Does your firm have an evil twin? Business identity theft

The issue

Cloned websites and criminals impersonating law firms have plagued UK lawyers for years, and this is now an emerging threat in Australia.

We are all too familiar with the problem of identity theft for individuals. Unfortunately, businesses are at risk too and professionals with a high trust rating are common targets. In the UK, several law firms are "cloned" a week. Attacks take several forms, most commonly their website or parts of their website being copied and republished (yourfirm.biz instead of .com, for example).

Phone calls, email and web search can be diverted to the 'evil twin'. Sometimes the business being cloned is the target of the attack, but most commonly the objective is a fake law firm to represent fraudsters, intercept funds transfers or distribute phishing email – leaving a trail of confusion and reputational damage behind.

What to watch for

In 2019 a long established Brisbane CBD firm found that its directors had been substituted on the ASIC register, possibly as a first step to take over their domain registration.

Around the same time a suburban firm faced repeated attempts to change the 'Find a solicitor' listing at QLS to an evil twin's web domain. This was part of a concerted campaign to clone the firm for use in a series of fraudulent mortgage transactions.

There are two things to watch for:

1. Knowing you are dealing with a fake firm.
2. Knowing your firm has been cloned.

Transferring client funds to a supposed 'solicitor' on the other side of a matter would lead to a difficult client discussion, and before accepting the bona fides of a counterpart law practice (especially if their contact details do not match those from past dealings), you should check their listing on public registries and confirm by phone.

Other businesses, such as lenders and agents can be cloned as well, so do not allow similarities of name to lead to the assumption that you are dealing with a genuine subsidiary of an established brand. Several Gold Coast firms were recently unable to settle transactions supposedly financed by a multinational lender, where the true approval had been provided by a Pty Ltd with a similar name.

What to do about it

(See annexure for an action checklist)

Prevention and early warning is key to detecting these criminals early. Such measures are cheap and fairly simple to implement.

Detecting that your own firm has been cloned is best done by setting up google alerts to tell you if your firm name is mentioned or content from your website (especially biographical information) has appeared elsewhere. Other services such as Copyscape can help detect duplication that is similar but not quite identical.

Google alerts are also a useful early warning that you are being targeted by a hostile review campaign before too much reputational damage ensues.

Company alerts are essential to give you early warning of changes to the register (this is what alerted the Brisbane firm of attempts to alter office holders).

Domain name and business name searches are also useful to check whether close or deceptive names have been registered, but these are harder to automate without using a paid monitoring service.

The most effective measure is a security culture – train staff to be aware that not everyone is who they may claim to be, and to note and follow up discrepancies and anomalies.

In the mortgage fraud example given above, the scheme was identified when a diligent mortgage broker sent a confirmation email to the website of the firm supposedly acting for the borrower, rather than just replying to the email he had been sent.

The receptionist at the firm who monitored that in-box noted that they did not have such a matter, and rather than dismissing the issue followed up with phone calls and alerts to her supervising partner. Both organisations were lucky that their staff were diligent – but both had training in place to make their own luck.

For further information please contact the **QLS Ethics and Practice Centre** on **(07) 3842 5843** or **ethics@qls.com.au**.

Business identity fraud prevention: action checklist

The golden rule: security relies on an informed workforce with a see-it-report-it mindset.

Procedures

☐ Ensure your file opening procedure checks:

1. New firms you have not dealt with before; and
2. Changes in contact details for opposing solicitors or parties.

☐ Ensure requests to change the contact details for clients, opposing firms or other parties in your practice management system are verified before being actioned. Criminals can be very convincing on the phone, so all staff need to ensure changes follow the required process.

Alerts

☐ Set up a Google alert to warn the firm if:

1. The firm name, domain name or email addresses (or close approximations) are mentioned.
2. Partner biographical details appear elsewhere.
3. Original text from your website is copied.

☐ Set up a company alert to warn of any changes to the firms' registered entities.

Make sure the alerts go to a mailbox that will be monitored and will remain in use if an individual leaves the firm. The alert should go to the position tasked with the job not the specific person.

☐ Diarise a business name search to check for deceptively similar business names on a periodic basis.

☐ Diarise a domain name search to check for deceptively similar domain registrations on a periodic basis. Consider a paid subscription service.

Compliance and Risk

Although client Verification of Identity (VOI) is beyond the scope of this note, do a quick check:

☐ Do client intake VOI procedures comply with any mandatory requirements?

☐ Does the procedure afford the firm 'safe harbor', and if not, are you happy to accept the commercial risk?

☐ Are there higher risk transactions you undertake that might need tighter procedures?

☐ If no mandatory requirements apply, how do you check that persons presenting themselves to you as clients (online or in person) are who they claim to be and represent who they claim to represent?

Considerations

- Email copies of ID documents are easy to alter
- Check that ID documents are genuine using database searches if available.
- Consider using remote VOI services. The highest standard is an in-person identification by a verification agent. For lower risk transactions, a cheaper online verification process may be sufficient.
- Register searches and minutes of appointment may be needed to confirm authority to act for an entity.