Print whole section

Help with data breaches

What to do if you or your business has been affected by a data breach.

Data breach guidance for individuals

If you have experienced a data breach that has compromised your tax identity, we have advice to help protect you.

Data breach guidance for businesses

If your business experiences a data breach, there are steps you can take to limit damage to your business.

Data breach guidance for tax professionals

If a data breach occurs, we may put safeguards in place to protect information that belongs to you and your clients.

QC 101655

Data breach guidance for individuals

If you have experienced a data breach that has compromised your tax identity, we have advice to help

protect you.

Last updated 23 March 2026

How data breaches can happen

You may be impacted by a data breach where your personal information is stolen by an unauthorised third party. Data breaches can include both physical and digital records.

A data breach may be a result of:

- your employer, tax agent or another organisation's accounts being compromised
- a home or office break-in
- someone gaining unauthorised access into your computer systems or using targeted phishing emails to compromise your electronic devices
- your records being inadvertently left in an unsecured location.

Criminals can use personal information stolen during data breaches to commit identity crime. If your identity is stolen, it is difficult to recover.

How to prepare for a data breach

A data breach can happen to anyone, whether through unauthorised access, phishing, stolen devices, or large-scale corporate incidents.

Preparing ahead of time can greatly reduce harm and help you respond quickly if your personal information is compromised.

Steps you can take to reduce your risk

1. Strengthen your digital security

Use strong, unique passwords or passphrases for each digital account or platform. Reusing the same or similar passwords across platforms increases the impact if one service is breached.

2. Turn on multi-factor authentication (MFA) where possible

MFA adds an extra layer of protection by requiring a second form of verification, such as a code sent to your phone or an app. This significantly reduces the risk of unauthorised access, even if your password is compromised.

3. Keep your devices and apps up to date

Where possible, automatic software and system updates should be enabled to ensure updates are applied in a timely manner. Antivirus and security software should be enabled and maintained at a current version.

4. Regularly review your accounts

Check bank accounts, online services and email accounts for suspicious or unusual activity, such as:

- logins you don't recognise
- unexpected charges
- changes to account details.

Report anything unusual to the provider immediately.

5. Learn to recognise scams

Scammers often exploit data breaches or other events to make fraudulent messages seem more convincing. Be cautious of unexpected emails, text messages, or phone calls asking for personal information, payments, or login details, even if they appear legitimate.

For more information, see:

- Cyber security tips for individuals for more information on how to protect your identity
- Verify or report a scam for information on what to do if you think you have encountered a scam.

What to do after a data breach

If you are notified of a breach or suspect you have been a victim of a data breach, you can contact us to discuss the level of security safeguards you may need applied to your account. Phone our Client Identity Support Centre on **1800 467 033** between 8:00 am and 6:00 pm AEDT, Monday to Friday.

IDCARE provide free and confidential support to victims of data breaches and identity theft. If you are concerned about the security of your personal information and the wider impact of identity theft, phone IDCARE on **1800 595 160**.

Find out more about how to help secure your identity:

- Top cyber security tips for individuals
- Increasing your online security with myID.

How we protect clients affected by a data breach

If fraud has occurred on your tax records, we will work with you to fix your account. We may also apply protective measures to protect your account from future identity and refund fraud incidents. These protective measures may include:

- Additional proof of identity
- Additional monitoring processes
- Additional security measures

Additional proof of identity

If you are the victim of a data breach and you contact us, we may ask you for additional proof of record ownership before we discuss your tax affairs. If you use a tax professional, we may request that you contact us directly.

To discuss additional levels of security safeguards that you can apply to your account, phone our Client Identity Support Centre on **1800 467 033** between 8:00 am and 6:00 pm AEDT, Monday to Friday.

Additional monitoring processes

We will continue to monitor your record. If we identify any irregular activity, we may contact you or your registered tax professional to make sure the activity is legitimate. This may delay the processing of tax returns and other forms.

