COMMONWEALTH OMBUDSMAN

Keeping myGov secure

An investigation into Services Australia's response to myGov fraud arising from unauthorised linking to member service accounts

6 August 2024

Highlights

Why did we investigate?

In 2022, media reported escalating incidents of tax fraud committed by unauthorised third parties linking genuine taxpayer records to ‘fake’ myGov accounts. The Office also received and investigated complaints involving unauthorised linking in Centrelink and Medicare accounts.

Unauthorised linking is where a genuine myGov customer's member service account is linked to a 'fake' myGov account without the customer's knowledge or authorisation.

We wanted to look at what Services Australia, as the myGov administrator, is doing to strengthen security for unauthorised linking. We also wanted to understand why there was an apparent lack of co-ordination across Centrelink and Medicare when helping people impacted by identity theft and my Gov fraud, including unauthorised linking.

What we found

- myGov’s current security controls do not adequately protect people from unauthorised linking where identity theft has occurred.
- The preventative control for unauthorised linking is each individual member service’s ‘proof of record ownership’ (PORO) processes.
- Variability in the standard of proof required to satisfy PORO processes across member services presents shared risk for myGov participants.
- There are no additional security checks to ensure high risk transactions are authorised by the genuine customer.
- An apparent lack of formal processes for managing shared risks across the myGov ecosystem.
- Services Australia’s ability to provide a co-ordinated response to customers reporting data breaches and fraud may be limited by its enabling legislation.

What did we recommend?

We made 4 recommendations and 2 suggestions, aimed to improve:

 Security controls for unauthorised linking and high risk transactions	 Management of shared risks across the myGov ecosystem	 Services Australia's approach to responding to individual reports of fraud and breaches to individual records

Lessons for all agencies

Agencies who administer a system or program involving multiple agencies, such as myGov, should ensure they have a holistic view of associated risks to identify opportunities to improve the system and support other participating agencies to uplift their capability.

These agencies should also understand the levels of risk involved in the system and ensure risks that could impact other participants are managed effectively, including through identifying and managing shared risks.

Recommendations and suggestions

R1. Consistent with its responsibilities for driving improvement in fraud control practices, we **recommend** Services Australia:

a. assess existing PORO processes across the myGov ecosystem to identify and document shared risks and work with member services to agree and implement appropriate controls
b. consider establishing baseline PORO requirements which must be met by all member services.

R2a. We **recommend** Services Australia implement additional security controls such as two factor authentication across its three member services for all high risk transactions, including linking a member service account to myGov and updating contact and bank account details.

R2b. Services Australia should ensure that a high standard of security settings for high risk transactions applies consistently across all available service delivery channels for its member services.

R3. We **recommend** Services Australia establish formal processes for managing all shared risks across the myGov ecosystem, including identifying, assessing and documenting shared risks, periodically assessing the effectiveness of agreed controls, and responding to indications that risk assessments should be updated.

R4. We **recommend** Services Australia seek external legal advice about options to facilitate a greater level of information sharing across linked member services and support member services to act proactively to reduce fraud risk or other unlawful activity while meeting their other legislative obligations.

S1. We **suggest** Services Australia share learnings and information about its authentication and PORO processes with other myGov member services to support them to build their capability.

S2. We **suggest** Services Australia regularly reviews and updates its communications regarding potential myGov and member service account breaches, including security notifications, staff guidance and online content, to ensure people are supported to take real time action to mitigate breaches to their myGov and or linked member service accounts.

Understanding myGov

Launched in 2013, *'myGov is the Australian government's front door for digital services and supports individuals to access services of participating government agencies.'*[1]

MyGov operates on a 'hub and spoke model',[2] in which myGov serves as the hub, or central entry point, from which users access their linked online accounts (the spokes) with entities such as Centrelink, Medicare or the Australian Taxation Office (ATO).

The 17 entities using the myGov platform to connect their customers to their online services are referred to as 'member services'. While users can access their linked member service accounts via myGov with a single sign in credential, a myGov account holds very little personal information about the person who created it. Almost all personal information, along with transaction data, is held in the relevant member service's records.

