QBE Europe

Cyber attacks on solicitors. Are you protected?

In recent months, there has been a significant rise in the number of legal firms being targeted for fraud, from bogus law firms and bank impersonators conducting identity fraud to email hacking and the interception of post. These attacks have financial, operational and reputational consequences for both the firms involved and their clients. The solicitors' profession has clearly been identified as a soft target and one where the costs and risk of perpetrating fraud are considered to be outweighed by the potential gains. The variety and frequency of fraud is escalating to such an extent that it can no longer be ignored. Effective measures must be put in place now.

In the case of a fraud in relation to a property sale, recently highlighted by the media, a large sum of money was stolen by hackers who hijacked an email account to send an email to a client's solicitor, advising them to transfer the property sale proceeds to the hackers' own bank account. From the solicitor's point of view, this request appeared to be legitimate and by the time the client discovered the fraud, several days later, the proceeds could not be reimbursed. Hackers use extremely smart techniques which make their crimes almost imperceptible, but in this case duty of care and possibly money laundering concerns should have arisen as soon as the request to change the destination of funds was made.

We recommend that solicitors consider the following:

i. How and at what stage does your firm verify that the destination account for proceeds of sale aligns with your client identity checks and is agreed by both parties?

ii. What checks would you conduct if one of the parties in a dual authority transaction were to request a different destination for the funds?

iii. What client identity / ultimate owner questions are raised when an account without an ID is requested for funds transfer?

iv. What policies and procedures are agreed and understood practice-wide to deal with the above in a consistent way?

It is easy for conveyancing firms to become complacent when the handling of large sums of money is a routine occurrence and the pressure to complete is ever-present. Now that more and more firms are being targeted for fraud however, this complacency can have serious ramifications.

Under Principle 10 of the SRA Handbook, the SRA places a duty on regulated firms to protect client money/assets. If your firm holds personal identity information (PII) or banking details, and has a high reliance on IT systems, websites and email to conduct business, it is essential that appropriate time and investment is attributed to IT security, good practice policies and processes, and education and awareness raising within your practice in order to reduce your cyber risk.

What can You do to Protect Your Firm and Your Clients?

It would be impossible to write a bulletin to advise of some individual control or other that would prevent or reduce the likelihood of attack each time a new type of fraud emerges. IT controls do of course help but fraudsters will always work to find a way through the weakest link in the chain. In this document we look at other controls, that also need to be considered when looking at ways to mitigate against fraud in your firm.

People Power

While robust IT controls are essential, your best defence is your people. Ensuring everyone is educated in the risks, prepared to ask the awkward questions, and knows how to investigate anomalies, is critical in the fight against fraud.

Hackers know that people tend to follow orders without question, respond to authority, genuinely want to help clients and colleagues alike, and start from a position of trust. Often a fraud cannot be successfully completed without cooperation, willing or otherwise, from someone within a firm who is needed to complete a stage in the transaction, e.g. giving out authorisation codes, changing the destination bank account, or issuing funds without adequate checks. Just recognising that something is outside of the usual protocol can be enough to protect your firm.

Practices should encourage employees to:

- be vigilant and to assume that any unusual request has potential to be a fraud attempt
- consider the evidence in requests – is there enough for you to be certain you are dealing with your client? Try to contact the individual to see if location and contact ease appear normal and verify their email request
- ask questions, and obtain further evidence – request a copy of a paying slip (includes account name) for funds transfer
- discuss unusual requests with peers, or your COLP, COFA or MLRO
- question instructions.

Preventive Action

Q. When you read or hear about fraud committed against other firms, do you:

A Spot the opportunity, you might pick up some worried clients of theirs

B Breathe a sigh of relief that it wasn't your firm

C Smile smugly because you know your systems and training are all up to date and are the best they can be (aren't they?)

D Find out as much as you can, discuss the issues openly with everyone and make sure your own controls would have stood up to the attack, and if not, strengthen them?

