

Ombudsman finds more can be done to protect Australians from myGov fraud

Today the Commonwealth Ombudsman released the investigation report, **‘Keeping myGov secure – An investigation into Services Australia’s response to myGov fraud arising from unauthorised linking to member service accounts.’**

Commonwealth Ombudsman, Iain Anderson said:

“myGov fraud causes affected Australians stress, anxiety and frustration. Following complaints to my Office, and media reports about incidents of tax fraud linked to myGov. I commenced an investigation based on concerns previously raised with Services Australia that there were not adequate security controls in place to protect people from the impact of myGov fraud.”

“Unauthorised linking” is where a genuine myGov customer’s member service account is linked without their knowledge to a ‘fake’ myGov account created by a fraudster. The investigation found that preventative security controls for unauthorised linking are limited to the proof of record ownership processes that are implemented by the individual myGov member service agencies. These processes vary across those individual agencies.

There are no additional security controls in place to ensure high-risk transactions such as changing bank account details are authorised by genuine customers, presenting a shared risk to all myGov participants.

Mr Anderson noted, “APS agencies responsible for administering a system or program that involves other agencies, like myGov, should understand the levels of risk across the system and ensure risks that could impact other participants are managed effectively, including through identifying and managing shared risks.”

The Ombudsman made four recommendations and two suggestions to Services Australia aimed at improving:

- the security controls for unauthorised linking and high-risk transactions
- how Services Australia and individual member services manage shared risks within the myGov ecosystem
- Services Australia's approach to responding to customer reports of fraud and breaches to individual records across its three member services.

Reflecting on the importance of APS agencies putting people at the centre of public administration, Mr Anderson said:

“People have told us about the stress and anxiety they experienced when their personal information was stolen, and fraud committed in their name. In these circumstances, it is particularly important that Services Australia provide accessible, consistent and clear information to help people.”

Services Australia accepted the Ombudsman's recommendations and suggestions. The response and planned actions to implement the Ombudsman's recommendations are at Appendix A to the report.

Mr Anderson said, “Given the volume and sensitivity of information held in member service accounts linked to myGov, robust protections to stop fraudsters gaining unauthorised access to myGov accounts are essential.”

The Office will monitor the implementation actions in accordance with its usual monitoring practices.

The full report is available via our website here: <https://bit.ly/4fuVfcL>

For more information visit ombudsman.gov.au or for media enquiries please email media@ombudsman.gov.au.