Regulation Report

Cyber-Crime and Fraud Risks

We return this month to the increasingly worrying topic of cyber-crime and fraud losses, an issue not surprisingly highlighted in the recent SRA Risk Outlook update for 2016-2017. The various forms of fraud attacks have resulted in losses of large sums for a number of firms, with the SRA reporting earlier this year that they were aware of 100 large scale losses of £50,000 to £2m or more. Meanwhile the fraudsters are becoming increasingly convincing and clever, which is hardly surprising given the rewards on offer for those who succeed.

Most of the losses depend on e-mail intercepts which are possible as a result of the open nature of messages while in transmission and the use of powerful software developed for the purpose of detecting and accessing confidential data. For example, problems can be caused by *"Firm to client"* communications where the client receives a request for a payment which seems to be authentic. The fraudsters have set up a bank account to receive the funds and explain that this is a new or alternative client account. This will often be for additional funds required to complete or could be for the exchange or completion monies in a transaction. This risk can be countered by clear warnings to clients that the firm will not be changing its banking arrangements and also consider requesting funds by letter, or with accompanying phone call if by e-mail (i.e. never by e-mail alone). A warning notice should be worked into retainer letters, email footers, notices in reception areas and any conveyancing forms in use in order to flag up the risk to clients.

A further risk arises from *"client to firm"* communications where, again, the firm receives what appears to be a genuine request from the client to divert funds which are due to them to another destination such as a building society account rather than the bank account originally notified. Clients should be informed that changes to the clients' own account details are only accepted in person or by a letter which can be verified from the firm's knowledge of that client.

More direct are the *"fraudster to firm"* communications. These might take various forms, most commonly impersonating the firm's bankers. In the *"Friday afternoon"* scam, the accounts department receives a call supposedly from the bank alerting irregularities in the operation of the client account. The call is made more plausible through the use of background office noise and by any knowledge gained of the personnel involved through research by the fraudsters. The person receiving the call is tricked into releasing confidential codes so as to enable the caller to access client account. If in doubt, terminate the call and report to the bank, your insurer and Action Fraud.

And finally, firms should be aware of the problem of *"colleague to colleague"* communications. This is often known as *"CEO fraud"*. The firm's email system is hacked into. The fraudster discovers that the Managing Partner/Finance Director will be out on a given date. The fraudster then sends an email or text requesting an immediate payment, often for *"special projects"*. Firms need to be aware of this risk and train staff to understand that such requests will not be made and, if they are, they will be checked and will require personal authorisation.

General preventive measures for firms should include investment in good security software protection and activating all suppliers' updates so that the protections remain valid. Firms should also take care over the choice of passwords and avoid using personal details which might be uncovered through social media or other public information such as children's names and dates of birth. Also remember that with social media, far too much information is made public and it allows the fraudster to become *"socially engaged"* e.g. by referring to a particular hobby as a means of introduction.

The need to be alert to identity fraud was highlighted earlier this year when the conveyancers on both sides of a property fraud were found jointly liable for the £470,000 loss suffered by the buyer. In *Purrunsing v A'Court* & Co [2016] EWHC 789, the vendor's solicitor purported to act for the vendor but was actually instructed by a fraudster who was impersonating the rightful owner. His Honour Judge Pelling decided that the vendor's solicitor had made *"no serious attempt"* to comply with the duties he was under in relation to checking the identity of his client even though the address supplied by the client was not the property's address or any other address listed at HM Land Registry for that property. It was further ruled that doubts as to the ability of the vendor to sell the property were apparent from replies to the purchaser's advisers and that they also should have raised queries in this respect.

Firms should also remember that it is not possible to exclude liability for losses that a client may sustain if they fall into the category of *"civil liability"* for which there must be *"qualifying insurance"* in place under the SRA Indemnity Insurance Rules. Although professional indemnity insurance should, in theory, cover the losses, insurers are becoming much more demanding on the issue of what safeguards were in place in the first place. There have been so many claims that the insurers' attitude has hardened. There are various specialist cyber risk policies available but these are no substitute for having the best preventative measures in position.

Jayne Willetts
Solicitor Advocate
Jayne Willetts & Co
Specialists in professional regulation

Firms should also take care over the choice of passwords and avoid using personal details which might be uncovered through social media or other public information such as children's names and dates of birth.

Jayne Willetts is also a director of Infolegal - a law firm compliance and risk management consultancy - www.infolegal.co.uk

infolegal
law firm compliance advice and training