Additional security measures

Depending on your circumstances, we may apply additional security measures in our systems.

If we apply these measures:

- you may not be able to use our online channels or myGov unless you have a Strong Digital ID, such as myID.
- pre-fill data may not be available
- we may need to make extra checks for tax returns and other forms that could delay processing
- we may prevent business activity statements from issuing automatically. You or your tax professional will need to contact us before each lodgment so we can generate these statements.
- your digital identity may be suspended while we investigate if there has been a compromise in our online environment.

QC 54174

Data breach guidance for businesses

If your business experiences a data breach, there are steps you can take to limit damage to your business.

Last updated 23 March 2026

How data breaches can happen

A data breach occurs when confidential taxpayer information has been accessed by an unauthorised third party.

This information may include:

- employee payroll, tax, and super information
- confidential business documents
- banking details.

Examples of data breaches include, but are not limited to:

- unauthorised removal of computers, data, or records in both paper and digital formats
- people with legitimate access to the data using it for fraudulent activity
- accessing taxpayer files using a fraudulently obtained credential, such as myID
- criminals exploiting vulnerabilities in your IT security controls, hacking or phishing for information
- accidental disclosure of information, for example, records emailed to an unauthorised third party or hard copies left in a public place
- payroll information for your employees being unlawfully accessed
- unauthorised access to cloud-based services you use to store information.

How to prepare for a data breach

It is crucial for businesses of all sizes to have a data breach response plan in place. It details the roles and responsibilities that need to be actioned if your business encounters a data breach.

The Office of the Australian Information Commissioner (OAIC) provides guidance on how to create a strong data breach response plan. For example, it should include:

- clear escalation procedures and reporting lines for suspected breaches
- processes that outline when and how affected individuals are notified
- a record-keeping policy to ensure breaches are documented
- strategies to identify and address any data handling weaknesses that could have contributed to the breach

You should regularly review and test your plan to ensure it is current and addresses the requirements outlined by the OAIC.

Educating yourself and your employees on potential red flags of a data breach can help you quickly identify and implement your response

plan. Indicators include:

- receiving texts or emails about login attempts, password resets or multifactor authentication codes that you didn't request, such as myGov codes
- noticing changes to files and document that were not made by you or your staff
- your devices behaving differently such as glitching or running abnormally slow
- logins from devices and locations you don’t recognise in your account activity or sign-in logs.
- unexplained or unexpected activity on your credit file or bank account statements.

Further information on detecting data breaches and cyber incidents is available from the Australian Cyber Security Centre.

What to do after a data breach

You should report any data breaches to us so we can place protective measures on client accounts.

If a breach occurs within your business, we recommend you:

- Phone our Client Identity Support Centre on **1800 467 033** Monday to Friday, 8:00 am – 6:00 pm AEST, so that we can apply measures to protect your business, staff and clients where necessary.
- If you are a digital service provider or software developer, use the Report data breach form within Online Services for DSPs, or phone the SBR Service Desk on **1300 488 231**, available every day, 8:00 am – 6:00 pm AEST.
- Review the Office of the Australian Information Commissioner's (OAIC) information about notifiable data breaches to make sure you comply with your obligations under the *Privacy Act 1988*, including the Notifiable Data Breaches (NDB) scheme.
- Tell affected employees or business associates about the breach. These may include software providers, such as your payroll services, especially if you suspect the breach originated in one of their service offerings.

- Consider what information was accessed during the breach and take steps to safeguard this where necessary. For example, you may need to report inappropriate access to your myID.
- Take steps to secure the information in your business by updating all security software and controls.
- Review systems access and remove it for people who no longer need it.
- Continue to follow security best practices and reinforce these practices with your staff to reduce the risk to your business.

If you, your impacted employees, clients or business associates are concerned about the security of other personal information and the wider impact of identity theft, we recommend you speak with IDCARE on **1800 595 160**. IDCARE provide free advice and confidential support to victims of data breaches and identity theft.

