



Australian Government



Be Cyber Aware

Presented by:

Greg Lewis, Board Member, Tax Practitioners Board

What we will cover today

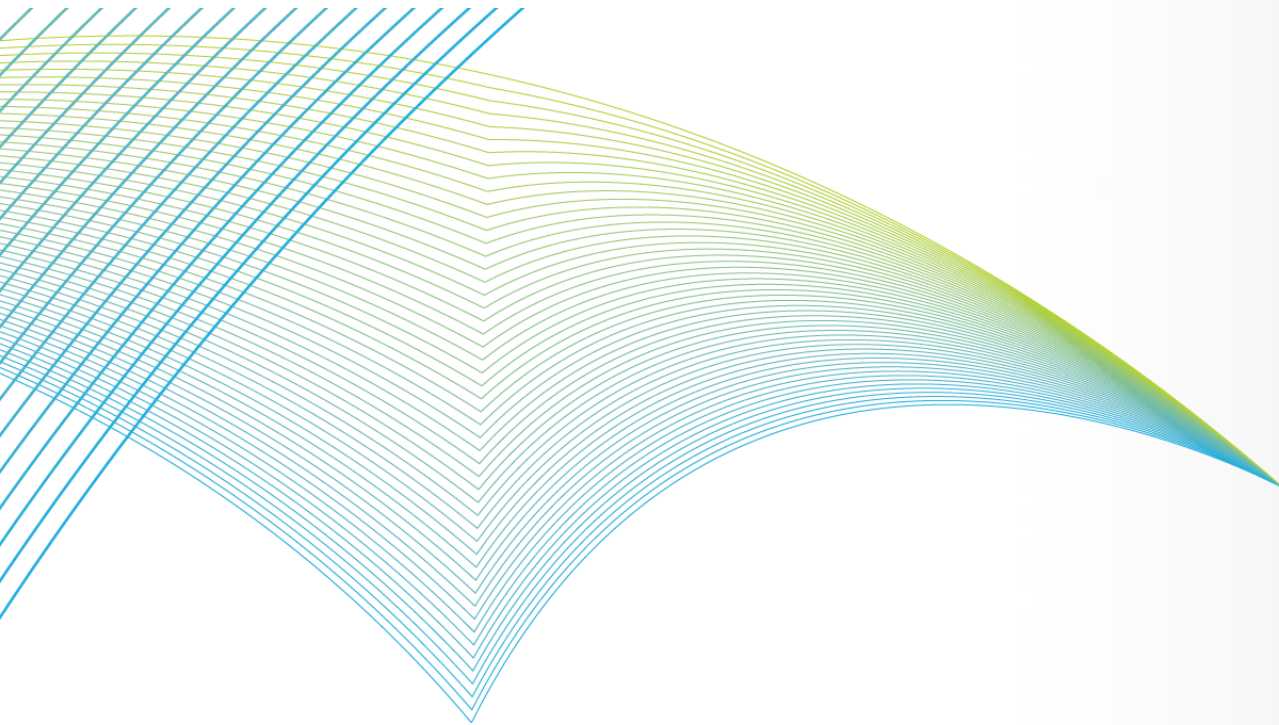
- What is a cyber-attack?
- Your obligations as a registered tax practitioner
- COVID-19 scams
- Sufficient IT controls
- What to consider when choosing software
- Notifiable Data Breaches scheme
- Where to get help
- Questions

Meet your presenter



Greg Lewis
Board Member
Tax Practitioners Board

What is a cyber attack?



Australian Government



**TAX
PRACTITIONERS
BOARD**

Types of cyber crime

Common types of cyber crime include:

- hacking
- online scams and fraud
- identity theft
- attacks on computer systems
- email spam and phishing
- illegal or prohibited online content.

