel from a company, but it turms out they don't actually own the motel yet (from what I can ascertain, the company seem to be out to make a quick profit on 'turning over' the motel before they've had to pay for it themselves).

Does the Bank have to be told anything about this? There's nothing to suggest anything suspect, so, as long as things are ir order at settlement, and the Bank gets a security, I can't see that there's anything to report to the Bank? I've done all the necessary checks and I'm satisfied that there won't be any problems with the title or security. The Bank is presumably happ with the valuation.

I don't want to over-complicate matters and risk scuppering settlement on Friday by raising issues unnecessarily – but I'd appreciate the 'ok' from you that it's alright to proceed

Rachel

Rachel Suchard, Assistant
Bloggz LLP

The concern in this scenario is that it could involve a fraud by the borrower on the lender. The facts provided are insufficient to establish this but the concern here is that the intermediate transactions are not genuine transactions. Could they be artificial transactions designed to create a false basis for the lender's lending decisions? Could it be that some of the intermediate parties are "nominees" of the ultimate buyers/borrowers or don't exist at all (other than as alter egos of the buyers/borrowers)?

RISK CONTROLS

- Ensure full compliance with reporting requirements in accordance with the letter of the lender's instructions.
- If there are facts about the transaction which could potentially influence the lender's decision to lend, be sure to bring those facts to the attention of the lender.
- Consider having a colleague review the transaction from the perspective of whether it "stacks up" or if there is any cause for suspicion of fraud.

8.7. LITIGATION — FAKE DEBTS AND FAKE CHEQUES/BANK DRAFTS

In some parts of the world, criminals have attempted to launder money by instructing solicitors to recover debts where no debt actually exists.

"Litigation solicitors are being targeted by criminals attempting to launder the proceeds of crime, the Law Society has warned" (Law Society Gazette, 17 March 2010).

HOW DOES IT WORK?

- The criminal engages solicitors in a debt recovery and produces documentation which bears to evidence the existence of a debt of some sort owed by a company overseas.
- Believing the instruction and the debt to be entirely genuine, the solicitors issue a letter to the would-be debtor warning that proceedings will be raised if the debt is not paid in full within a specified timescale.
- Payment is forthcoming and received by the solicitors by direct transfer of funds in to their client account prior to remittance to the client under deduction of the solicitors' fee
- In reality:
  - The criminal has fabricated the documentation to create the fiction of a debt owed to the criminal.
  - The debtor company has been set up by the criminal (or controlled by an accomplice of the criminal).
  - The funds remitted by the debtor company are in fact proceeds of crime being laundered through the solicitors' client account.

Imagine a different scenario also arising in the context of a debt recovery instruction:

- The facts are the same as the first scenario except that, instead of a direct transfer of funds in to the solicitors' client account, the solicitors receive from the debtor company a bank draft for the full amount of the outstanding debt.
- After advising the client that payment has been received from the debtor company, the client asks the solicitors if it is possible to have the funds remitted to them as a matter of urgency in advance of their financial year end.
- The solicitors still believe that both the client and the instruction are entirely genuine. They also believe that the bank draft is genuine and that it effectively represents a guarantee of cleared funds. They further believe that the client is a potential source of future profitable business. On this basis, the solicitors oblige the client by immediately remitting the funds to the client's bank account.
- It transpires that the bank draft, like the debt, is a fake. However, the deficit on the solicitors' client account is real and they (and their insurers) require to make it good.

KPMG *Fraud Barometer* 2013

"The data shows that con artists still rely on 'old technology' to perpetrate fraud, with a number of schemes in 2013 based on counterfeit cheques. In one strikingly simple case a local government employee processed cheques for legitimate payees, using disappearing ink. She secured the signatures of senior management for cheques reaching a total value of £162,000 and waited for the 'payee' details to disappear before substituting them with her own name."

RISK CONTROLS:

- Adhere to strict compliance with the firm's client and transaction vetting procedures and AML compliance. Don't cut corners. If, because you want to be helpful, you cut corners in following vetting procedures or AML compliance, you may be demonstrating to a criminal, and to the wider criminal fraternity, that your firm is an easy target.
- Check out the debtor company. A solicitor instructed to recover a debt from a Scottish company established that the supposed debtor company had been incorporated just a week or two prior to being instructed and more than a year after the date of the supposed unpaid invoice!
- Never be persuaded to remit funds to a client in anticipation of a cheque or a bank draft clearing. If the cheque is not cleared or the bank draft proves to be a fake, you will be the one left with the bad debt.

