On 11 October 2022, we announced on our Facebook page that Rumbalara Aboriginal Co-operative (Rumbalara) had become victim to a data breach. Since this time, we have been investigating and working to understand what personal information was leaked, and how many individuals may have been affected.

As a result of our investigation, we have found that there was no evidence of data exfiltration and as such, we did not assess any individuals as having been affected. We determine the matter now concluded.

In accordance with the requirements of the Privacy Act 1988 this notice provides impacted community with:

- a description of the data breach (**what has happened**);
- the kinds of personal information that was involved in the data breach (**what personal information was involved**); and
- the steps that individuals can take in response (including details of the support we have available) (**what you can do**).

What has happened?

- On 9 October 2022 we discovered that our IT system had been hacked and ransom software added and our data had been crypto locked.
- On 13 October 2022 an external third party was requested to assist, investigate and respond to this data breach, specifically to determine the extent of the compromise, find the initial vector, find indicators of data exfiltration, and guide containment and recovery of data.
- No application usage artefacts showing data exfiltration were observed. No traces of large archive creation or deletion were observed either.
- Deep and dark web searches conducted did not identify any Rumbalara data as being for sale or available.
- Based on no evidence being found that any data left the organisation, there are no affected individuals identified.
- Rumbalara have been assisted by Victorian Aboriginal Community Controlled Health Organisation Inc. (VACCHO) with containment, rebuilding and restoring of our infrastructure following the breach.
- Software has been installed on all Rumbalara computers to monitor and alert to any suspicious activity on the network.

What personal information was involved?

For Rumbalara staff:

- personal contact details

- documents submitted for identification purposes (including licenses, birth certificates, medicare, credit cards, WWCC, etc.)

- financial details such as bank accounts

- workforce performance and disciplinary action.

For Rumbalara clients:

- personal contact details
- personal information about individuals' health.

For Rumbalara service providers:

- contact Details
- bank account details.

What you can do

We recommend being vigilant with all online communications and transactions, namely:

- Being alert for any phishing scams that may come to you by phone, post or email.

- Making sure to verify any communications you receive to ensure they are legitimate.

- Being careful when opening or responding to texts from unknown or suspicious numbers.

- Regularly updating your passwords with 'strong' passwords, not re-using passwords, and activating multi-factor authentication on any online accounts, where available.

Specific advice on the personal information involved in the data breach can be found below.

Contact information

- **Change your email account passwords.** Make sure you have strong passwords that you haven't used for other accounts. If you emailed yourselves passwords, change these as well. Enable multi-factor authentication for your email accounts if possible.
- **Take care with emails and phone calls** as you may be targeted by scammers. Do not share your personal information until you are certain about who you are sharing it with. Don't open attachments or click on links in emails or social media messages from strangers or if you're unsure that the sender is genuine.

Identify information

- **Contact the agency that issued the identity document** for advice using the contact details on the website to advise them that your information has been involved in a breach.

Health information

- **Contact your health service provider** using the contact details on their website to advise them that your information has been involved in a data breach.
- **If you experience distress**, contact your doctor, a support service or your family or friends. If your physical safety is at risk, contact the police.

Financial information

- **Change you online banking account password and your banking PIN number**. Use a strong password that you've not used for other accounts.
- **Advise your financial institution** that your information has been involved in a data breach.
- **Check your account statements**. Monitor your account transactions online or using paper account statements if you receive them. If you spot any purchases, you didn't make report these immediately to your financial institution.

Tax related information

- **Contact the Australian Taxation Office** using the contact details on ato.gov.au. they can monitor any unusual or suspicious activity with your tax file number.

Support Available

We encourage you to contact our communication and public relations team for any enquiries. Please telephone our corporate office on 5820 0000 between the hours of 9am and 5pm.