First party losses from a cyber-attack

First party losses can include:

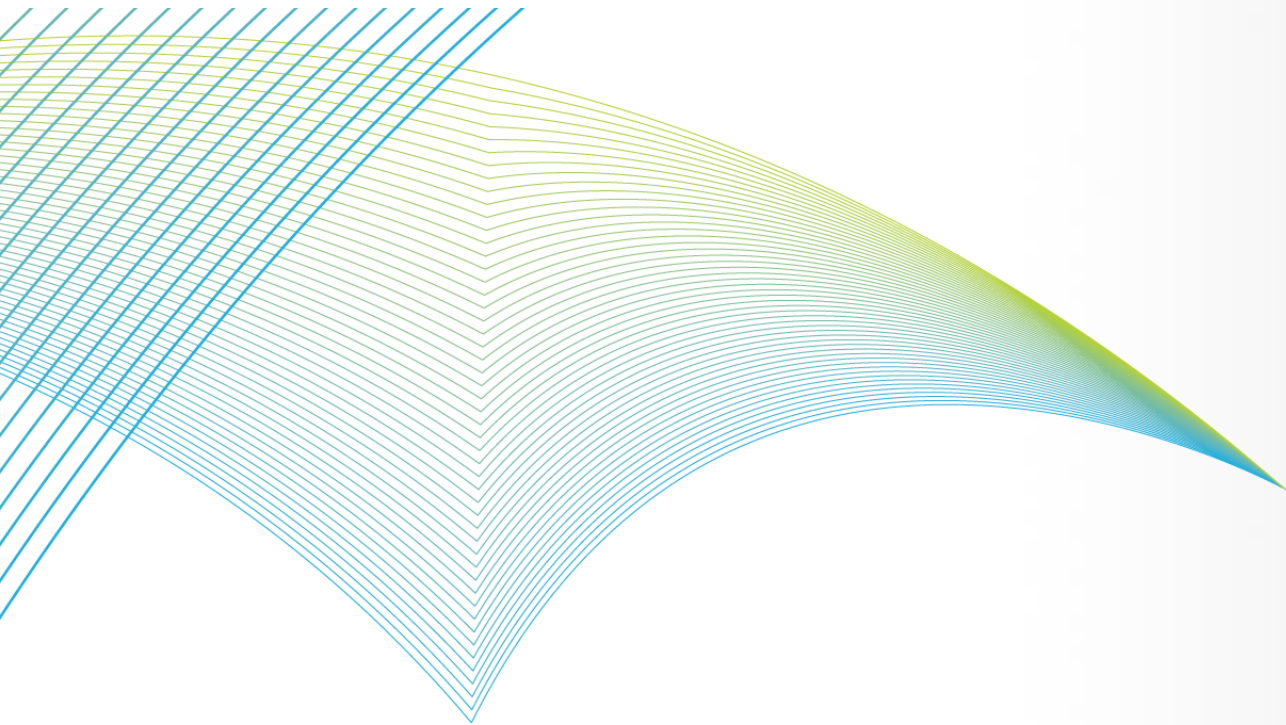
- business interruption losses
- the costs of repairing and restoring systems, or improving cyber security
- reputational damage
- extortion costs.

Third party losses from a cyber attack

Third party losses can include:

- liability in negligence for failing to properly protect client information
- fines imposed by regulators.

