NORTHERN LAND COUNCIL

FRONTIER SOFTWARE EMPLOYEE DATA BREACH

Our Land, Our Sea, Our Life

On the 14th December 2021 the Northern Land Council received advice from our payroll provider, Frontier Software that NLC Employee data had been stolen. This data was stolen from Frontier Software systems and not NLC systems.

On analysis we have determined employees who were employed on the 30/6/2019 are affected (209 current employees and 479 past employees). If employees commenced after this date their data was not stolen.

The employee data that was stolen includes:

- First name, last name, middle name initial
- Date of Birth
- Tax file number
- Suburb of home address as at 30/6/2019. No street names, numbers or phone numbers
- Payroll ID number, Name of employer (Northern Land Council) and NLC ABN

Actions

The Northern Land Council has taken the following steps:

1. Notified the Office of the Australian Information Commissioner of the data breach.
2. Notified the Australian Taxation Office, who will be adding additional security measures to all affected tax file numbers. These measures aim to detect fraudulent activity. There is nothing further employees need to with the ATO, however if employees have concerns they can contact the ATO's specialist service on 1800467033.
3. Notified Australian Super, Services Australia and the NLC salary packaging provider CBB.
4. Strengthened ID verification from all employees for validating changes to employees' personal details including bank account, address, email, phone numbers and deductions.

The NLC is sending written correspondence to all employees who have been impacted and it is anticipated that this will be sent via email/home address by COB 16/12/2021.

What do you need to do?

It is recommend all employees consider undertaking the following steps:

- Protect accounts with multi-factor authentication
- Change passwords
- Keep a close eye on bank accounts
- Be alert to any emails, text messages or unsolicited calls from people requesting person or account information including access to devices. Do not respond to any requests until you are certain they are legitimate. Scammers often impersonate government and businesses. Never respond to requests to provide personal and account information, or access to your device. Make sure you disconnect and make your own enquiries. Consider subscribing to www.scamwatch.gov.au for the latest information about scams impacting our community.
- Review your payroll details including salary deductions, allowances etc. via the HR21 portal
- Consider updating personal antivirus software

If you observe any suspicious activity report it to the relevant organisation and:

- Scamwatch – www.scamwatch.gov.au
- Australian Cyber Security Centre - www.cyber.gov.au/acsc/individuals-and-families

The NLC is continuing to work closely with Frontier Software who have implemented an elevated level of security monitoring and response which allows for real-time monitoring and an ability to react to any evidence of concern on a 24/7 basis.

Further Information

IDCARE

The NLC has engaged a specialist service IDCARE for all impacted employees. IDCARE is Australia's national identity and cyber support community service and is available to you without cost. Their Case Managers can talk through specific concerns you may have and develop unique plans to address risks. IDCARE can be accessed at www.idcare.org and quoting referral code **NLC22** and completing a Get Help Form for Individuals or by calling 1800 595 160 (0730am to 430pm ACST Monday to Friday, excluding public holidays).

NLC People & Culture team

If you have further queries please send these to hr@nlc.org.au please do not contact the payroll office at this time as they are currently working on the end of year pays. 1800 645 299 (free call), (08) 8941 4104, (08) 8980 1914, (08) 8920 5140, (08) 8920 5242.

Other

- ATO's specialist service on 1800 467 033
- Staff counselling service EASA 1800 193 123
- Services Australia scam & identify theft line 1800 941 126