NOTICE REGARDING FRONTIER SOFTWARE DATA BREACH

23 September 2022

Bedford uses Frontier Software ("**Frontier**") to support its payroll function. In December 2021 Frontier advised Bedford that some of our old payroll data stored by Frontier was subject to a cyber-attack on their systems. We advised those affected at the time. Recently, in June 2022, Frontier told us that other files were also part of the cyber-attack. Both these files contained personal information.

Between November 2021 and now, a large amount of work has been undertaken together with Frontier's external cyber advisors to determine precisely whose and what information was impacted. Based on Frontier's review, they have confirmed that the stolen data **was not** published on the dark web. Frontier has also taken preventative measures to protect against misuse of this information. We are hopeful that these matters reduce the risk associated with this data breach. We have sent notices to all affected persons regarding these exposures to their last recorded postal address in Bedford's payroll system.

What personal information was stolen?

Frontier's investigations have shown that for a majority of affected persons, their stolen personal information contains identifying information such as:

- First name
- Last name
- Date of birth
- Tax File Number ("**TFN**")
- BSB and bank account number
- Superannuation details (such as membership or account number and fund name)

Has Bedford's systems been compromised?

No. Bedford's systems has not been compromised. Frontier is an external service provider and their systems were compromised.

Why does Frontier Software have personal employee information?

Frontier has been providing payroll software services to Bedford since 1994, including assisting with the combination of Bedford Group Inc and Phoenix Society Inc's payroll systems in 2016. As part of this, they had access to payroll data from that time. Frontier is required to comply with a range of contractual requirements. Frontier must also comply with the *Privacy Act 1988* which governs how organisations manage and handle personal information.

What action has Frontier taken to minimise impact to the release of personal information?

Frontier has reported the incident to the Office of the Australian Information Commissioner, the Australian Cyber Security Centre, and the Australian Federal Police and relevant state police.

1. About TFN

Where a person's tax file number (**TFN**) was part of the stolen data, Frontier is advising the Australian Tax Office (**ATO**) so they can apply additional security measures and monitor for any potential misuse of that TFN. These security measures may impact access to myGov accounts. If you are affected and need further information or assistance, you can contact the ATO Client Identity Support Centre on 1800 467 033 Monday to Friday 8:00 am–6:00 pm (Sydney time).

More information about the security safeguards that may need to be applied to accounts is available at https://www.ato.gov.au/general/online-services/identity-security-and-scams/help-for-identity-theft/data-breach-guidance-for-individuals/. If you need assistance in accessing this weblink, please contact the ATO Client Identity Support Centre.

2. Services Australia

Frontier has notified Services Australia about the incident. Services Australia has added additional security measures to protect personal information where relevant. This includes Centrelink.

We strongly recommend taking these precautionary actions:

Support is available from IDCARE

Frontier has arranged for those affected to receive free support from IDCARE, Australia's national identity and cybersecurity community support service. IDCARE is also highly experienced in supporting high-risk and vulnerable people (such as victims of domestic violence).

If you were notified, or believe you may be affected, you can access IDCARE's services by contacting IDCARE Case Manager via IDCARE's Get Help Web Form at https://www.idcare.org/contact/get-help or by calling 1800 595 160. When accessing IDCARE's services please provide the referral code 'FDI2-ID'.

You can also visit IDCARE's Learning Centre for further general information and resources on protecting your personal information at https://www.idcare.org/learning-centre.

Be alert of scam activity

Always be alert to any increased scam activity, especially email and SMS or telephone phishing scams. These fraudulent communications are often disguised to look like they come from an organisation you trust. In particular, be alert to any such scam activity that says it is coming from Frontier, Bedford or a government agency. Always check with someone you trust if you're not sure.

Never give out your personal details until you have checked with someone you trust that it is safe to do so.

Change your online account passwords regularly and consider setting multi-factor authentication

We suggest you change your online account passwords regularly and consider setting multi-factor authentication for your online accounts. Multi-factor authentication is where you provide information in two or more steps to prove who you are when you log in to a system, for example the system sends a code by text message that you then have to enter. You can ask someone you trust to help you set this up.

Keep a close eye on bank and superannuation accounts

We suggest you change your online banking account and superannuation account passwords regularly. You should also monitor your accounts for unauthorised transactions and unusual activity. If you identify anything of concern, contact your bank or superannuation fund as soon as possible.

Your bank or superannuation fund can provide advice on the actions that will be taken to identify and investigate unauthorised transactions and unusual activity.

More information on how to protect yourself online

Further information on online safety, cyber security and helpful tips to protect yourself and respond to scams, identity theft and other online risks, can be found at the following government agency websites:

https://www.cyber.gov.au/acsc/view-all-content/threats

https://www.scamwatch.gov.au/

Report any anomalies or suspicious activity

If you observe any anomalies or suspicious activity with any of your accounts, you should report it to:

- The relevant institution (for example, your bank or your superannuation fund)
- https://www.scamwatch.gov.au/
- https://www.cyber.gov.au/acsc/individuals-and-families
- Services Australia

If I want to know more who do I speak to?

Should you require more information please email us at FrontierDataBreach@bedfordgroup.com.au.

You can contact Frontier directly by email at cyber@frontiersoftware.com.au or by calling 1300 007 446.