Your obligations as a registered tax practitioner



Australian Government



**TAX
PRACTITIONERS
BOARD**

Code item 6

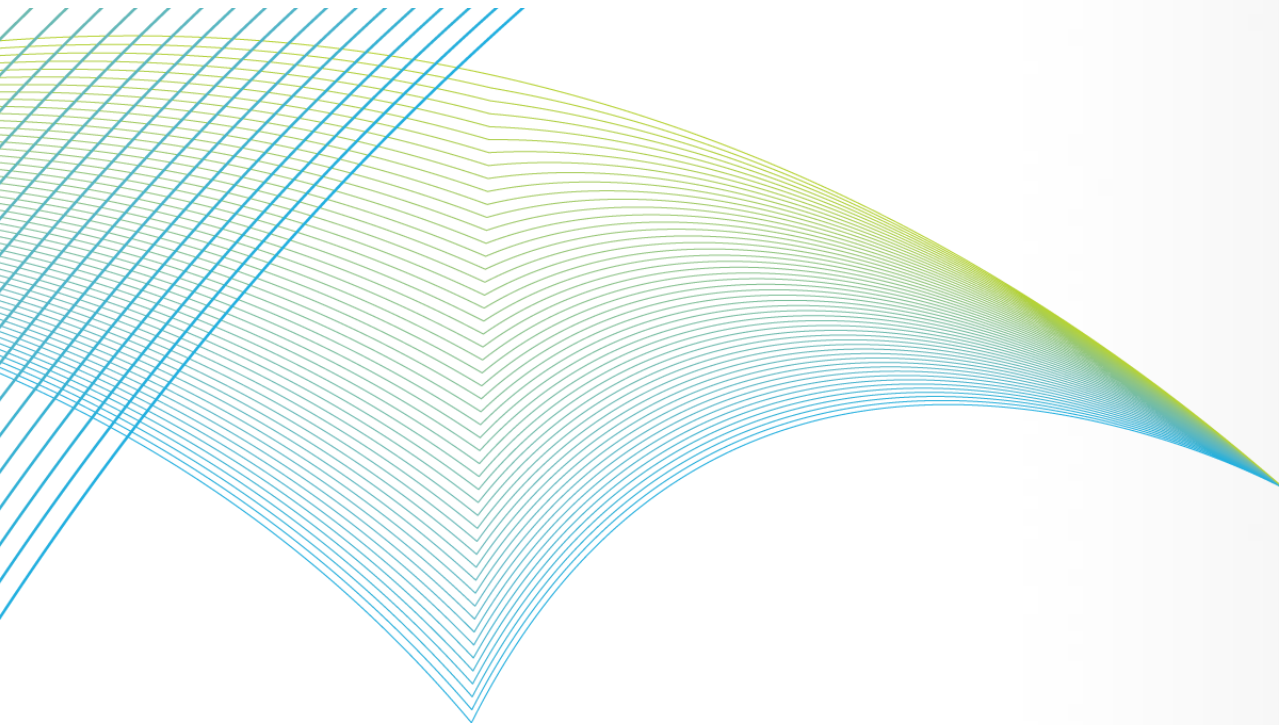
Code Item 6 - You must not disclose any information relating to a client's affairs to a third party unless you have:

- obtained the client's permission; or
- there is a legal duty to do so.

Code item 7

- Code item 7 - You must ensure that a tax practitioner service that you provide, or that is provided on your behalf, is provided competently.
- Sanctions for breaches of the Code can range from a written caution to termination of registration.

COVID-19 scams



Australian Government



**TAX
PRACTITIONERS
BOARD**

Phishing scams

- Phishing scams are one of the most common COVID-19 scams circulating currently.
- They are a fraudulent attempt to obtain sensitive information, disguised as a trustworthy entity through electronic means.
- The intent may be to get you to download malware onto your device and work systems, or to steal your personal and financial information.

Phishing scams: Financial institution


Text Message
Today 5:45 am


IMPORTANT MESSAGE FROM WESTPAC

For the safety of our customers due to the recent COVID-19 virus, all customers are required to review and update their personal details. You will be unable to use Westpac services until you have done so. Please go to <https://westpac-mobile.cc/?update> or call us on 132 032.

- Is the sender asking you to open an attachment or access a website?
- Is the URL suspicious?
- Is the sender asking you to perform a specific activity for them?
- Is the sender asking for information they wouldn't necessarily have a need to know?
- Is the message suspiciously written?

Phishing scams: Government agency


 **DSS** <dss@dssofficial.co>
[Redacted]

 **Australian Government**
Department of Social Services

The government has taken urgent steps to list coronavirus as a notifiable disease in law. As a precaution measure against COVID-19 in cooperation with Apple Inc. and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan. You are eligible to a tax refund (rebate) of \$119 (AUD)

[Access your funds now](#)

At 6.15pm on 29 March 2020, a statutory instrument was made into law that adds COVID-19 to list of notifiable disease and SARS-COV-2 to the list of notifiable causative agents.

 **by Apple**

- Is the sender asking you to open an attachment or access a website?
- Is the URL suspicious?
- Is the sender asking you to perform a specific activity for them?
- Is the sender asking for information they wouldn't necessarily have a need to know?
- Is the message suspiciously written?

<https://dss.website.official-covid19.com>

Business scams

 中國銀行
BANK OF CHINA

International Wire Authorization

To Whom It May Concern:

Our mutual member/customer [REDACTED] has informed us of their plans for wire transfer from your company. We set up a subsidiary trading account for them in the name of [REDACTED] CO., LIMITED for credit to [REDACTED]. Please set up the beneficiary account information exactly as specified below. Please contact our office if further information is needed.

