Epping Office Break-in

Recently an unfortunate incident occurred at our office premises.

We are posting this information on our website as well as contacting clients directly as we are conscious that for some of the historical and resigned clients our contact information may be old and no longer valid.

We are yet to receive any reports from current or past clients of their data being used for any purpose as at today's date 14/7/2022.

What happened?
There was a break-in at our office building sometime between Friday 29/4/2022 and Monday 2/5/2022. Staff members arrived at the office premises on Monday 2/5 to discover cupboards and draws broken into and various items strewn around the office.

The sophistication of the robbers is unknown however they took a tub of loose change, an iPad, laptops from another business and two external hard drives.

All client hard copy files were safely locked in the filing cabinets so no hard copy client files were taken. Our computers remained secure, these were not taken or accessed by the robbers.

However, external hard drives were stolen which contained client data and our own business and personal information. The data on one of the external hard drives was encrypted and the other drive containing much older information was not encrypted. The encrypted data did have protection in place and cannot be accessed normally on a laptop or computer, the unencrypted drive did not have these protections in place.

The data we held on file was different for different individuals.
For some clients we held no data except for a name and contact detail such as an email or phone number.
For other clients we held a Fact Find document containing personal & financial information, forms related to investment products. For some clients this data included ID documents to satisfy AML requirements and/or Tax File Numbers.

What are we doing to mitigate the possibility of reoccurrence?
We are completing a full review of the security at our office premises. We are looking at ways to keep your data more secure and have completed the following actions to date:

- The incident was reported immediately to Police. The Forensics Team attended the office to dust for fingerprints on 2/5. The Police conducted interviews with staff and our Building Management provided them with security access data, their investigation is still ongoing.
- The Police offered us a briefing from their specialist team to help guide the office security change decisions. We have accepted this offer and are awaiting the team's availability for the meeting.
- We have reported the data breach to the Office of the Australian Information Commissioner (**OAIC**)
- We have met with our IT provider to discuss data security enhancements. We are in the process of installing an industrial strength steel cage to house our IT equipment which will be bolted down to the concrete floor. This will be padlocked shut and secure all of these

critical devices that contain client data. We are also introducing a stronger layer of data encryption on all external Hard Drives.
- We have updated our passwords
- The issue was reported to our licensee, Hillross.
- We are reviewing and pricing additional security solutions for our office

What can you do to protect yourself?
Our key concern with the data theft that occurred, despite this data being encrypted, is the potential for identify fraud. As the Police investigation is ongoing we are still uncertain of the sophistication of the burglars so we cannot yet determine the risk associated with this data being stolen.

- For more information on identity fraud you can follow this link to the Office of the Australian Information Commissioner (OAIC) - OAIC website.
- The stolen data did not contain any of your website login information however we would recommend that you update your password if you haven't done this for some time.
- Be vigilant for any suspicious activity in unsolicited emails, text messages or phone calls.
- Further information about scams can be located on ACCC's Scamwatch which also has the ability for you to report any suspicious matters – Scamwatch website.
- You can setup additional protections for your Tax File Number (TFN) like special authorisation numbers or voice recognition by contacting the Australian Tax Office (ATO) Client Identity Support Centre on 1800 467 033.

We acknowledge the delay in informing you of these events however this is the first time we have experienced a break-in. You can appreciate there are official processes to follow, investigations to complete and solutions to research.

If you suspect that there is some suspicious activity occurring please contact our office for further assistance on (02) 9037 1434.

Kind Regards,

Susan, Sarah & Jordan