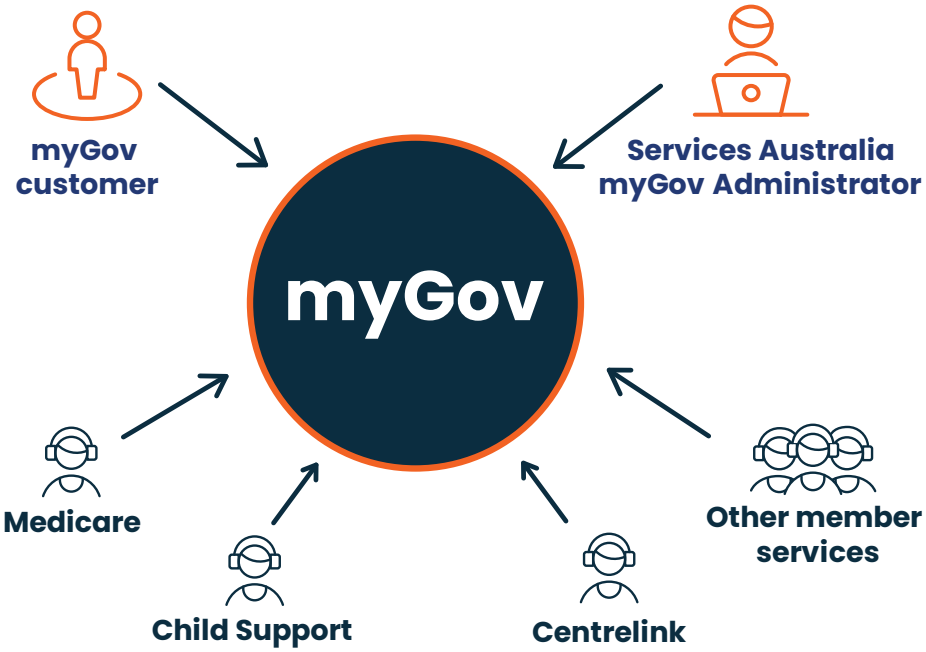

Figure 1 - myGov ecosystem

[1] Critical National Infrastructure – myGov User Audit January 2023 Volume 1 Findings and recommendations page 1 of 34

[2] Critical National Infrastructure – myGov User Audit January 2023 Volume 1 Findings and recommendations page 1 of 34

The problem

In recent years, myGov has increasingly been targeted by people and organisations seeking to gain financially through cybercrime (fraudsters).

In late 2022, media reported that a large volume of confidential information, including myGov login details, was available for sale on the internet.[3] Media also reported that fraudsters were creating myGov accounts and using stolen identity information to link these to genuine ATO accounts, so they could lodge false tax returns to generate and claim refunds.[4]

Quote

''a fraudster can create one or more myGov accounts in respect of another individual simply because the fraudster has detailed information about that other individual. This serious risk needs to be addressed."

– myGov user audit January 2023[5]

Services Australia's myGov responsibilities

Services Australia has two roles in the myGov 'ecosystem'. First, it administers the myGov platform. This means it is responsible for providing the technological capability which allows people to create myGov accounts and link their member service online accounts to myGov.

[3] Cyber black market selling hacked ATO and MyGov logins shows Medibank and Optus only tip of iceberg - ABC News
[4] Fake myGov profiles are being used to hack ATO accounts. Sue found this out the hard way - ABC News
[5] In September 2022, the Minister for Government Services, the Hon Bill Shorten MP, announced an independent User Audit of myGov to consider the user experience, functions and performance of myGov to shape the future direction and its connection with government services.

Second, Services Australia directly administers the Centrelink, Child Support and Medicare programs. These 3 programs are individual myGov member services, with their customers accessing their online services through myGov.

Services Australia's member service agreement with all member service entities and the myGov Member Service Handbook set out the:

- myGov technical capability Services Australia will provide to the member service, and the
- Responsibilities of each party to the agreement, including for managing cyber security and fraud.

Why we investigated

As media reported increased myGov fraud, we also received complaints from people affected by fraudsters using stolen personal information to access their Centrelink, Medicare and ATO online accounts through myGov. People told us that fraudsters submitted false claims for Centrelink payments, advances and loans in their name, and redirected their pension payments. People also reported being unable to claim financial assistance, such as Child Care Subsidy, until Services Australia and the relevant member service investigated and corrected the fraudsters' actions.

