

Potentially Impacted Personal Information

The information involved varies between individuals and may potentially include personal information collected during onboarding, employment and contractor engagement processes. Depending on the individual, this may include contact information, Tax File Numbers, identity documents (e.g. passport and driver licence), financial information, health information and other personal information (e.g. superannuation and visa information) provided to Tripod Farmers.

Steps can you take to protect your information

General Guidance

If you have concerns about the incident (or your information more generally), below are some precautionary steps you can take to protect your information against potential misuse.

- Be aware of email, telephone and text-based scams. Do not share your personal information with anyone unless you are confident about who you are sharing it with.
- Remain alert for any phishing scams that may come to you by phone, post or email.
- When on a webpage asking for your login credentials, take note of the web address or URL ('Uniform Resource Locator'). The URL is located in the address bar of your web browser and typically starts with https://.
- If you are suspicious of the URL, do not provide your login details. Contact the entity through the usual channels to ensure you are logging into the correct web page.
- Enable multi-factor authentication for your online accounts where possible, including your email, banking, and social media accounts.
- Ensure you have up-to-date anti-virus software installed on any device you use to access your online accounts.
- Check the strength of your passwords and whether they have been involved in any data breaches on the NSW Government password checker website (this tool can be used by all Australians and is not restricted to those living in New South Wales):
<https://www.nsw.gov.au/id-support-nsw/passwords>.
- Visit Scamwatch for guidance for protecting yourself from scams:
<https://www.scamwatch.gov.au/get-help/protect-yourself-from-scams/>.
- Visit the OAIC's tips for further guidance about protecting your identity:
<https://www.oaic.gov.au/privacy/your-privacy-rights/tips-to-protect-your-privacy/>.

Specific Guidance

Tax File Number (TFN)

A copy of your TFN information may have been contained within the impacted data. You may wish to contact the ATO to set up monitoring and apply protective measures to help prevent future misuse of your TFN. You can contact them on **1800 467 033** (available 8:00 am to 6:00 pm AEST, Monday to Friday). More information is available on the ATO website:

<https://www.ato.gov.au/online-services/scams-cyber-safety-and-identity-protection/help-with-data-breaches/data-breach-guidance-for-individuals>.

Australian passport information

A copy of your passport may have been contained within the impacted data. Any unauthorised access to your passport does not affect the document's validity and you are still able to use it for travel and as a valid form of proof of identity.

However, a copy of your passport may provide credentials that can be used to conduct fraudulent transactions when combined with other forms of identification. As a rule of thumb, the more ID documents available, the easier it is to construct a fake profile for fraudulent purposes.

Where a passport may have been accessed by an unauthorised third party, you may wish to consider replacing your passport by contacting the issuing authority. Before replacing your passport, we recommend that you refer to the data-breach frequently asked questions (FAQs) on the Australian Passport Office website <https://www.passports.gov.au/data-breaches>.

Also please carefully consider the impact of replacing your passport if you are thinking of doing so. Replacing a passport may prevent you from using it as a valid form of ID, obtaining credit for legitimate purposes or affect your travel plans in the short term while a new passport is being issued. Please consider this advice and your own circumstances before deciding to replace your passport. If your passport has expired more than two years ago, or has been replaced since it was provided to us, you do not need to replace your passport again.

Australian driver licence

A copy of a driver licence may have been contained within the impacted data. Any unauthorised access to a driver licence does not affect its validity and it can still be used for its intended purpose, and as a valid form of proof of identity.

Where a driver licence has been accessed by an unauthorised third party, you may wish to consider replacing it through contacting the issuing authority. While the driver licence number will remain the same, receiving a new card will provide a new card number and expiry date to prevent it from being misused. Please consider this advice and your own circumstances before deciding to replace your ID. If your licence expired or has been replaced since it was provided to us, you do not need to replace your licence.

Bank account details (account name, account number, BSB number)

Some of your bank account details may have been contained within the impacted data.

