# Are you at risk of cyber fraud?

**ETHICS AND PRACTICE UNIT**

The Ethics and Practice Unit has become aware of a growing and worrying trend in Australia whereby emails between lawyers and clients are being intercepted and criminals (or "fraudsters") are impersonating the clients and authorising payments from the law practice's trust and office accounts and sending instructions to divert their payment to a fraudulent account.

An all too common scenario is this:

The practitioner receives an email relating to an existing client in relation to a real property settlement. The "client" requests a change in bank details for which the settlement funds of $600,000 are to be deposited into. The client provides his unique matter ID given to him by the law practice. The law practice does not question this believing that its internal system is secure and the unique matter ID is sufficient identification of the client. Settlement funds are ultimately paid into the new account, only to be discovered later that it was a fraudulent account and client.

As recently reported in *Lawyers Weekly*,[1] quoting Clyde & Co partner Jenny Thornton:

> *"Your standard of care 12 months ago, 18 months ago or two years ago, is very different to what the appropriate standard is now … It won't be sufficient now just to have an email from clients authorising transfer of trust funds."*

An example used by Ms Thornton where her firm encountered a cyber breach was where a hacker intercepted a client's emails to their accountant and then forged a reply to authorise a trust account transfer. Ms Thornton recommended that as a minimum, law practices should encourage face-to-face meetings to establish the client's identity and discuss sensitive information. In addition, law practices should introduce authorisation passwords or security questions for any authorisations, establish confidential storage systems that are disconnected from networks, and double-check email authorisations via alternative means of communication: "If you're not introducing those systems – the double-checks or triple-checks – you may be considered negligent, under your PI insurance or to the client." There is also a personal risk of liability for directors and officers if their law practice is exposed to cyber breaches in future.

If you're not introducing those systems – the double-checks or triple-checks – you may be considered negligent, under your PI insurance or to the client.

ASIC's ***Cyber resilience: Health check*** report[2] released in March last year provided a checklist for companies seeking to protect their technology systems.

More recently, the Law Council of Australia President Stuart Clark has stated in relation to the Federal Government's $230 million Cyber Security Strategy[3] initiative that will seek to assist firms in protecting client information, cyber security posed a "real risk to the delivery of legal services … [and] the threat – to both lawyers and their clients – is undeniable, unrelenting and growing at an exponential rate."[4]

## HOW DO YOU VERIFY A CLIENT'S IDENTITY?

Whilst the Society does not currently have prescribed standards in place regarding client identification and verification (or VOI) it is prudent for legal practitioners to obtain and record evidence of the identity of all clients.

As a first step, we suggest that you become familiar with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* and *Anti-Money Laundering and Counter-Terrorism Financing Rules*[5] in relation to Know Your Customer (KYC)[6] – devising and adopting client identification policies which are clear about when identity checks need to happen, and ensure that all staff understand the policies - how clients will be identified, and what, if any, evidence needs to be recorded and/or stored. For example, for all clients ask for identification that will satisfy the 100-point check and record the evidence produced.

It is vital that you understand the difference between identification and verification.

Identification refers to the basic information you need to obtain and record about your client to know who they are when you are retained to provide legal services, including the client's name, address, telephone number and occupation. You are required to make reasonable efforts to obtain and record this information.

Verification refers to the information you need to obtain to confirm that your client is who or what they say they are. Verification is usually only required when you are acting for a client or giving instructions on behalf of a client regarding the receiving, payment or transferring of money, i.e. a financial transaction. When you are verifying a client's identity, you must take reasonable steps to obtain and retain a copy of every document used to verify the client's identity.

Also keep in mind that, just because a lawyer needs to ensure that something takes place, it doesn't mean that you have to do it personally. You may wish to consider outsourcing the VOI process to a third party provider. Risk management will then move from having your own processes to ensuring that you have chosen the right third party provider.

Other resources include the identification standard set out in Schedule 8 in the latest version of the Australian Registrars National Electronic Conveyancing Council (ARNECC) Model Participation Rules (MPR)and ARNECC's MPR Guidance Note 2 on VOI.

