LEGAL OMBUDSMAN

Guidance

Our approach to dealing with cybercrime

Summary

Cybercrime is now one of the most prevalent types of crime in the UK and because of the amount of money and sensitive information you handle, lawyers are an obvious target.

In the last year there has been an increase in the number of complaints we have received where money or data has been lost to cybercrime. The most common example we see relates to modified email fraud where the criminal impersonates the lawyer and asks the client to send their house deposit to another bank account.

While being the victim of an attack will not in itself mean your service has not been reasonable, we have directed a number of lawyers to reimburse clients for losses they have incurred where the lawyer failed to take reasonable steps to protect themselves and their clients from the risks, and/or where they have not taken appropriate steps after being informed of an attack.

What do we expect from you?

In considering these types of complaints, we will look at whether or not you have followed best practice issued by your regulator and professional body. Over the last four years the Solicitors Regulation Authority, Law Society, Bar Council and the Council for Licensed Conveyancers have all published information, good practice, guidance and suggestions about protecting against the risk of cybercrime which we expect you to take seriously.

The steps you take will differ depending on what risks you have assessed, your needs and the size of your firm and each case will be considered on its own merits. However, at a basic level, the steps we would expect you to take should include:

- keeping browsers, servers, operating systems, anti-virus software, malware protection and firewalls up to date (using the ‘automatic update’ option where available);
- making sure all laptops, PCs and mobile devices are encrypted and require a password when switched on;
- ensuring staff use a suitably complex PIN or password and they change their passwords if you suspect systems have been compromised;
- making sure staff are trained to recognise scams and unsolicited emails;
- creating a security focused culture in the office where people are encouraged to adopt secure ways of working that are backed up by up to date IT security policies and effective training;
- considering ways to mitigate the risk of using removable media, such as ending or restricting the use of USB sticks and SD cards and use cloud storage instead;
- considering investing in a corporate email solution that can be properly protected and controlled rather than a web-based solution such as Yahoo, AOL or Hotmail;

- ensuring clients know how you will work with them during the retainer and they know what to expect, especially concerning money; and
- warning clients about the risk of cybercrime both at the outset and at appropriate times throughout the retainer, such as when sharing bank details over email, or avoiding sharing bank details over email where possible and confirming it in writing or over the phone.

In addition to taking proportionate measures to protect against the risk of data and/or money being lost, we will also look at what steps you took to deal with the incident when you became aware of it. The steps we expect you to take will differ depending on the nature of the attack, what has been stolen and from whom. However, in most cases, we expect to see you have acted swiftly and taken the following steps:

- investigated the incident, analysed the strengths and weaknesses of your security systems and taken any necessary remedial action;
- informed your regulator, your insurers and the police/National Crime Agency; and
- depending on whether money or data has been stolen, informed your bank or the Information Commissioner's Office, or advised the client to contact their bank.

Complaints handling

Complaints about cybercrime should be treated the same as any other complaint and investigated under your internal complaints handling policy. It is likely your insurers will also be involved, especially where a client's money has been lost. The case studies set out below should give you some idea as to how we approach these types of cases.

If you are dealing with a complaint involving cybercrime and are unsure about a remedy, please contact us early on in the process where we may be able to offer some guidance.

Case studies

1. Mr M

Mr M instructed a solicitor in relation to his house purchase in late 2016. Mr M emailed his solicitor asking for the firm's bank details so he could transfer his deposit in readiness for contracts to be exchanged. His solicitor emailed him back confirming the details.

However, Mr M then received a second email, sent from the hackers but appearing to come from his solicitor, explaining that the account was actually being audited and asking him to transfer the deposit to another account. Mr M followed the instructions in the second email and sent his deposit to the fraudulent account.

Our investigation discovered that the firm were using an unsecure web-based email provider whose accounts had been hacked and users' details compromised. The email

provider published details of the hack two months before Mr M emailed the firm asking for their bank details. However, in that time the firm failed to take any steps to protect against the risk that their details may have been stolen, such as ensuring staff changed their passwords.

Furthermore, the firm failed to warn Mr M about the risks of cybercrime at any point throughout the retainer and their bank details were not included within their client care letter as per published best practice. The firm were ordered to reimburse Mr M's lost deposit as well as the costs he incurred having to abort the purchase.

2. Miss C

Miss C instructed a solicitor in relation to a house purchase in early 2017. Miss C emailed the firm asking for their bank details to transfer the house deposit. In their response, the firm attached a draft completion statement which contained their details.

However, Miss C then received a second email, sent from the hackers but appearing to come from her solicitor, asking her to transfer the deposit to another account, which she did.

In this case it was Miss C who was hacked which meant we did not have to consider the strength of the firm's security systems. However, we looked at what steps the firm had taken to warn Miss C about the risks of cybercrime and found that they had:

- included their bank details in their client care letter, which Miss C signed, along with a warning that these details would not change and should she receive an email purporting to be from them asking for money to be sent to a different account, to contact them immediately before transferring any money; and
- included a similar warning in the footer of all their emails in red font as well as in the draft completion statement underneath their bank details.

As the firm provided Miss C with sufficient warnings about the risks of cybercrime, including at the point where she was due to transfer the deposit to them, we concluded their service had been reasonable.

Further information

If you have any questions about the guidance provided in this document please contact us using the details below.

Email: enquiries@legalombudsman.org.uk

Tel: 0300 555 0333