The Friday Afternoon Cyber Threat

The Legal Sector

Friday afternoon fraud causes chaos and leaves a trail of financial and reputational destruction in the legal sector. More information and warnings to clients are needed to help mitigate the problem.

Friday afternoon fraud, as the name suggests, regularly takes place on Friday afternoons - the traditional time-period for completion of property conveyancing transactions when vulnerabilities due to pressures on time and resources are high. It accounts for the vast majority (75%) of cybercrimes reported to the Solicitors Regulation Authority (SRA). The crime has the added tactical advantage of being just before the weekend, decreasing the possibility of detection as businesses close for the weekend.

Conveyancing scams are widespread due to the significant amount of money passing between law firms and clients. Further, conveyancing clients are a key target due to the volume of information they receive from their lender, estate agent, mortgage broker and solicitor.

The criminal relies on the likelihood that the client will be an easier target, less attuned to the risks than the law firm and possibly likely to miss something amongst the sheer volume of information.

A standard attack involves a criminal hacking into a computer system. A hack will be by virtue of unauthorised access to a computer system, perhaps via a weak password, keylogging or phishing. Once access has been obtained (by whatever means) the criminal typically inserts him or herself into the email conversation and following that, falsifies emails.

Classic fraudster emails include:

- Contacting the client pretending to be the law firm. The email (ostensibly from the law firm) typically asks the client to pay their completion funds into a bank account which is, in fact, the fraudster's bank account; or
- Contacting the law firm pretending to be the client or the client's bank. The intention of this strategy is somehow to gain access to the client's bank account details; or
- Business email compromise (BEC). BEC is a type of scam relying on tactics to trick employees and executives and often involves official-looking email communications impersonating a CEO or CFO to induce others to transfer company funds to the fraudster's account.

These types of crime are all forms of social engineering i.e. engineering a situation to a point where a person voluntarily departs with funds, as opposed to the outright theft of funds i.e. the cyber equivalent of a "smash 'n' grab". These crimes may also be referred to as "payment instruction fraud," "invoice manipulation", "email modification fraud", "social engineering fraud" or "payment impersonation fraud."

Insurance cover

Among the many considerations arising when these kinds of scams occur is the question of insurance coverage for the loss. Often, the wronged party expects that their cyber liability insurance will cover their loss, presumably (and understandably) as the loss has taken place in the cyber sphere by use of computers and a network system.

An inherent difficulty with this position is that these scams rarely involve the cyber security breach which we traditionally recognise as a trigger for cyber coverage. While there may have been a hack into someone's system for the purpose of either installing malware or infiltrating an email conversation, the money was not taken but paid voluntarily.

The money loss has happened, not due to a lack of IT security or a breach of the network perimeter, but due to a lack of appropriate accounting controls, culminating in a "passive" receipt of funds by the fraudster. The root cause of the money being lost is actually human error.

There is a long-standing debate (and some confusion) as to where insurance coverage should lie. As the event is not strictly a cyber event as typically contemplated under a cyber policy, should the incident be covered more appropriately under a traditional crime policy, or perhaps it should come under the coverage of a PI policy?

The relevant question may be: whose money has been lost?

If the lost funds are client funds, then the PI policy should respond to pick up the lost money and related costs and it is generally considered to be a lawyer's professional duty to keep client funds safe.

If the lost funds belong to the law firm itself, on the basis that a PI policy is a claims-based 3rd party policy, it would be more appropriate to look to a cyber or crime policy.

However, one problem is that many crime policies have exclusions precluding coverage for "voluntary parting with funds"; precisely the nature of these types of scams. That said, crime insurers have been willing to modify their policies to provide affirmative coverage for these kinds of losses.

Unfortunately, in granting this coverage extension, the crime insurers have been willing to offer relatively low coverage sub-limits for SMEs. These tend to be in the range of £100,000 to £250,000 although some insurers appear to be willing to offer higher sub-limits in some circumstances, subject to further underwriting and the payment of additional premium.