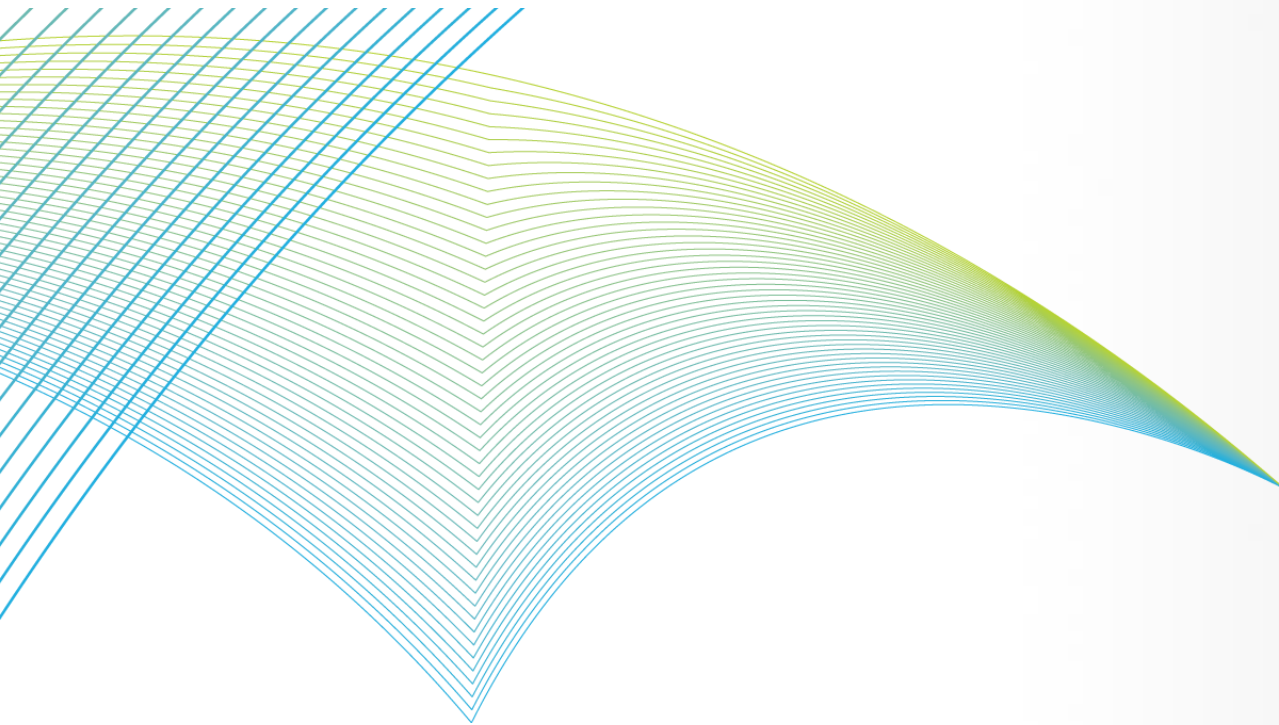
Financial Institution	BANK OF CHINA HK LTD.
Address	[REDACTED] [REDACTED]
SWIFT	[REDACTED]
Account Number	[REDACTED]
For Credit To	[REDACTED] CO., LIMITED

- Have you heard of their company before?
- Can you verify the details they've provided?
- Is this the first time they have contacted you?
- Is the sender asking you to perform a specific activity for them?
- Is the premise of their request suspicious?
- Is the spelling, grammar or tone of message unusual?

Avoiding common COVID-19 scams

- Never respond to unsolicited messages that ask for personal or financial details.
- Be very careful when clicking on hyperlinks.
- Verify the legitimacy of a contact by finding them through an independent source.
- Never provide a stranger remote access to your computer.
- Verify requests to change bank details by contacting the supplier directly using trusted contact details.
- Consider a multi-person approval process for transactions over a certain dollar amount.
- Keep the security on your network and devices up-to-date.

Sufficient IT controls



Australian Government



**TAX
PRACTITIONERS
BOARD**

Ways to protect your practice

- Remove system access from people who no longer need it.
- Ensure all devices have the latest security updates.
- Use strong and unique passphrases and multi-factor authentication.
- Work on password-protected internet and avoid public Wi-Fi.
- Comply with Protective Security Policy Framework requirements.
- Secure devices and remote desktop clients when not in use.
- Monitor your accounts for unusual activity or transactions.
- Exercise caution when downloading programs or opening attachments.
- Increase cyber security measures on remote access technologies.
- Be vigilant about what you share on social media.
- Keep updated with Australian Cyber Security Centre.