Case study: Compromise of business email account

Compromised business email accounts are an increasing risk to business. Fraudsters gain access to corporate email accounts and spoof the business email address. They do this to steal personal identifying information or to defraud the company, its employees or customers of money.

Spoofing is where an email is sent from a fake website or email address disguised as a legitimate website or email address. If you hover the mouse icon over the email address, the true source of the email will be shown.

A recent report advised a tax agent's email address was spoofed by a fraudster. The fraudster sent an email, which seemed legitimate, to the agent's client list asking them to complete a personal data request form. This was an attempt to harvest client identifying information to commit future identity and tax fraud.

We took immediate action and applied protective measures to the affected client, entity and employee accounts.

Cyber and phishing attacks can be very damaging for business and can often lead to further attacks on your client, business and

employee data.

Staff education is critical. If you receive a suspected scam phishing email, **do not**:

- click on any links
- open any attachments
- download any files
- install any applications.

These files may install a virus on your computer to steal identity credentials.

How we protect clients affected by a data breach

If a data breach has occurred at your business, it is important you understand the steps we may take to safeguard taxpayer data and our tax and superannuation systems.

To protect the community we may apply treatment options to any files impacted by the data breach, which may include:

- Additional proof of identity
- Additional monitoring processes
- Additional security measures
- Appointment of a data breach manager

Additional proof of identity

If your business is the victim of a data breach, we may ask you for additional proof of record ownership before we discuss your tax affairs. This will apply when you interact with us. Even if you use a tax professional, we may request that you contact us directly.

Asking questions only you will know assures us we are dealing with your business and not an unauthorised third party.

You may also choose to have a secret password created on your record. Secret passwords validate your identity when you deal with us.

You can set up a secret password with our staff over the phone. However, if we are unable to establish your proof of identify over the phone we may request you visit a shopfront with proof-of-identity documentation or complete the tax file number enquiry form on the Australia Post website.

Additional monitoring processes

When a breach has occurred we will continue to monitor any impacted ATO records to make sure transactions on these accounts are accurate. If we identify any irregular activity, we may contact you to verify the accuracy of the information provided or the legitimacy of any account activity.

This may delay processing of tax returns and other forms.

Additional security measures

Depending on the circumstances, we may apply additional security measures within our systems.

If we apply these measures:

- you may not be able to use our online channels or myGov
- pre-fill data may not be available
- we may prevent business activity statements from issuing automatically. You will need to contact us before each lodgment so we can generate these statements.
- we may need to make extra checks for tax returns and other forms that could delay processing.

Appointment of a data breach manager

In some cases, we may assign a data breach manager who will assist you in the management of data breaches within your business. They can provide support to reduce the impact on your business and your client.

Inappropriate access to myID

myID uses encryption and cryptographic technology, and the security features in your device (such as face or fingerprint recognition) to protect your identity.

If you're aware or suspect someone has inappropriately accessed your personal information in your myID, you need to report this immediately by contacting the myID support line.

For more information and tips about staying safe online, see Protecting your Digital ID.

To help protect your business from a data breach, we recommend you review our top cyber security tips for business.

QC 54172

Data breach guidance for tax professionals

If a data breach occurs, we may put safeguards in place to protect information that belongs to you and your clients.

Last updated 23 March 2026

How data breaches can happen

A data breach occurs when confidential taxpayer information has been accessed by an unauthorised third party.

Tax professionals hold a large amount of client, staff and business information, which makes them a growing target for identity thieves.

Tax professionals who experience a data breach may discover their clients' identities have been stolen and refund fraud has been committed in the clients' names.