Quote

"I have not done anything wrong but be a victim of identity theft. We do not earn a huge income."

– Caller to our Office

In August 2023, we asked Services Australia what action it was taking, as the myGov administrator, in response to reports about fraud involving myGov and ATO online accounts. In October 2023, we gave Services Australia feedback about how Centrelink and Medicare handled a complaint involving identity theft, after our investigation into that complaint found fraudsters were able to successfully navigate authentication processes to access the customer's Centrelink and Medicare records, using stolen identity information.

The Ombudsman subsequently commenced an own motion investigation because, based on Services Australia's response to our enquiries and feedback in late 2023, we were not assured adequate security controls were in place to protect people from the impact of myGov fraud.

The information also suggested a lack of a co-ordinated approach between Services Australia's 3 member services, when responding to breaches and myGov fraud reported by customers. Given the stress and anxiety people have told us they experienced after finding out their personal information had been breached and fraudulent actions taken in their name, we consider it is essential for Services Australia to provide accessible, consistent and clear information when helping people impacted by myGov fraud.

Investigation and report scope

This investigation focussed on unauthorised linking, which is the type of myGov fraud commonly reported in the media[6] and in complaints to our Office. Unauthorised linking is often tied to identity theft, which can occur through:

- targeted attacks, such as the Optus and Medibank data breaches
- phishing scams which trick people into revealing their personal details and/or passwords
- buying someone else's information through the dark web[7]
- collecting personal information from documents found in household or business refuse or stolen from mailboxes.

Our investigation had regard to the findings in the Inspector General of Taxation's (IGOT's) interim report published on 30 April 2024,[8] which considered how the ATO is addressing fraud risks as a myGov member service.

We also considered how Services Australia, as the owner of Centrelink, Child Support and Medicare, safeguards and supports customers affected by unauthorised activity in their online accounts.

---

[6] Fake myGov profiles are being used to hack ATO accounts. Sue found this out the hard way - ABC News
[7] Cyber black market selling hacked ATO and MyGov logins shows Medibank and Optus only tip of iceberg - ABC News
[8] 240430-IGTO-TaxID-fraud-investigation-Interim-report.pdf

We considered Services Australia's responsibilities as the myGov administrator, for managing security across the myGov ecosystem and helping member services improve their capability to address shared risks, including those arising from unauthorised linking.

We did not consider myGov's general operation, fraud by genuine customers or staff, broader cybercrime threats to myGov security, or the overall effectiveness of myGov fraud controls. We also did not look at the processes of myGov member services other than Centrelink, Child Support and Medicare.

This report sets out our views based on the information Services Australia provided in response to our investigation. We included detail to explain processes and support our conclusions where appropriate, but in some instances we limited this to high level information to avoid compromising existing myGov fraud prevention and detection arrangements.

What we found

Finding 1

myGov's current security controls do not adequately protect people from unauthorised linking where identity theft has occurred.

myGov security settings

Given the volume and sensitivity of information that may be held in member service accounts linked to them, it is clear that robust protections to stop fraudsters gaining unauthorised access to myGov accounts are essential.

Services Australia has established several types of security mechanisms to protect myGov accounts, including two factor authentication or digital identity sign in; forced closure of compromised myGov accounts; locking myGov accounts; and sending security notifications to alert customers to potential unauthorised access.[9]

The information Services Australia provided in response to this investigation demonstrates its ongoing work to improve myGov security. For example, since June 2024, users can choose to assign a passkey to their myGov account, an option that is generally accepted as being a stronger alternative to password based authentication systems. We found that overall, the current security measures focus on stopping fraudsters getting into genuine customer myGov accounts, but do not necessarily prevent them taking a side entrance to member service accounts through unauthorised linking.

[9] How we protect your myGov account | myGov

Unlimited myGov accounts - a weak link in linking

In response to this investigation, Services Australia explained myGov was designed with the ability to open multiple myGov accounts, to avoid becoming a central database of information with a unique government identifier issued.