Guidance on sufficient IT controls

- We consider the following to be best practice:
 - install and maintain anti-virus software
 - deploy firewalls
 - ensure you have the latest security patches
 - protect client records or files using encryption
 - regularly change your passwords
 - consider using a second form of authentication.
- You may wish to seek expert advice from an IT security provider.

Professional indemnity insurance

- One of your responsibilities under the Code is to maintain PI insurance that meets our requirements.
- The TPB does not recommend specific policies.
- Assess the risk of a cyber attack and consider if you need to take out additional professional indemnity insurance cover to assist with first party losses.

PI insurance: Example

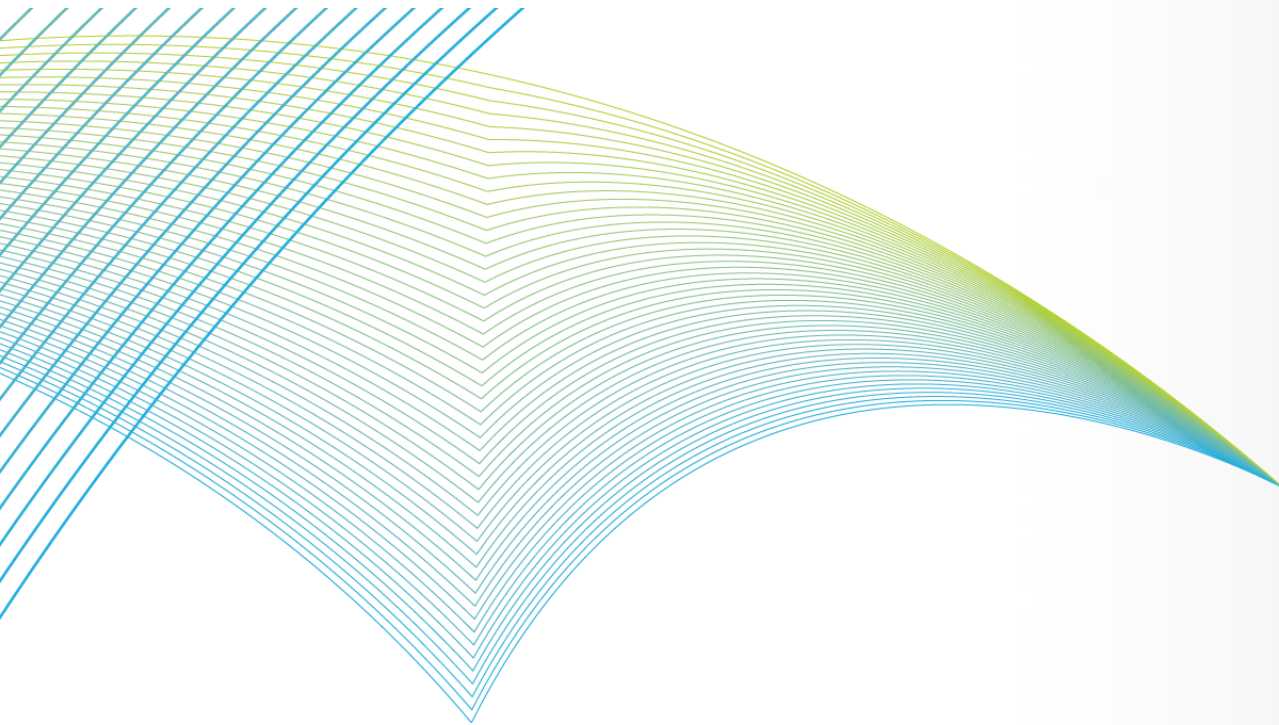


- A company had a \$2 million turnover and 8 employees.
- Their server and client records were locked by ransomware software.
- The company had the files released after paying a ransom of \$50,000 to hackers.
- Their insurance company paid them \$150,000 to cover the loss of income, the ransom demand, consultants costs, and costs to restore the network.

Continuing professional education

- You can undertake cyber security awareness training via an online course, a webinar or through professional or technical reading.
- We will recognise cyber security awareness training as relevant CPE.
- CPE activities should be provided by persons or organisations with suitable qualifications and/or practical experience in the relevant subject area.

