THE LAW SOCIETY
OF SOUTH AUSTRALIA
THE VOICE OF THE SOUTH AUSTRALIAN LEGAL PROFESSION

risk watch

MAY 2016

Keeping a watch on fraudsters

- **Grant Feary, Deputy Director, Law Claims**

Don't get caught out by fraudsters. Make sure that all your internal systems – including IT systems – are robust and up to date.

The Solicitors Regulatory Authority in England, as well as the professional indemnity insurers of English solicitors, have reported a significant number of claims against solicitors as a result of criminal frauds being perpetrated on English law firms, particularly those firms with practices in conveyancing. These scams tend to involve a combination of identity fraud and cyber fraud, such as "*hacking*" and "*spear-phishing*". It would be short-sighted and foolish to think that these sorts of frauds could not happen in South Australia.

Firms with practices in conveyancing are particularly targeted because of the large amounts of money that pass through their trust accounts. In England these sorts of frauds have become known as "*Friday afternoon frauds*" because the fraudsters realise that, in England, many property transactions are completed on Friday afternoons and that is a time when large amounts of money are moving in and out of various bank accounts. The term "*Friday afternoon fraud*" has helped to raise the profile of the risks, however it is obvious that these frauds do not occur only at particular times and vigilance **at all times** is required.

The techniques used are sophisticated and targeted: these are not necessarily opportunistic "*smash and grab*" type frauds: the fraudsters may spend weeks preparing for each fraud. According to insurers in Australia – who are making significant efforts to alert businesses to the risks of "*cyber-fraud*" - it is not unusual for those behind these frauds to be organised crime syndicates, sometimes based in Russia.

The fraudsters may use a variety of methods to convince a law firm that they are someone else – eg the firm's bank, the client's bank or even another law firm. They try to trick the firm into releasing information that will allow them to gain access to bank accounts, or even into transferring funds to their account. They may, for example, call pretending to be the firm's bank, saying that they think the firm may have been subjected to a fraud already and seeking account details.

The experience in England is that these calls can be very convincing and professionally done. The person on the other end of the phone may come across as credible, well-spoken and articulate and sound like they are speaking on a local landline: things have well and truly moved on from calls from a Nigerian Prince seeking assistance in moving his oil-wealth off-shore!

"*Spear-phishing*" emails –emails that appear to be genuine but aren't – seeking bank account details/passwords and the like are also common. Other techniques are creating an email address that looks like it belongs to your firm's client, as well as hacking the client's genuine email account and sending emails from that account.

It is not only client money which is potentially at risk. In one case in England, a medium size firm (XYZ Solicitors) sent invoices to nine clients by email. The firm provided details of their bank account and asked for payment within four weeks. Not having received payment, the firm practice manager called one of the clients and was informed that the client had already paid, using the bank details provided on the invoice. The practice manager obtained the bank details from the client and found that the client had made a payment to an account held by XYZ Law (rather than XYZ Solicitors). The other eight clients had also made payment into XYZ Law's account.

Subsequent investigations revealed that XYZ Law did not exist and that the fraudsters had hacked into XYZ Solicitors' email server, intercepted the emails and replaced the genuine invoices with fake ones containing the different bank account details. According to an IT security expert subsequently engaged XYZ Solicitors, up to date antivirus, internet browser and operating system software may have prevented the fraud.

The best protection is for there to be strong internal controls as to the verification of the proper destination of trust funds as well as robust IT security. Important risk management tools include:

- protecting operating systems with up to date security;
- using secure wireless connections with encryption software;
- making sure that all account operators use strong, unique and regularly changed passwords; and
- training employees about the risks so that they are constantly vigilant.

GRANT FEARY
Deputy Director (Law Claims)
Email: ***gfeary@lawguard.com.au***