Examples of data breaches include, but are not limited to:

- unauthorised removal of computers, data or records, in both paper and digital formats
- people with legitimate access to the data using it for fraudulent activities

- accessing taxpayer files using a fraudulently obtained credential, such as myID
- criminals exploiting vulnerabilities in your IT security controls, or hacking or phishing for information
- accidental disclosure of information, for example, records emailed to an unauthorised third party or hard copies left in a public place
- payroll information for your employees being unlawfully accessed
- unauthorised access to cloud-based services you use to store information.

How to prepare for a data breach

It is crucial for tax professionals to have a data breach response plan in place. The plan should step out the roles and responsibilities that need to be actioned in the event of a data breach.

The Office of the Australian Information Commissioner (OAIC) provides guidance on how to create a strong data breach response plan. For example, it should include:

- clear escalation procedures and reporting lines for suspected breaches
- processes that outline when and how affected individuals are notified
- a record-keeping policy to ensure breaches are documented
- strategies to identify and address any data handling weaknesses that could have contributed to the breach.

You should regularly review and test your plan to ensure it is current and addresses the requirements outlined by the OAIC.

Educating yourself and your colleagues on potential red flags of a data breach can help you quickly identify and implement your response plan. Indicators include:

- lodgments being made on client accounts that you did not action
- noticing changes to files and document that were not made by you, such as updates to your clients' details

- not being able to log in to your online accounts or noticing unusual activity, such as account verification emails being deleted
- your devices behaving differently, such as glitching or running abnormally slow.

Further information on detecting data breaches and cyber incidents is available from the Australian Cyber Security Centre.

What to do after a data breach

Tax professionals should report data breaches to us to make sure protective measures can be placed on client accounts.

If you have experienced a breach, we recommend the following actions:

- Phone our Client Identity Support Centre as soon as possible on **1800 467 033** Monday to Friday, 8:00 am – 6:00 pm AEST. We can apply measures to protect your business, staff and clients.
- Review the Office of the Australian Information Commissioner's (OAIC) information about notifiable data breaches to make sure you comply with your obligations under the *Privacy Act 1988*, including the Notifiable Data Breaches (NDB) scheme. Review the Tax Practitioners Board (TPB) information on how the NDBS can impact your TPB registration.
- Tell affected clients and staff about the data breach. We may also contact your clients or staff directly.
- Contact your software provider, especially if you suspect the breach originated in one of their service offerings.
- Consider what information was accessed during the breach and take steps to safeguard this where necessary. For example, you may need to report inappropriate access to your myID.
- Take steps to secure the information in your business by updating all security software and controls.
- Review systems access and remove access for people who no longer need it.
- Continue to follow security best practices and reinforce these practices with your staff to reduce the risk in your business.

If you or your clients are concerned about the security of other personal information and the wider impact of identity theft, we recommend you speak with IDCARE on **1800 595 160**. IDCARE provide free advice and confidential support to victims of data breaches and identity theft.

Case study 1: Stolen equipment

A tax agent reported to us that a laptop and documents were stolen from their car. The items contained confidential information, including business credentials and records for individual and business entities managed by the tax agent.

It was later confirmed that the tax agent's identity had been stolen and used to lodge fraudulent PAYG summaries on their clients' accounts.

We applied protective measures to the client, entity and employee accounts relating to the affected tax agent's business.

Reports of stolen equipment and data used for business occur regularly. There are a number of ways in which the data you hold on behalf of your clients, employees and business can be stolen, such as:

- dumpster diving
- letterbox theft
- paper or electronic files left unattended
- cards stolen from wallets
- stolen briefcases or laptops.

To keep your client and business information safe:

- do not leave your information unattended
- make sure you keep your electronic devices secure
- make sure client and staff data is securely stored at the end of each day
- apply multi-factor authentication to all devices used for your business.

Case study 2: Ransomware

A tax agent reported an incident in which they received an authentic looking email from a large Australian business requesting information. The agent clicked a link in the email, which released a 'crypto virus' that locked their computer systems. Fortunately, their IT specialist was able to recover their systems, but the security of their data was put at risk.