In practice, a single user can create as many myGov accounts as they wish, with the only limitation being that each account must be established using an email address that has not already been used to create a myGov account.

When first created, a myGov account is a 'shell' record with no personal information attached to it. Once the first member service is linked, a myGov profile is created, using the name and date of birth recorded by the member service or a digital ID, and applying it to the 'shell' myGov account. Services Australia also advised there is nothing to stop a single member service account being linked to different myGov accounts at different times, which might be needed if a person loses access to their original myGov account.

To link a member service account to myGov, users must satisfy the member service's 'proof of record ownership' (PORO) process before the member service can give them the 'linking code' required to link a member service account to myGov. PORO requirements differ across individual member services.[10]

However, PORO generally involves a user proving their identity by providing personal information that only the record owner should know. We found this is the only security control for preventing unauthorised linking.

[10] Link services to your account | myGov

Case Study

In early 2022, a myGov customer contacted Services Australia after fraudulent online claims were lodged in their name. Services Australia identified that their Centrelink account had been linked to a myGov account operated by a third party. Services Australia closed the fraudulent myGov account and placed a secret password on their Centrelink record. Five months later, the customer received a text message stating they had submitted a Centrelink claim. The customer contacted Services Australia again, who confirmed a fraudulent claim had been submitted on their Centrelink record. They complained to the Ombudsman about how Services Australia handled the second breach.

Our investigation found that the second breach occurred because claims staff did not ask all the required security questions of the fraudster. During the phone call the fraudster was able to change the address, bank account details for the account and lodge a disaster recovery payment claim.

We found that the customer's Medicare record was also breached via a phone call a few days after the Centrelink breach. Again, the fraudster changed their address and requested a new Medicare card. The customer told us the fraudsters then used their Medicare details to access his ATO record, submit fraudulent tax returns and change the bank account details recorded on their ATO record to intercept the resulting refunds.

(continued page 21)

Ideally, PORO prevents unauthorised linking as only the true record owner should be able to provide the information required to verify they own the record. However, cases like the one above demonstrates that:

- fraudsters can circumvent this security control by using stolen identity information to meet PORO requirements
- one failed PORO process can open the door to fraudsters obtaining additional personal information which they can use to access other member service accounts.

Finding 2

Variations in the standard of proof to satisfy PORO requirements across member services present risk for all member services and for the people who use myGov to access their online accounts.

Member services are responsible for developing their own PORO requirements based on the level of fraud risk they assess applies to their program. While we did not consider the effectiveness of individual member services' PORO arrangements, we note the 2023 myGov user audit report highlighted that the standard of proof to establish PORO varies significantly across myGov's member services.[11]

Under their myGov member service agreements, member services are required to declare to Services Australia that their PORO requirements are appropriate to their assessed level of fraud risk. However, our investigation did not identify information to suggest that Services Australia has assessed individual member services' PORO processes to consider if they sufficiently address the identified fraud risk. It remains unclear to us how, as the myGov administrator, Services Australia assures itself the controls implemented by member services are adequate for identified risks across the myGov ecosystem, and ensures other myGov participants are not placed at undue risk.

It is also not clear if member services have visibility of one another's risk assessments or PORO requirements, to support them to make informed decisions about whether another member services' arrangements might pose an unacceptable risk to the security of their own services.

Based on the information provided to us during our investigation, it is unclear whether or how Services Australia and/or the broader group of entities within the myGov ecosystem have formally recognised or engaged with this risk.

[11] Critical National Infrastructure – myGov User Audit January 2023 Volume 2 Detailed analysis - page 14 of 124

Recommendation 1

Consistent with its responsibilities for driving improvement in fraud control practices,[12] we recommend Services Australia:

a. assess existing PORO processes across the myGov ecosystem to identify and document shared risks and work with member services to agree and implement appropriate controls
b. consider establishing baseline PORO requirements which must be met by all member services.

During this investigation, Services Australia shared its work to improve and strengthen the authentication and PORO processes for its own member services - Centrelink, Child Support and Medicare. We consider that other member services could benefit from Services Australia's experience and expertise in protecting personal information.

