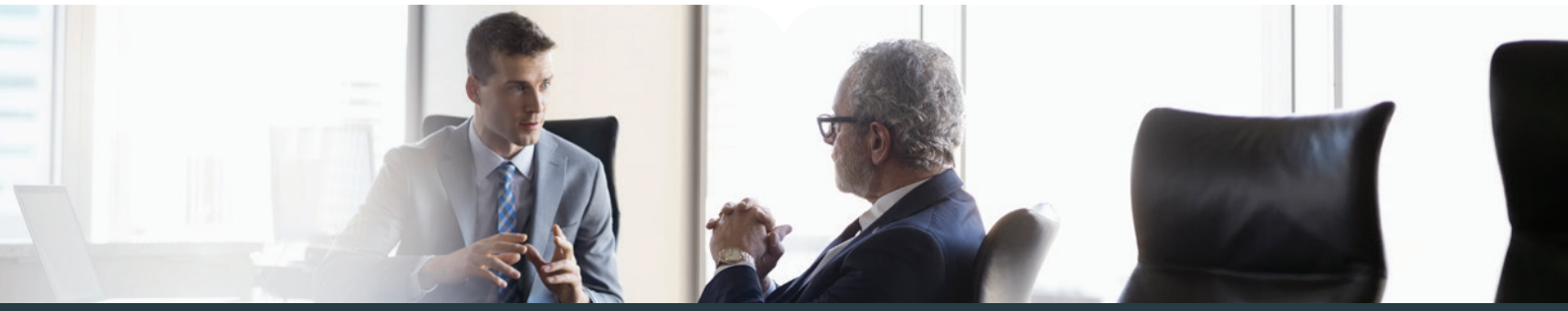
TRAVELERS



GUIDANCE NOTES FOR LEGAL PRACTICES

Fraud and dishonesty

Dishonesty in law firms

Theft, fraud and dishonesty are a risk for all businesses, but law firms are doubly vulnerable. Not only do they often have significant amounts of money in their accounts, they are also at risk of being used to launder money. The first could lead to a claim on your indemnity policy, the second to disciplinary sanctions and criminal proceedings.

In order to succeed most fraud must be disguised as legitimate activity. In almost all cases there could be a genuine reason for the actions described and it is your job to distinguish the real from the false activity. Fraud and dishonesty can be divided broadly into two types, that from inside the firm and attacks from someone outside the firm.

Internal fraud

Internal fraud is often the most difficult to detect because it is likely to be carried out by someone who has detailed knowledge of the firm's systems including those intended to prevent fraud. Sadly such fraud is sometimes perpetrated at the highest level in the firm and by senior and respected staff.

It often involves simple theft from clients' accounts although it can also be perpetrated by permitting someone outside the firm to access the firm's systems. It can also be theft from the firm by way of secret transactions which are not entered through the accounting system but for which the perpetrator receives payment. There may be someone within the firm who is assisting another party to defraud or steal from the practice.

Indicators of fraud

After a theft has been discovered, colleagues often recognise a pattern of behaviour:

- excessively long hours
- a reluctance to ask for help
- insisting that nobody should look at their files when they are absent. Typically, a fraudster may insist on doing routine administrative tasks themselves
- seeing clients out of hours or outside the office
- removing files from the office/files not available for audit

There may of course be genuine reasons for these actions, but anyone who is bypassing the firm's risk control systems and avoiding compliance with policies around file-keeping, accounts and reporting should be kept under review.

Theft from client account often begins on a very small scale. If the theft is not discovered, then it is likely to be repeated at increasingly frequent intervals and for larger amounts as the thief grows in confidence. 'Teeming and lading' occurs when money is taken from one account and then replaced by money stolen from another client, making it both difficult to detect and difficult to trace when the theft is discovered. In many cases however theft is straightforward, and when it is from a probate account or from that of someone under a disability it can be some time before it is discovered.

