Data breach impacts 80,000 South Australian govt employees

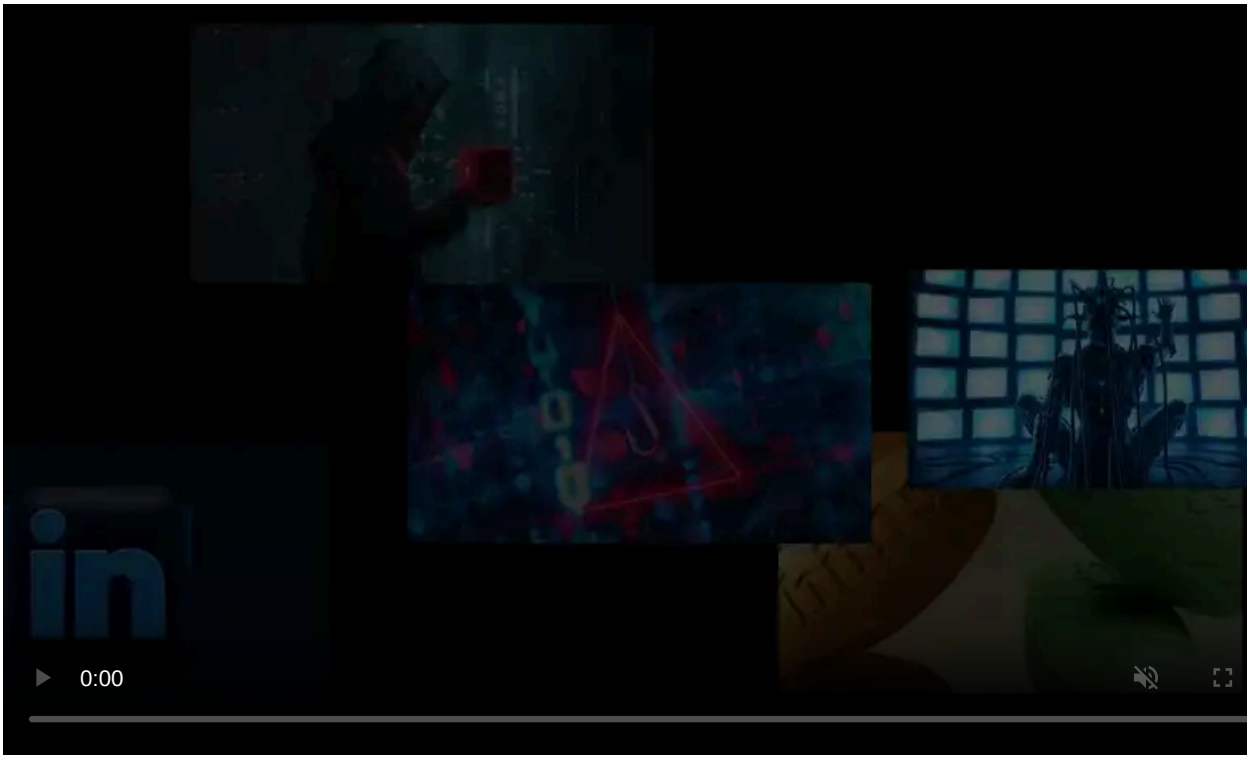
By Bill Toulas

Published: 2021-12-10 · Archived: 2026-04-05 18:21:27 UTC

The South Australian government has disclosed that the sensitive personal information belonging to tens of thousands of its employees was compromised following a ransomware attack that hit the system of an external payroll software provider last month.

The number of records accessed by hackers corresponds to at least 38,000 SA government employees, but it could be as high as 80,000 according to South Australia's Treasurer Rob Lucas.

The breached company behind this data breach is Frontier Software, which suffered from a ransomware attack on November 13, 2021.


0:00

According to the company's statement on the incident, the threat didn't pivot to client systems through their products and the data exfiltration only affected a specific segmented environment.

"The ongoing forensic investigation and other response activities conducted by Frontier Software and CyberCX has now confirmed evidence of some data exfiltration from Frontier Software's internal Australian corporate environment," the company said.

"We have not identified evidence of compromise or exfiltration outside this segmented environment."

The data that has been compromised according to the South Australian government includes the following:

- First name
- Last name
- Date of birth
- Tax file number
- Home address
- Bank account details
- Employment start date
- Payroll period
- Remuneration
- Tax withheld
- Payment type (where applicable)
- Lump-sum payment type and amount (if applicable)
- Superannuation contribution
- Reportable fringe benefits tax amount (where applicable)

The only public entity that wasn't affected by the incident is the Department for Education, which does not use Frontier products.

"The highest of the high to the lowest of the low and all of the rest of us in between are potentially impacted, with the exception of teachers and the Department for Education," Lucas told ABC News after disclosing the data breach.

"Having the bank account details doesn't give you access to the bank account, but it's the first step in trying to crack a code in terms of passwords.

"We expect the state government to take all possible steps to review its cyber security measures in order to prevent such an event in the future."

Government employees affected by this incident are advised to treat incoming emails, calls, and SMS with caution. Additionally, everyone should reset their passwords and activate two-factor authentication where possible.

Affected individuals should closely monitor bank statements and account activity and report any suspicious transactions to the authorities. Exposed people can take advantage of a free IDCARE cyber-security support service offering, following the instructions laid out on the incident announcement on the SA government website.

Conti ransomware behind the breach

Bleeping Computer has seen an announcement on Conti ransomware's data leak portal dated November 16, 2021, which matches the attack details shared by Frontier Software in their statement.

However, the listing has since been removed from the portal, which probably means the negotiations have ended.

Frontier listing on the Conti portal

Conti, a long-lived Ransomware as a Service (RaaS) operation, still manages to evade prosecution even after high-profile incidents against vital national resources such as Ireland's Department of Health.

The gang is believed to be behind the recent revival of the notorious Emotet botnet, which could lead to a massive new wave of ransomware infections.

This week, Conti took responsibility for the attack against Nordic Choice Hotels, a Scandinavian hotel chain with 200 properties.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