## TRUST ACCOUNTING CONSIDERATIONS

Law practices are responsible for safeguarding client funds and to replace any money that is improperly withheld or withdrawn from a client account.

There is a risk to your law practice's office account, general trust account, investment accounts, controlled money accounts, and power money by receiving fraudulent directions to make payments. Why should clients and law practices be exempt when security checks may ultimately protect both?

We urge you to consider the following:

- Never include account numbers, unique client ID numbers or pin numbers within emails.
- Refer to the client file for contact details rather than use any provided in an email especially if they differ.
- After KYC or verification of identity (VOI), obtain client bank details at commencement of matter, in person – these details must be kept securely, not on a central database that can be hacked or stolen, and definitely not on post-it notes on your computer where other staff and cleaners can see them!
- Advise clients that you will never ask them for bank details by way of email or text, only in person or over the phone and once the client has been verified,
- Advise your clients that you will not accept emails changing payment instructions, only by phone and once the client has been verified.
- Law practice security checks should be implemented in which the clients are asked to verify key data such as client name, address, date of birth and possibly a password before any sensitive information is discussed or exchanged.
- Challenge questions and a back-up email address could be implemented as part of the law practice security checks.
- Take care when replying to emails. Verify the email address, client address and contact numbers from the client file and check for any slight variances such as a change in font type, colour and size, and an altered signature or email address.
- If in doubt challenge! It's may be too late once the payment has gone!

## FURTHER CONSIDERATIONS TO REDUCE YOUR RISK

- Review your internal processes, identify weaknesses and put controls in place.
- Regularly train your staff and review internal processes to identify non-compliance and process failures as well as new and emerging risks.
- Test your systems - the easiest way to check if your systems are robust is to frequently test them without advertising your intentions in advance.
- Ensure your office and staff email accounts have strong passwords that are different to online accounts and these passwords are changed regularly and not shared, and as with bank details, definitely not on post-it notes on your computer where other staff and cleaners can see them!
- Ensure that you, your practice and clients utilise encrypted emails for confidential or financially sensitive information – this means emails cannot be opened without a secure password.
- Where the client has limited English, use an independent interpreter.
- Protect your office's devices (including computers and phones) with security software and regularly and diligently install updates. B

**(Endnotes)**

1 20 April 2016, *Firms, MPs could be exposed to cyber security liability*, Stefanie Garber: http://www.lawyersweekly.com.au/news/18401-firms-mps-could-be-exposed-to-cybersecurity-liability

2 http://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf

3 https://cybersecuritystrategy.dpmc.gov.au/ to download

4 http://www.lawyersweekly.com.au/news/18426-turnbull-cybersecurity-policy-tipped-to-safeguard-legal-profession

5 https://www.oaic.gov.au/privacy-law/other-legislation/anti-money-laundering

6 http://www.austrac.gov.au/elearning/pdf/intro_amlctf_know_your_customer.pdf



# CPD Events

For further details and to register:
www.lawsocietysa.asn.au
cpd@lawsocietysa.asn.au

All sessions that are being held at LSSA, will be held at Level 10 Terrace Towers, 178 North Terrace Adelaide

**Required CPD Activity Seminar**
17 June 2016
9.00AM – 12.00PM 3 Units *

**Employment Law Conference**
27 June 2016
9.00AM – 5.00PM 6 Units *

**Confiscation of Assets**
29 June 2016
9.00AM – 12.30PM 3 Units *

**Anti-Money Laundering**
29 June 2016
5.30PM – 7.00PM 1.5 Units *

**Unfair Contract Terms**
6 July 2016
5.30PM – 7.00PM 1.5 Units *

**Inheritance (Family Provisions) Act Update**
12 July 2016
5.30PM – 7.00PM 1.5 Units *

**Cross Examination of Documents**
13 July 2016
5.30PM – 7.00PM 1.5 Units *

**Defamation, Privacy and Search Engines**
20 July 2016
5.30PM – 7.00PM 1.5 Units *

*Total CPD Units are accurate at time of printing and should be taken as a guide only.
HAVE AN IDEA FOR A FUTURE SEMINAR?
We invite practitioners to tell us what seminar they would like to see conducted next. Email us at cpd@lawsocietysa.asn.au with your ideas.