Internal theft can take place in other indirect ways ranging from improper use of the firm's facilities to using the firm's letterhead to carry out private work which is charged for independently of the firm's accounting processes. Whilst this is usually on a small scale it can be very damaging to the firm's reputation and compliance record.

Controls

Controlling internal theft relies on good staff training, proper systems for the transfer of money and payment of accounts and a high degree of alertness in particular by supervisors and managers.

Nobody should be allowed to bypass or disregard the firm's systems no matter how senior they are. Only approved personnel should be able to sign cheques or to input matters into the firm's accounting system. No matter how busy the firm, everyone should be encouraged to take their full holiday entitlement – at best employees who don't use all their holiday are liable to become stressed but at worst they could be concealing some sort of

problem. Accountants for example are usually required to take at least two weeks' holiday consecutively during the year – consider whether this rule should be imposed on your accounts staff. Nobody other than those with staff files or confidential material should be permitted to lock their filing cabinet. File audits should be on a genuinely random basis and excuses such as 'it's in typing' or 'I've taken that one home' should be met with a request to produce the file within a short time period. You may want to consider introducing a policy about taking files out of the office.

Be aware of employees who may be suffering from stress or financial problems as a result of illness, bereavement, divorce or other family issues. Look out also for anyone whose lifestyle seems to be at odds with what you know of their income – there may be a genuine explanation for this but exotic holidays, expensive clothes or new cars could indicate someone living beyond their means. Sadly sometimes fraud is committed to pay existing commitments or to meet gambling debts and so there may be no external indicators.

External theft

Theft from someone outside the firm is an obvious risk and most firms will have systems designed to defeat this. It is unfortunately still possible for theft to take place and sometimes this will require someone working at the firm to co-operate with the thief in order to circumvent those systems.

Cyber-attacks have become more common; this can involve 'hacking' a firm's website and substituting different bank account details, or even contacting a firm's clients directly and supplying 'new' bank details. Direct access to a firm's bank accounts is unlikely but there has been an increase in reports recently of fraud which the law firms concerned say could only have been executed by someone with access to the bank's details.

Criminals also commit theft by hacking email traffic between firms and their clients – our Claim team has seen cases where emails purporting to come from the client have authorised the firm to remit monies to a new bank account, which is in fact under the fraudster's control. There are also cases of clients receiving what appear to be genuine emails from their lawyers, providing bogus account details to which the client is asked to send funds, say on a property transaction. Some potential controls include – The adoption of 'strong' passwords – using a combination of letters, numbers and symbols, for example – by both lawyers and their clients on their email accounts, which are not used elsewhere.

Both lawyer and client being clear from the start of the retainer about account details and that notification of any changes will require separate verification – for example, a telephone call – to check whether an email providing new account information is genuine.

Other cyber-related crime includes:

Phishing
The use of emails from apparently genuine sources to obtain money or information

Malware
Malicious software which is downloaded by opening apparently innocuous emails

Controls around these issues include maintenance of anti-virus software and the need for care when dealing with emails from an unfamiliar sender.

Social engineering

Social engineering is a common element of fraud. Broadly speaking it is action which manipulates people into performing actions or divulging information. The concept is similar to 'phishing' but often involves telephone contact, so it has become known as 'voice phishing' or 'vishing'. One recent development is known as 'Friday afternoon fraud'.

Conveyancing firms are targeted, usually on a Friday when the accounts department is likely to have a number of transactions to complete. The fraudster will have done some homework to identify the firm's bank account details and sometimes the name of the cashier or accounts staff. They may also have been able to clone a genuine telephone number so that it looks as if the call is from a number associated with the firm's bank.

Sometimes the fraudster refers to genuine transactions made by the firm that day, which tends to suggest they have some inside information or the ability to hack into the bank's accounts; on other occasions they list bogus transactions which they say have been made, thereby making the cashier believe that fraud has already been committed on the account and that it needs resolving urgently. Having established that they are from the firm's bank and that the account is under attack at a very busy time, they will then persuade the accounts staff to disclose details of the firm's security code.