Suggestion 1

We suggest Services Australia share learnings and information about its authentication and PORO processes with other myGov member services to support them to build their capability.

[12] myGov Fraud and Corruption Control Plan – page 8 of 11

Finding 3

Services Australia and member services should do more to verify linking requests and other high risk transactions are authorised by the genuine member service record owner before the transaction is finalised.

In their April 2024 interim report, the Inspector General of Taxation found that overreliance on gateway access controls (such as PORO, myGov and myGov ID processes) to provide 24/7 protection against unauthorised changes in ATO member service accounts is inappropriate and inadequate, no one type of control is sufficient to mitigate the fraud risk by itself, and instead a variety of types of controls are needed.[13]

Case Study

A retiree receiving the Age Pension told us they spoke to Services Australia after becoming aware their superannuation account had been locked and Age Pension had not been paid. During this contact, they found out a fraudster had successfully accessed their Centrelink accounts. Their payments were stopped because of the fraudster's actions.

Our preliminary inquiries with Services Australia confirmed the fraudster had accessed their Centrelink member service accounts online and changed certain personal information to make false claims with Centrelink in their name.

Services Australia did restore the Age Pension payments and re-issued to the retiree the payments that had been diverted to the fraudster's bank account. If additional security measures had been in place to verify whether the retiree authorised the changes to their personal information, however, the disruption to their payments and accounts could have been stopped before any damage was done.

[13] 240430-IGTO-TaxID-fraud-investigation-Interim-report.pdf page ix

We consider that certain transactions present a particularly high risk of loss via fraud, including:

- Providing a linking code, which allows someone to link or re-link a member service account to a myGov account – particularly since myGov does not verify the identity of the person operating a myGov account
- Changing bank account details – because it enables redirection of payments to fraudulent accounts.
- Updating phone, email or address information - because this can prevent security notifications being delivered to genuine customers.

Once a customer is signed into their myGov account, there are currently no additional security measures for high risk transactions. Services Australia advised this is because myGov was designed to provide a single sign on to securely access government services and reduce the need for multiple online accounts and passwords.

We acknowledge Services Australia's advice that it is currently considering how to strengthen the process for changing bank account details for its member services. We also acknowledge that implementing additional security controls for high risk transactions completed online would require member services to implement controls in their respective systems.

At the same time, the Australian government actively recommends and promotes the use of multi-factor authentication by all Australians, for example through the Australian Cyber Security Centre.[14]

In our view, requiring multi-factor authentication for high risk transactions offers substantial mitigation against the risk of loss resulting from unauthorised linking and access to genuine customer accounts, by alerting customers in real time that their records may have been breached and stopping unauthorised transactions before they are finalised.

[14] Multi-factor authentication | Cyber.gov.au

Finding 4

Authentication requirements for high risk transactions should be consistent across all service delivery channels, including online, in person or by phone.

Currently, before they are permitted to change bank account details over the phone, Centrelink customers must confirm the bank account details already recorded. However, no such check is required when a user updates bank details in a Centrelink online account.

While Services Australia advised us it is considering strengthening the online process, we consider Services Australia's customers should be able to rely on a consistently high standard of security across all service delivery channels, for all its member services.

Recommendation 2

a. We recommend Services Australia implement additional security controls such as two factor authentication across its three member services for all high risk transactions, including linking a member service account to myGov and updating contact and bank account details.
b. Services Australia should ensure that a high standard of security settings for high risk transactions applies consistently across all available service delivery channels for its member services.

Finding 5

Processes for identifying, assessing and documenting shared risks across the myGov ecosystem should be formalised.

Interoperability – the risk impacts everyone

Under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), Commonwealth entities are obliged to take all reasonable measures to prevent, detect and deal with fraud.[15] Section 16 of the PGPA Act imposes a duty to establish and maintain systems and appropriate controls to oversee and manage risk. Entities must also comply with the Commonwealth Risk Management Policy (Risk Management Policy), which requires them to collaborate to manage shared risks.[16]

While it may be rare to find a single myGov account linked to most or all 17 member services, complexity in the myGov ecosystem arises as each member service linked to a myGov account:

- may hold sensitive information about the customer
- uses a different system, and
- applies different security controls for inputting or changing the information recorded.