What to consider when purchasing software



Australian Government



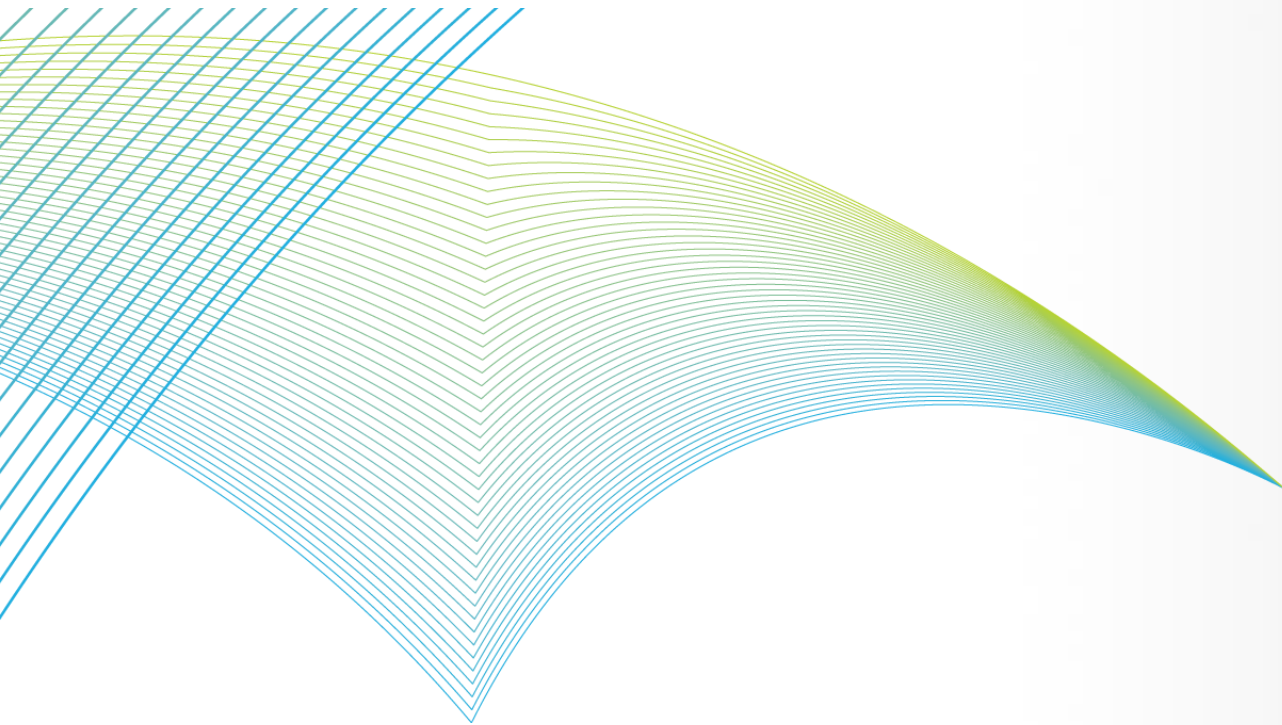
**TAX
PRACTITIONERS
BOARD**

Purchasing practice management software?

We recommend you consider:

- Does the software include security certification?
- Where will the data be stored?
- What data breach support services are offered?
- Does the software adhere to the Australian Signals Directorate Essential 8?

Notifiable Data Breaches scheme



Australian Government



**TAX
PRACTITIONERS
BOARD**

Notifiable Data Breaches scheme explained

- The Notifiable Data Breaches (NDB) scheme is an amendment to the Privacy Act 1998.
- It requires organisations covered by the Act to notify any individuals likely to be at risk of serious harm by a data breach.
- The notice must include recommendations about the steps to be taken.
- The NDB scheme commenced on 22 February 2018.

Quarterly statistics: A snapshot

- 537 notifications
- 64% were cyber incidents linked to a malicious or criminal attack that compromised personal information, including:
 - contact information (77%)
 - health information (23%)
 - financial details (37%)
 - TFNs (15%)
 - identity information (30%)
- Another common cause of notifiable breaches was human error (32% of breaches), including sending an email containing personal information to the wrong person.

