NSW Health

Frontier Software cyber security incident

Information sheet for impacted staff

This information sheet is provided to assist people affected by the cyber-attack to understand what has happened, what we have done and what response options are available.

How did the breach occur?

Frontier Software (Frontier) was the victim of a cyber-attack in which an unauthorised third party gained access to its corporate network and illegally accessed and copied data stored on that network.

Frontier investigated the incident and carried out a comprehensive review of the impacted data which identified your personal information as part of the data that was copied from their internal corporate network.

Frontier informed NSW Health that they took immediate steps to prevent any further access to the data, prevent it being published on the dark web, and to protect against it being misused either now or in the future. Ongoing monitoring confirms that no data from the breach has been uploaded to the dark web.

Why am I only being notified now?

Upon discovering the cyber-attack, Frontier Software immediately began investigating the incident. Between November 2021 and now, an extensive amount of work has been undertaken together with Frontier Software's external cyber advisors to determine precisely whose and what information was impacted. This has included undertaking a detailed manual review of the impacted data to identify all potentially impacted persons. NSW Health then needed to compare this data with its own data to obtain, where possible, up to date contact details of impacted individuals.

This has been a complex and time-consuming exercise, complicated by the volume and largely unstructured nature of the data and the need to ensure in identifying, cataloguing and matching the data. Having completed this very detailed exercise, we can confirm that you were impacted.

What personal information was accessed?

The data accessed related to payroll and includes:

- Name
- Residential address
- Telephone number
- Date or birth
- Bank account number and BSB
- Tax file number

What action has been taken?

Frontier Software has reported the incident to the Office of the Australian Information Commissioner (OAIC), the Australian Cyber Security Centre (ACSC), the Australian Federal Police (AFP) and NSW Police. The Ministry of Health has notified the NSW Privacy Commissioner.

Where a tax file number (TFN) has been accessed, Frontier Software informed the Australian Tax Office so they can apply additional security measures and monitor for any potential misuse of that TFN. Please be aware that these measures may impact access to your myGov account, but this is all with a view to providing additional protection. For further information contact the ATO Client Identity Support Centre on 1800 467 033 Monday to Friday 8:00 am–6:00 pm AEST. Additional information about the security safeguards that may need to be applied to your account is available on the ATO website.

Frontier Software has also alerted Services Australia to the incident. Where impacted information includes information for which Services Australia is responsible, Services Australia has added additional security measures to protect those details where relevant.

What can you do?

If you are concerned about the potential misuse of your personal information, Frontier Software has arranged free support from IDCARE, Australia's national identity and cybersecurity community support service.

To access this support, complete IDCARE's Get Help Web Form or call 1800 595 160 and provide the referral code 'FDI2-ID'.

You can also visit IDCARE's Learning Centre for further information and resources on protecting your personal information.

Please remain alert to any increased scam activity, especially email and SMS or telephone phishing scams (i.e., fraudulent communications disguised as if to look like they come from an organisation you trust) and, in particular any scam activity purporting to come from Frontier Software or the Ministry of Health or another NSW Health organisation. 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:

- Australian Cyber Security Centre
- Scamwatch

NSW Health recommends changing your online account passwords and setting multi-factor authentication for you online accounts if you have not done so already. You can do this by calling the Statewide Service Desk on 1300 28 55 33.

If you are feeling distressed by this information, your employee assistance program is confidential, free, and available 24/7 to you and your immediate family. Find out more on your local intranet page.