9. INFORMATION SECURITY

There are various terms used around information security. Cyber security, for example, may sound like the stuff of science fiction or, to some, the stuff of scaremongering or sales pitches. Whatever terms are used, the objectives are essentially the same — keeping information safe and secure and preventing it getting in to the wrong hands or being interfered with or compromised.

We've already considered social engineering (the psychological manipulation of people in to divulging confidential information or performing actions) as a way that criminals have managed to commit online banking frauds by overcoming the obstacles of the firm's security measures and the resistance of cashroom personnel. How did fraudsters acquire information enabling them to commit "con tricks" or to access email exchanges?

There is a clear link between information security and exposure to external frauds and scams. This is an additional critical reason why protecting information, whether held electronically or as hard copy, is essential for solicitors.

WHAT IS "INFORMATION SECURITY"?

Information security is about protecting:

- The confidentiality of information — and preventing its misuse.
- The accuracy of that information — and preventing unauthorised alteration of data or documentation.

WHY IS IT PARTICULARLY RELEVANT TO SOLICITORS?

Information security is a critical issue for solicitors because confidentiality of client information and integrity of data are at the heart of the solicitor-client relationship.

The external frauds and scams scenarios we have considered in this newsletter have involved situations where fraudsters have acquired and misused information about:

- Transactions on solicitors' client bank accounts.
- Solicitor-client relationships including transaction details and email correspondence.
- Colleague names, roles, and responsibilities.

However, fraudsters have managed to acquire such information, that information has assisted them commit confidence tricks and access firms' systems or online banking. Perhaps some of this information has been elicited by eavesdropping conversations, shoulder-surfing on public transport, gaining entry to office premises, using malware to access computer systems or by harvesting personal details on social media.

Preventing fraudsters accessing information is at least a partial obstacle in their way. Observing good information security practices is at least part of the solution.

IS IT REALLY CRITICAL FOR ALL SOLICITORS?

Information security is relevant not just for solicitors working on high-profile corporate deals or big name clients. It's equally relevant to all solicitors. Clients instructing solicitors in relation to wills, house purchases, or matrimonial matters are entrusting their solicitors with confidential information which requires to be appropriately safeguarded. Any breach of information security could result in exposure to a claim against the firm as well as potential regulatory action.

WHAT OTHER INFORMATION IS AT RISK?

In addition to information relating to the particular instruction, client verification information (for example, bank details, address, and passport numbers) stored as part of the firm's anti-money laundering procedures could be very valuable to criminals. Our identity is important and valuable, and, as we have already seen, fraudsters are increasingly using the identities of others for the purposes of committing frauds.

MARSH

INFORMATION SECURITY IN PRACTICE

Information security isn't just an IT issue, although IT is an important factor to be considered in ensuring effective information security. Consider the following facts from CompTIA's 2012 Annual Trends in Information Security study:

- 10% of information security lapses are caused by technology problems.
- 30% are the result of inadequate procedures.
- 60% are caused by human error.

WHAT RISK CONTROL MEASURES ARE APPROPRIATE?

All firms are likely to have policies and procedures to address key risk priorities. These will typically include:

- Physical office security measures.
- Clear desk policies.
- Password disciplines.
- Policies on the use of internet, memory sticks, etc.

INFORMATION SECURITY — ACTIONS

All colleagues also have an individual responsibility to ensure that their actions are not leaving them or their firms exposed to an information security lapse, by:

- Complying with the firm's policies and procedures.
- Not having identification passes on view when out of the office.
- Locking computers and other electronic devices with secure passwords, and using encryption technology where possible.
- Not leaving items containing confidential information on public view or unattended.
- Ensuring that conversations on public transport about confidential matters cannot be overheard.
- Ensuring that, while travelling, information being accessed by laptops/tablets cannot be read by others.
- Maintaining awareness of key risks and risk controls by reading risk management articles and risk alerts.
- Consider undertaking the Marsh e-learning module on information security.
- Consider undertaking the e-learning module Cyber Security for Legal and Accountancy Professionals developed by UK Government as part of its National Cyber Security Strategy with the support of both the Law Society of England and Wales and the Institute of Chartered Accountants of England and Wales.

CONTACT US

For further information and assistance please contact:

JOHN KUNZLER
0207 178 4277
john.kunzler@marsh.com

 Ref: MC150512493 exp: Nov2016

INSURANCE BROKERS CII CHARTERED