Quote

"the growing use of collaborative approaches by government such as through shared services public-private partnerships and inter-agency task forces means that shared risk is becoming more prevalent."

Commonwealth Risk Management Policy Toolkit, Element 6: Shared Risks

[15] Section 10(a) of the Public Governance, Performance and Accountability Rule 2014.
[16] Risk Management Services | Department of Finance

It is important that Services Australia, as the administrator, and the various member services understand and engage with these complexities, including the inherent risk to the security of each member service's systems if there are gaps or weaknesses in other member services' security arrangements.

While member services are required to declare they have identified and assessed fraud risks related to their program under the member service agreement, there was nothing provided to us to suggest that member services provide details of their risk assessments to Services Australia. We suggest that it is only with the benefit of awareness of the overarching system that member services can accurately assess and address risks (including of fraud) associated with their systems' integration with the myGov platform.

In response to this investigation, Services Australia advised that it collaborates with member services in forums where fraud risk and associated controls are discussed, but did not provide any evidence of formal processes which guide conversations or resulting outcomes. While agencies often manage shared risk informally, guidance for managing shared risk under the Risk Management Policy[17] explains that managing risk with formal processes, where there are complexities, provides agencies with:

- a greater ability to identify and manage challenges, and
- better clarity and understanding of risk drivers.[18]

Recommendation 3

We recommend Services Australia establish formal processes for managing all shared risks across the myGov ecosystem, including identifying, assessing and documenting shared risks, periodically assessing the effectiveness of agreed controls, and responding to indications that risk assessments should be updated.

[17] Element 6: Shared Risks | Department of Finance
[18] Element 6: Shared Risks | Department of Finance

Finding 6

Enabling legislation may be impeding Services Australia's ability to provide a co-ordinated and consistent response to help people secure their member service accounts after a breach

myGov fraud – helping people re-secure their accounts

Case Study

(continued from page 13)

Our investigation into a complaint found that after Services Australia confirmed the myGov customer's Centrelink account was breached in August 2022, Services Australia did not check whether their other member service account (Medicare) had also been compromised. Similarly, it did not take preventative action, such as placing an alert on the Medicare record to prompt staff to be aware of any further unauthorised attempts to access their account.

We provided Services Australia formal feedback about this case and suggested it develop and implement protocols to notify other myGov member services to be alert to signs of further unauthorised activity. In our view, if Services Australia had notified Medicare that the customer's Centrelink record had been breached, Medicare could have acted to reduce the risk of breaches of his Medicare record, and in turn prevented his ATO account being misused.

It was unclear to us why Services Australia could not disclose the breach to another member service, where they were a mutual customer.

When we suggested to Services Australia that it develop processes to share information about breaches across its member services, following our investigation into the complaint, Services Australia advised that disclosing information between its member services (which are simply separate programs run by Services Australia, not separate entities) could only occur if their respective enabling legislation permits, despite the occurrence of a data breach.

We noted that section 16A of the *Privacy Act 1988* allows agencies to disclose personal information in 'general permitted situations,' which is where an agency has reason to suspect that unlawful activity is occurring that relates to its functions and the disclosure would be necessary to take appropriate action in relation to the matter.

Services Australia agreed that a data breach or fraud involving the myGov platform is a general permitted situation where it could disclose personal information.

However, Services Australia stated that section 16A cannot be used to circumvent the secrecy laws prescribed in its member services' enabling legislation.

Documents provided to us confirm member services are required to report fraud incidents involving myGov to Services Australia as the administrator. Those documents also show that Services Australia may share information with member services impacted by fraud incidents. Secrecy provisions frequently contain exceptions allowing disclosure to protect revenue. Service Australia has not advised which or how the secrecy provisions in member service enabling legislation prevent Services Australia's member services from sharing information about data breaches occurring in mutual customer records, when it could be taking proactive action to reduce the risk of fraud and its impact on customers. As noted above, Service Australia and its member services also have legislative obligations to manage shared risks and to address fraud.

Recommendation 4

We recommend Services Australia seek external legal advice about options to facilitate a greater level of information sharing across linked member services and support member services to act proactively to reduce fraud risk or other unlawful activity while meeting their other legislative obligations.

