Risk alert

Fraud warning: Beware funds transfer instructions received by email

We have been made aware of thefts and attempted thefts of client funds and firms' own money where, believing them to be genuine, law firms have acted on emails providing bank details or payment instructions for funds transfers.

Scenarios:

- In one case, in another jurisdiction, 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.

In reality:

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.

These cases follow a case where solicitors acted on payment instructions in an email erroneously believing the email to come from the beneficiary of an executry estate. This scenario was flagged in the Journal in November 2014 and, for ease of reference, the Journal text is reproduced below.

Risk controls:

Before acting on instructions for funds transfers:

- **ENSURE** validation/verification of ALL bank account details.
- **CONTACT** the client/other firm by a different means for confirmation of instruction and bank account details.

If possible **DO NOT** send bank account details other than by encrypted message with a password.

SHARE this Risk Alert with all colleagues.

ENSURE the Risk Alert is read, understood and acted on.

March 2015

JOURNAL ARTICLE

“Frauds and scams – increasing awareness”

17 NOVEMBER 14

Against an increasing risk of falling victim to fraud, which some still underestimate, this article considers the profession’s exposure, and steps to reduce the risk

by Alistair Sim

External frauds and scams

Happily, relatively few firms have been through the distressing experience and financial impact of a fraud, but that does not mean it is safe to assume that it will never happen to your practice.

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 risks and their consequences.

Sadly, we are all exposed to frauds and scams in our business and personal lives. On their website, ActionFraud lists a veritable A to Z of frauds and scams, including:

Account takeover

When a fraudster or computer criminal poses as a genuine customer, gains control of an account and then makes unauthorised transactions.

Cheque fraud

Any illegal use of cheques to acquire or borrow funds, including counterfeiting, forged cheques, fraudulently altered cheques, bad cheque writing, cheque washing and using disappearing ink.

Invoice scams

Fraudsters may send an invoice or bill to a company, stating that the due date for payment has passed, or threatening 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.

ActionFraud's website includes news items highlighting types of fraud and scam which are particularly prevalent. At time of writing they highlight frauds and scams which have afflicted smaller businesses and which could target law firms.

Experience of the profession

The role solicitors play in client transactions, and the fact that solicitors often have control over substantial sums of client money, may make the profession a particularly attractive target for fraudsters' activities. Some fraudsters are opportunists, but many of those who target the profession and its client funds are members of 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" and to commit confidence tricks to overcome barriers and risk controls that might have been considered more than adequate.

Theft from client bank account

Case study

Firm A had £500,000 stolen from its client account after a member of the firm's finance team was tricked into disclosing password/PIN information. With that information, the fraudster was able to transfer client funds using the bank's automated bank transfer facility. Transfers of funds were effected overnight and this was only discovered the following day.

It's an uncomfortable fact that a number of firms have had client funds stolen from their client bank accounts in the way described. Members of cashroom teams have been victims of very clever confidence tricks. They were all convinced the caller was a genuine member of the bank's staff legitimately responding to a real fraud involving the firm's client account and helping the firm to put things right.

In each case, the fraudster posed as a member of the bank's fraud investigation team contacting the firm under the pretext of suspicious activity on the solicitors' client account with the bank. 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.

Reality check

The client bank account thefts relied on persuading staff in the firms' cashroom/finance teams to reveal security information (or otherwise comply with the fraudster's instructions), and thereby facilitate access to client bank accounts via online banking.

This necessarily requires a range of measures starting, importantly, with risk awareness and including other checks and controls.

A series of risk alerts has been issued highlighting a number of important risk management points:

- the need to maintain awareness of current frauds and scams by reading risk alerts and tapping into other sources of warnings;
- the importance of ensuring that all colleagues (including cashroom/finance team colleagues) are fully aware too – this is a situation where a weak link in the practice's risk management can undermine the best efforts of everyone else;
- that you never disclose password, PIN or other security information;
- not allowing yourself to be persuaded or tricked into believing someone must be genuine just because they have private information about you, your practice, your bank account, bank account transactions or your clients to which only a genuine bank employee could legitimately have access.

Interception of email correspondence

Case study

Solicitors handling the administration of an executry 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 solicitors handling the executry were suspicious of the email and made contact with the beneficiary (not by email) to establish whether it was genuine. Their vigilance meant the fraudster's attempted fraud was thwarted.

This “near miss” arose in the course of the administration of an executry, but could a fraudster commit a similar fraud by intercepting email correspondence between solicitors and their clients in other types of work? Debt collection? 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, a personal injuries award or a company sale.

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 of fraud.

What else?

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 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 is also in a position to provide false validation by intercepting your email request for confirmation.

Also watch out for any change to your client’s email address. It may be a subtle change, designed to deceive.

Alistair Sim and Marsh

Alistair Sim is a former solicitor in private practice, who works in the FinPro (Financial and Professional Risks) National Practice at Marsh, global leader in insurance broking and risk management. To contact Alistair, please email *alistair.j.sim@marsh.com*