The tax agent has since:

- added additional measures to protect their systems and data holdings from future attacks
- provided training to all staff on how to check for spoofing in emails.

We asked the agent to provide the names of potentially compromised clients and applied protective measures to their accounts, including entity and employee accounts.

There are many variations of ransomware that can affect business systems and data in different ways. At the time of ransomware attacks it’s impossible to know precisely what a virus will do.

Some ransomware spreads into computer systems and silently steals information. Other ransomware is used to extort money from businesses by locking their computer files using an unbreakable code that only the criminal knows. If you pay the ransom money, the fraudsters may unlock your systems and release the data, but you could be targeted again.

Staff education is critical. If you receive a suspected phishing scam email, **do not**:

- click on any links
- open any attachments
- download any files
- install any applications.

Make sure your data is secure by backing it up regularly. Consider using off-site data storage options to effectively back-up your data.

How we protect clients affected by a data breach

We protect the privacy of client records by our proof of record ownership processes. If a data breach occurs within your practice, we may implement a range of additional safeguards.

Understanding what treatments we may apply to protect your clients will help you support them.

Treatment options can include one or more of the following, depending on the severity of the breach and any resulting fraud attempts:

- Additional proof of identity
- Additional monitoring processes
- Additional security measures
- Appointment of a data breach manager

Additional proof of identity

We may issue an alert to our staff requiring them to seek additional proof of record ownership from your client.

The requirement will apply when your client interacts with us. The alert prompts our staff to ask additional questions when validating your client's identity. This alert does not:

- prevent you from dealing with us on behalf of your client
- change how we will identify you.

Asking questions only the genuine client will know assures us we are dealing with the actual client, and not an unauthorised third party.

Your client may also choose to have a secret password created on their ATO record. Secret passwords validate a client's identity when they deal with us. The client can create their secret password with our staff over the phone.

If we are unable to establish proof of identity, we may request your client complete a tax file number enquiry form on the Australia Post website.

Additional monitoring process

We will continue to monitor your client's ATO records. If we identify any irregular activity, we may contact you or your client to make sure the activity is legitimate. This may delay processing of tax returns and other forms.

Additional security measures

Depending on your client's circumstances, we may also apply additional security measures within our systems.

If we apply these measures:

- your client may not be able to use our online services or myGov
- pre-fill data may not be available
- we may prevent business activity statements from issuing automatically. You or your client will need to contact us before each lodgment so we can generate these statements.
- we may need to make extra checks for tax returns and other forms that could delay processing.

Appointment of a data breach manager

In some cases, we may assign a data breach manager who will assist you in the management of data breaches within your practice. They can provide support to reduce the impact on your practice and clients.

Inappropriate access to myID

myID uses encryption and cryptographic technology and the security features in your device, such as fingerprint or face, to protect your identity.

If you are aware or suspect someone has inappropriately accessed your personal information in myID, you need to report this immediately.

Contact the myID support line on **1300 287 539** (select option **2**) between 8:00 am and 6:00 pm AEST, Monday to Friday.

International callers can contact us by phoning our switchboard on **+61 2 6216 1111** between 8:00 am to 5:00 pm AEST, Monday to Friday, and request your call be transferred to the myID support line.

For more information and tips about staying safe online, see myID security.

To help protect your business from a data breach, make sure you:

- undertake proof-of-identity checks
- review our top cyber security tips for business.

QC 54173

Our commitment to you

We are committed to providing you with accurate, consistent and clear information to help you understand your rights and entitlements and meet your obligations.

If you follow our information and it turns out to be incorrect, or it is misleading and you make a mistake as a result, we will take that into account when determining what action, if any, we should take.

Some of the information on this website applies to a specific financial year. This is clearly marked. Make sure you have the information for the right year before making decisions based on that information.

If you feel that our information does not fully cover your circumstances, or you are unsure how it applies to you, contact us or seek professional advice.

Copyright notice