We confirm that a BSB and account number alone do not present a direct misuse risk as they do not allow unauthorised access to your bank account. However, the BSB does identify who the financial institution is, which may make impersonation scam attempts appear more legitimate.

Should you have any concerns, you can do the following:

- review your transaction history and bank account statements for any suspicious activity;
- contact your bank to report this event and flag any suspicious activity identified;
- where available use two-step authentication – such as SMS codes to your mobile phone;
- check your credit report yearly (this alerts you to any attempts to open a credit account in your name). Information about obtaining a credit report is provided below; and
- never respond to, open or click on links in emails purporting to be from your bank (it is always safer to call).

Other identity information (e.g. birth certificate, citizenship certificate and marriage certificate)

Some of your other types of identity information (e.g. birth certificate, citizenship certificate and marriage certificate) may have been contained within the impacted data.

Unauthorised access to this information does not affect its validity and it can still be used for its intended purpose, and as a valid form of proof of identity.

For birth certificates, you may, be able to request an alert and block be placed on the certificate from being verified through the online Australian Government Document Verification Service. We therefore recommend that you contact the issuing authority to let them know that a copy of your birth certificate may have been accessed by an unauthorised third party, and request that they place an alert or restriction on the file.

For other types of identification information, replacing the certificate may not reduce the risk of misuse as it will be reissued with the same registration number. We recommend monitoring your credit record, as these types of information may provide credentials that can be used to conduct fraudulent transactions when combined with other forms of identification. As a rule of thumb, the more identification documents available, the easier it is to construct a fake profile for fraudulent purposes.

Health information

Some of your health information may have been contained within the impacted data.

For context, we note that cyber-criminals typically seek to misuse information that can be easily manipulated for financial gain (such as credit cards and identity documents for identity theft). For this reason, health information by itself is generally not useful to a cyber-criminal.

We know that it will be concerning to learn that your health information may have been accessed in this manner. Should you experience any anxiety or distress in relation to this, please seek medical advice from your regular treating physician or GP. If you would like more information about the health information related to you that may have been involved, please contact us.

Other personal information (e.g. superannuation membership ID, visa information)

Some of your other types of personal information may have been contained within the impacted data (e.g. superannuation membership ID and visa information).

A superannuation membership ID by itself cannot be used to allow unauthorised access to your superannuation account. However, you may wish to take the following actions:

- Regularly check your transaction statements;
- contact your super fund to report this incident and request to have tighter security on your account, where available use two-step authentication; and
- never respond to, open or click on links in emails purporting to be from your superannuation company (it is always safer to call).

Any unauthorised access to your Australian visa number or document does not affect the validity of your Australian visa, and it can still be used for the purposes of employment, travel or other activity that is in line with your Australian visa conditions.

However, a copy of your visa document may provide credentials that can be used to conduct fraudulent transactions when combined with other forms of identification. For any changes to an Australian Visa Document or application, information is provided on the Department of Home Affairs website at: <https://immi.homeaffairs.gov.au/change-in-situation>.

Credit report

You can apply for an annual free credit report from one of the consumer credit reporting agencies below.

You can also consider contacting the below credit reporting bodies to place a temporary ban on your credit report. This means that they will not be able to share your credit report with credit providers without your consent for 21 days (unless extended).

- Equifax: <https://www.equifax.com.au/personal/products/equifax-credit-report>
- Experian: <http://www.experian.com.au/consumer-reports>

Who can I contact for more information about cyber security?

Additional general resources on identity and cyber security support can be found here:

- <https://www.oaic.gov.au/privacy/data-breaches/data-breach-support-and-resources/>
- <https://www.idcare.org/>
- <https://www.cyber.gov.au/protect-yourself>
- <https://www.cyber.gov.au/report-and-recover/have-you-been-hacked>

If you have any other questions, please contact our team at enquiries@tripodfarmers.com.au.