There are other forms of manipulation; the client who is impersonating a property developer or a businessman is likely to use language designed to convince you that they are bona fide, they may take 'urgent' calls during their meeting with you or produce documents which indicate their financial wealth.

Another form of social engineering is Advance Fee Fraud or 'S.419 fraud', after the section of the Nigerian Penal Code prohibiting this. Typically the writer of a letter or email will claim to be entitled to a large sum of money to which they are presently unable to gain access. They will ask for help, usually in the form of financial assistance to pay taxes or legal fees and will promise to pay commission or a fee to the person who has helped them to release these funds. Despite this type of fraud being well-known for a number of years many people – including solicitors – have fallen foul of this and continue to do so.

Money laundering

Law firms are often targeted by people outside the firm to assist them in laundering the proceeds of crime. Failure to detect this is not only a breach of regulation for lawyers but can also lead to criminal prosecution of the individuals involved. The process could simply involve the firm being used to purchase property with illicit funds or your practice could be used to receive money and then to transfer it elsewhere thereby 'laundering' it. Conveyancing practices are particularly at risk of this because a property sale/purchase is an easy way to transfer a large sum of money, but firms may also be instructed on (say) a litigation matter and paid a large sum of money on account of costs only for the client to withdraw their instructions shortly afterwards and request repayment.

Mortgage fraud

Mortgage fraud is probably the highest risk for theft and dishonesty claims against lawyers because a mortgage advance is an easy way to get hold of a large sum of money in one transaction. This type of fraud can include social engineering, the knowing involvement of someone within a law firm and collusion by others such as mortgage brokers, surveyors or estate agents.

Even though the money is not being stolen directly from the firm, it can lead to claims if the money was in their possession and it cannot be accounted for – a mortgage advance for example which is paid to a fraudster rather than to the seller. In other circumstances the firm, or rather an individual within the firm, could be charged with having assisted a criminal to launder the proceeds of crime.

The fraud could be a simple application fraud – the client is claiming an income or assets that they do not possess – or the client could be using a false identity. The fraud could involve an inflated valuation of the property designed to persuade a lender to offer a larger loan; or it could be a wholesale fraud involving a bogus firm which results in the entire mortgage advance being paid away to the thieves.

Remember that reputable firms are often targeted by money launderers and mortgage fraudsters because they want to give credibility to their transaction.

Know your client

The first defence to any sort of external fraud is 'know your client'. All clients must go through the firm's ID procedures and you must have valid and current identity documents on file. While you are not expected to act as forensic scientists, if there is an obvious error on the face of a document it will not protect you. Insurers have seen examples such as a copy passport purporting to identify the seller of property. A glance at the office copy entries would have shown that the person purporting to be the vendor was only five years old at the time that the property was purchased. Other examples are passports or certificates which have obvious defects such as missing watermarks or white correction fluid over parts of the document. Documents for new clients should be checked by a fee-earner; it is unfair to delegate this task to reception or support staff.

Even if the identity documents seem satisfactory, take the time to get to know the client – if you are not able to meet face-to-face then you should be particularly careful to get proof of identity. If the client seems vague or uninterested in the details of the matter, particularly where property is concerned, then this should ring alarm bells. Find out why they have instructed your firm especially if they do not live locally. Classic signs of mortgage fraud are identified in the Law Society's practice note and all fee earners working in the Property team should be familiar with this. Clients may instruct the firm on a different matter in order to gain credibility before attempting a fraud. For example they may seek matrimonial advice but decide not to take any action; or they may instruct you to claim a debt and even pay money on account of costs. The debtor is likely to be part of the scam because acting for the client in this matter will build their profile and convince you that they are genuine. When they subsequently instruct the firm on a property matter, you may not feel it necessary to make any further enquiries as they have established themselves as an existing client.