Complying with the NDB scheme

- Have procedures for assessing a suspected breach.
- Ensure you have procedures and systems in place to secure client's personal information.
- Be prepared to conduct quick assessments of suspected data breaches.
- Provide training to relevant employees.
- Keep up-to-date with developments.

Examples of an eligible breach

A data breach may occur when:

- a device containing customers' personal information is lost or stolen
- a database containing personal information is hacked
- personal information is mistakenly provided to the wrong person.

What to do in the event of a data breach

If you have experienced a breach you should:

- contact the ATO
- advise any of your affected clients
- contact your software provider
- take steps to secure your information
- contact the Office of the Australian Information Commissioner
oaic.gov.au

Consequences for failing to comply



Termination



Suspension



Order

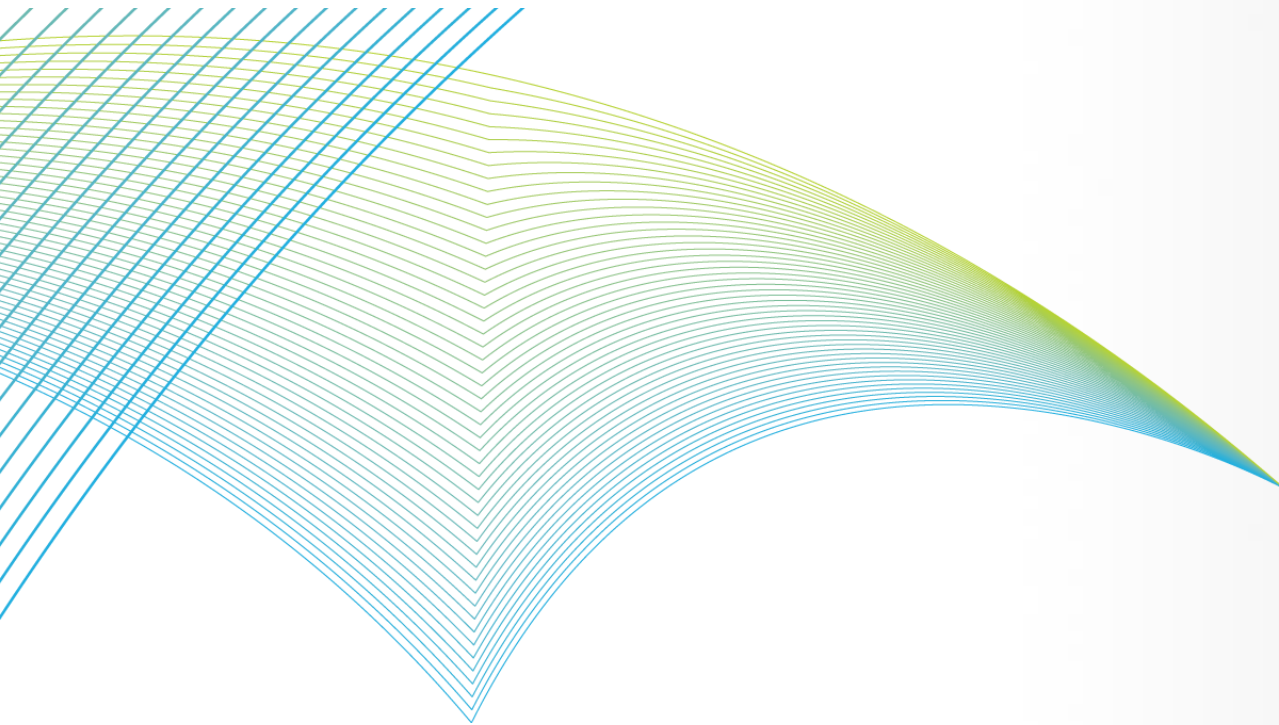


Written
caution

Where to get help

- In the event of a data breach, contact the ATO on **1800 467 033**
- TPB website **tpb.gov.au/protect-your-practice**
- Subscribe to TPB eNews at **tpb.gov.au/newsroom**
- ATO website **ato.gov.au/tpnews**
- OAIC website at **oaic.gov.au**

Questions



Australian Government



**TAX
PRACTITIONERS
BOARD**

Stay in touch



tpb.gov.au



tpb.gov.au/contact



1300 362 829
Mon–Fri 9am to 5pm (AEST)



YouTube