A. If the answer to the above is anything other than D, you may find you are leaving yourself open to attack. As we have said before the nature of the attack and the tactics that fraudsters employ are changing constantly, firms need to stay on top of this to ensure they are as protected as they can be.

Assess & Respond

If you have completed a QBE Risk Assessment Questionnaire at some point, we will have asked you whether you regularly conduct risk assessments aimed at the prevention of financial crime. Unsurprisingly the vast majority of firms answer 'Yes' to this. Consider this however, with what vigour and competence are those assessments completed?

Firms don't know what they don't know, so we would advise they seek expert help. This will cost money, but it could be one of the best investments a firm makes. If you have already got a Cyber Risk Policy, there will likely be contacts on there that can assist, so contact your broker in the first instance to find out what is available under your policy.

Leadership

Part of your activity in D above will be to educate. How you choose to do this can be the difference between success and failure in delivering your message. You could simply flick on a copy of the article to the whole firm with a cover note saying 'Please be aware!'. Or, you could gather people together, get a debate going, and agree on the action to be taken. Most importantly leaders need to give their people a mandate that says it is okay to stop a transaction and to ask questions. Giving this reassurance face-to-face and in a group is so much more effective because it demonstrates openly a firm's commitment to the policy, removes doubt and unites the team into the right behaviours.

Systems

All firms are likely to have some of the following controls in place, but need to challenge whether they are doing as much as possible. Is everything as up to date and robust as it could be; is everyone up to speed and fraud-savvy? If you are asking questions on how, why or what in relation to the controls listed below, you can bet others are too so it is essential that someone within each practice is responsible for keeping fully informed and can cascade information as relevant.

Key controls are as follows:

- Protect your operating systems with up to date security software (e.g. anti-virus, anti-spam, anti-spyware, firewall).
- Ensure secure wireless connections such as a virtual private network (VPN) software is used to encrypt any wireless communications. Note: Avoid insecure Wi-Fi connections which provide an opportunity for hackers.
- Encourage strong and unique passwords by introducing a "resilient password policy". Tip: long passwords with a mix of words, letters and numbers are more effective.
- Establish clear procedures for email usage on all devices, for example, ensuring any confidential/ financially sensitive data is both requested and sent in encrypted (password protected) emails, or better still discourage the use of emails for obtaining or confirming bank details - obtain them when you meet, use alternative channels, and destroy them once they are finished with.
- Train staff in good security practices, e.g. unfamiliar emails should be deleted immediately, preferably unopened; if opened, think twice before opening attachments, clicking links or replying.
- Encourage vigilance to inconsistencies in emails/personal details, e.g. spelling errors; email addresses; poor use of language; names on bank accounts; or any details or transactional changes that arouse suspicion should be questioned.
- If your IT is outsourced, how secure do you feel about your service provider? Ensure you ask questions of them to understand how your systems are protected.

Training

As insurers, we have been asked to promote the Law Society's free online CPD course. This was developed by the UK Government as part of its National Cyber Security Strategy with the support of both the Law Society and ICAEW. It may be a good place to start on education: **www.gov.uk/government/news/new-training-available-for-professionals-on-the-front-line-of-cyber-attacks**. Other training events are of course available. The main thing to remember is that as methods are constantly evolving, awareness training should be a regular feature and not just a one-off, so you should make this consideration part of your annual risk review each year alongside policies and processes to prevent fraud.

Insurance Cover

You may think your practice is covered for cyber exposures under your Professional Indemnity policy, however, cyber risk can span a range of cover, so it is worth asking your broker to find out what you are insured for.

At QBE we specialise in providing risk management advice for the solicitor's profession and are always available to provide counsel. If you have concerns or questions about any of the above subject matter, please feel free to contact the team directly at **solicitors.pi@uk.qbe.com**

QBE European Operations Plantation Place 30 Fenchurch Street London EC3M 3BD
tel +44 (0)20 7105 4000 www.QBEeurope.com

Made possible by QBE