An extensive crime policy for a larger client might provide full limits for social engineering on the back of a lengthy underwriting process requiring, amongst other things, evidence of strong financial controls, segregation of duties and fail-safe call-back procedures where a supplier changes bank details.

Interestingly, there has been a reaction from some cyber underwriters who, meeting the demand of their insureds, have begun offering coverage for this peril under cyber policies, at similar sub-limits.

Whether seeking cover under a cyber or crime policy, it is vital that coverage extends to all situations where the fraudster assumes a false identity. While some wordings restrict cover to impersonation of an officer or employee of the insured company, it is imperative that coverage wordings also include losses that arise from the impersonation of a customer, vendor, regulator, lender or outside professional (such as an attorney, accountant, or investment banker). A market-leading policy will provide cover to all impersonations.

Again, in order to try to ensure that wide coverage is available, any crime cover extension should be worded so that it applies not just to the employer company's funds, but also applies to fraudulently induced transfer of any funds, as well as inventory, supplies, and other goods.

"One problem is that many crime policies have exclusions precluding coverage for "voluntary parting with funds"; precisely the nature of these types of scams".

How to protect your firm

Quite apart from cyber or crime insurance, there are other steps that companies ought to take to protect themselves from these kinds of losses.

The best protection for any company is to implement strong financial controls. Well-advised companies will need to look to other risk management tools in order to protect themselves from these kinds of losses. One of the easiest mechanisms for a business is to adopt "out-of-band" communication processes; essentially putting in place alternative "off network" means of communication for the purposes of confirming instructions.

Internal training is vital as it will alert employees to the possibilities of the types of scams. Employees should be particularly wary of:

- Unusual instructions that appear to have come from a client
- Fund transfer requests in unusual amounts
- Requests made with an unusual level of urgency or that require the transfer of funds to an unfamiliar account or address
- Instructions that change at short notice, for example new bank details
- A client's bank contacting you to report a security breach and asking for a client's account details
- Emails with sensitive account information followed by a contradictory email with different information.

As far as clients are concerned, knowing in advance about these dangers may reduce the chances of their falling victim to fraud.

Clients should be advised:

- Of how they might be targeted
- Not to email on public wifi
- Of your firm's client account bank details in person, in a letter or over the telephone; this should not be done by email as it is not a secure form of communication
- That those bank details are unlikely to change and that if they do, the firm will confirm any change in your bank details using a secure method
- Not to transfer money to a bank account whose details don't match the ones you gave them
- To send a £1 "test fund transfer" and check that the law firm has received the money before sending the larger sum
- If the fraud has already been carried out, to contact their bank as soon as they become aware of the situation and ask them to contact the receiving bank and freeze the account.

Other protections include:

- Incorporating the following to the bottom of your email signature: "Please note that this firm's bank account details will not change during the course of a transaction and we will not change our bank account details via email"
- The development of multi-level authentication and verification processes
- If you are suspicious of an email, calling the client on a trusted number to confirm he or she sent the email
- Implementing and reviewing cyber security measures including wifi security and antivirus software
- Investing in an encrypted email service
- Using secure messaging services, for example, ensuring that all communications between firms and clients remain closed off to unauthorised access.

The Changing Nature of the Frauds

Friday Afternoon Fraud is not new – the SRA has been issuing warnings since 2016. However, as law firms become more sophisticated and aware of the threats, fraudsters are having to come up with ever more convincing and sophisticated methods of obtaining access to funds.

The very clear message is that the whole legal industry needs to be aware of the dangers. Scammers are not only looking at different mechanisms but also for targets outside the conveyancing sphere. Estates and probate administration is another obvious target. Be ever watchful and do your investigations; the fraudsters are doing theirs.

For further details please contact:

Vanessa Cathie | Account Executive,
Global Professional & Financial Risks

E vanessa.cathie@uk.lockton.com
T +44 (0) 20 7933 2478