Corporate clients can also present the potential for fraud. First and foremost of course you must be sure that the company instructing you is genuine, that it has not been struck off and that the individual giving instructions is authorised to do so on behalf of the company. Corporate structures are often used to commit fraud however because of the availability of 'layering' – funds can be transferred between different entities in order to disguise their origins. If the company you are dealing with has a parent company or corporate shareholders

then it is important to investigate the background until you are satisfied that you know for whom you are acting. If you are asked to transfer money between different entities or if the transaction is complex and involves a number of different corporate bodies then be alert to risk and make sure you have a clear line of instruction and that you know exactly who is representing the various bodies.

Bogus firms

Bogus firms have become an increasingly common way of committing fraud. The name and address of a reputable firm is often used to produce a letterhead, showing a branch office with a P.O. Box number and possibly a mobile phone number for contact. A bona fide purchaser's solicitor will correspond with the firm but when they have paid over the mortgage advance they will discover that the firm did not exist and that the purported vendor did not have title to the property.

Unless you know the other firm well, always check that they are genuine; ring the SRA to verify their identity, check the SRA's 'Scam Alert' facility, or call the firm's main office (at a number verified independently from their letterhead). Also check the Law Society's 'Find a Solicitor' website, though note that this is not infallible – in one case fraudsters managed to register a bogus branch office of a firm as part of a scam. Litigation has ensued and the defrauded firm is seeking recovery from the Law Society, which is defending the case.

Duty to lenders

If a client is intent on defrauding a lender they may also defraud your firm; as noted above they are keen to use a legitimate firm to give credibility to their actions and so they will not want your firm to see that a transaction is not genuine. You must however notify the lenders if there are any elements of a transaction which you think are suspicious including payments being made direct between the parties.

Probate fraud

This is increasing according to The Society of Trust & Estate Practitioners (STEP). This can range from impersonating a testator in order to make a will (see the 'know your client' notes above) to impersonating an executor or beneficiary, concealing assets, removing property from the estate and lying about the status or existence of beneficiaries.

More worryingly a high proportion of theft from clients' accounts takes place from Probate or Trust accounts. It is particularly important that cheques are not presented for signature without supporting documentation and ideally cheques should not be signed by the person dealing with the estate or trust although of course this is not always possible.

Trusts

Offshore trusts are increasingly used to launder money. As with all areas of work it is essential to know who you are acting for and the source of any funds being deposited or transferred. Any suspicious activity should be reported to the firm's Money Laundering Reporting Officer (MLRO) to consider whether a formal report is needed. It is a clear breach of the Solicitors Handbook to permit the firm's Client Account to be used to transfer money without a genuine underlying transaction. Always be wary of clients who are keen to pay money on account of costs, sometimes in excess of the sum you have asked for, and have a rule as to how much money you will accept in cash.

Payments into your firm

It goes without saying that bank accounts should be reconciled regularly and any deficit tracked down. It may seem less of a problem if your firm has an unexpected credit, however this is a tactic used by fraudsters to 'clean' money. Do not accept a payment into your account unless you have clearly identified the client concerned and understand the source of funds and the purpose of the payment in.

Conclusion

Fraud is a real and present danger to legal practices whatever the type of work that you do. The best defence is to have policies and procedures in place which will protect your employees as well as your firm.

Review these regularly and ensure that everyone in the firm is complying with them. Training on all aspects of fraud (not just on money laundering) is essential and encourage everyone in the firm to get to know their clients and to consult someone else for advice if they have concerns (suspected breaches of Money Laundering Regulation must be reported to the firm's Money Laundering Reporting Officer in any event).

Insist on random file checks, and be alert to colleagues who may be suffering from stress or financial problems – but remember that most fraud is based on transactions or behaviours which can have a legitimate cause. It is your job to distinguish these from the fraudulent ones.