Victorian Legal Services
BOARD + COMMISSIONER

Level 5, 555 Bourke Street Melbourne Vic 3000
GPO Box 492 Melbourne Vic 3001 DX 185 Melbourne
T 03 9679 8001 T 1300 796 344 (local call) F 03 9679 8101
E admin@lsbc.vic.gov.au W www.lsbc.vic.gov.au

RPA News

Regulation. Protection. Action.

News update for all practitioners from the Victorian Legal Services Board + Commissioner

Bulletin No. 44

Issued June 2018

Cybercrime: a growing threat to lawyers and clients

The number of scams aimed at defrauding law practices and their clients are on the rise as cybercriminals increasingly target professional services in Australia.

All lawyers must be alert to the fact that hackers are constantly seeking to exploit security weaknesses and infiltrate unsecured emails, websites and even client databases. It is a very real prospect that lawyers in Victoria, or their clients, will find themselves a target of an attempted hack or a scam designed to obtain confidential information or money.

Risks are ever present

Not all scams are as immediately recognisable as the wealthy Nigerian or an unexpected lottery win. Far more sophisticated scams are appearing regularly, catching out even cautious businesses.

The more recent examples include those where scammers have been able to compromise an email account, monitor email activity and strike at the point where trust money is to be transferred. Using the compromised email account the scammers were able to impersonate either the client or the lawyer, and sent new payment instructions to divert funds into the scammer's deposit account, before transferring those funds to untraceable or offshore destinations. Called *Business Email Compromise* scams, these have already netted significant funds from unsuspecting victims. Data from the LPLC indicate that at least one lawyer or client each week is falling victim to these scams, as is re-enforced by the most recent high-profile case. No lawyer can ignore the need for increased precautions when dealing with client instructions by email and electronic funds transfers.

How you should react

If you do discover that money has been diverted from your account, you should **immediately** contact your bank and the receiving bank to see if the funds can be frozen or recovered. The faster you do this, the better the chance of recovery. You should also contact the Victoria Police, report the matter to the Australian Cybercrime Online Reporting network (ACORN) and advise the Board if there is or was a deficiency in the trust account. Change all passwords.

Fidelity Fund will not pay

Where client money is lost to a scam, the Fidelity Fund will not provide compensation, even if the funds were held in trust. The test for a Fidelity Fund claim is whether a lawyer, or a law practice associate, acted dishonestly in their dealings with client trust money or trust property. Where the dishonesty lies on the part of the cybercriminal, the Board is not able to make a payment to compensate the client. In these circumstances the client might make a claim

against the lawyer, which may or may not be covered by the lawyer's insurer, depending on the circumstances and the insurance policy.

There is always the possibility that if you fall for a scam and your client's legal matter is affected or funds lost, you might become the subject of a complaint to the Commissioner. The Commissioner may then investigate your conduct to see if disciplinary charges are warranted. Whereas five years ago disciplinary charges as a result of a lawyer falling victim to a scam would have been less likely, today charges are not as remote, given the prominence of the issue in the media and the constant reminders about the risks that scams and hackers pose.

Protect your client, yourself and your reputation

Every lawyer has a responsibility for cyber security and it is important to recognise that secure systems alone will not protect against becoming a victim; you also have to exercise vigilance.

While there is no magic bullet to prevent your practice ever being the target of scammers, there are things you can do to minimise your risk.

- Install appropriate security software for your computer systems to prevent hackers gaining access to your email or computer systems.
- Keep your security software AND your operating system up to date. Unsupported or out of date software create vulnerabilities that hackers actively look for.
- Talk to a suitably qualified IT advisor about cyber security and identify the risks in your systems.
- Provide cyber security awareness training to all staff.
- ***Always*** check the legitimacy of ***any*** changes to payment instructions with the client directly. Do not rely on email in case your or the client's email account has been compromised.
- Ensure you have strong passwords that satisfy current best practices for length and complexity, and use a password manager.
- Use two-factor authentication wherever available for accessing cloud applications.

Resources

Law Institute of Victoria: Cyber Security Essential for Law Firms and Cyber Security Essentials for the Individual
Legal Practitioners' Liability Committee: Risk Management – Cyber Security
ACCC: Scamwatch
Australian Government: Stay Smart Online website

Fiona McLeay
Victorian Legal Services Commissioner
CEO, Victorian Legal Services Board

Contact Us
Phone: (03) 9679 8001
Email: RPAAlerts@lsb.vic.gov.au