As a key principle of good public administration, government agencies administering systems involving personal and sensitive information must build and maintain the community's trust and confidence. Where multiple agencies are involved, as with myGov, it is essential that the processes for helping people when things go wrong are robust, reasonably consistent across the agencies involved, and simple to navigate, to assure people their information is protected and maintain their trust.

Quote

"myGov, despite being a Government agency that we trust with a lot of important data, has no way to complain about issues caused by its own systems and staff, is issuing erroneous information about how to deal with possible security breaches, and does not train its staff in how to manage complaints. I am appalled at this and disturbed that we are trusting our data within myGov but it seems it can't manage complaints or issues appropriately."

– Caller to our Office

In response to this investigation, Services Australia advised that people can report breaches to their myGov and/or member service accounts by contacting the myGov Helpdesk, the Scams and Identity Theft Helpdesk, or their usual contact method for its member services (Centrelink, Child Support or Medicare).[19]

Services Australia advised us that, in situations where people become aware another person may have accessed their myGov account, they can reduce the risk of associated fraud by:

- changing their myGov password
- creating a passkey attached to the account
- changing their myGov second factor sign in method, which can be a one-time code sent by text or email, the Code Generator app, Digital ID, or secret questions
- closing their myGov account
- unlinking a member service from their myGov account.

[19] This investigation focussed on Services Australia member services only. However, we understand people can also report breaches to other member services linked to a myGov account by contacting the relevant agency (for example, the Department of Veteran's Affairs or the ATO).

Case Study

A myGov customer told us they received a text message from myGov Security advising them that someone may have accessed her myGov account and to contact the myGov helpdesk.

They told us that, after waiting on hold for half an hour, staff on the myGov helpdesk advised them to log into their myGov account and, if they identified any unusual activity in their linked accounts, to contact the relevant agency. The customer said there was no point asking them to call the myGov helpdesk, as the text message could have simply given them the information they had waited half an hour on hold to obtain.

MyGov helpdesk staff can take some actions to assist customers affected by unauthorised linking, but Services Australia noted they cannot access individual member service accounts to remedy breaches. The myGov helpdesk operates extended hours including weekends, but members services helpdesks are typically only accessible during business hours. If the action required to remedy a breach cannot be taken by the myGov helpdesk, people may be unable to report a breach to their member service account for hours or even days until the member service reopens - potentially leaving the customers (and government), susceptible to further fraud in the meantime.

Given the concurrent shift towards self service via online services and the constant evolution of cybercrime, Services Australia, as the myGov administrator, and member services should empower people with tools to identify and address threats presented by identity theft and fraud through myGov in real time.

This includes providing clear information about what action people can take to secure their accounts themselves, which agency they should contact if the impacted account cannot be secured by the individual themselves and, if the system does not enable the individual to secure the account themselves, having assistance accessible outside business hours.

We are pleased to note Services Australia's response to this investigation reflects plans to implement a range of future fraud control initiatives including a focus on improving users' ability to proactively identify and respond to fraud and security incidents in their accounts.[20]

Suggestion 2

We suggest Services Australia regularly reviews and updates its communications regarding potential myGov and member service account breaches, including security notifications, staff guidance and online content, to ensure people are supported to take real time action to mitigate breaches to their myGov and or linked member service accounts.

[20] myGov Fraud and Corruption Control Plan – page 8 of 11

Australian Government
Services Australia

Your Ref: A2419430
Our Ref: EC24-002597

Acting Chief Executive Officer
Jarrod Howard

Mr Iain Anderson
Commonwealth Ombudsman
Level 5, 14 Childers Street
CANBERRA ACT 2601
Via email: [redacted]

Dear Mr Anderson

Draft Report on Own Motion investigation – *myGov identity theft and fraud*

I refer to your letter of 11 July 2024 enclosing your draft report, *Keeping myGov secure - An investigation into Services Australia's response to myGov fraud arising from unauthorised linking to member service accounts*.

Thank you for the diligent and comprehensive approach taken to investigating Services Australia's (the Agency's) enhanced security measures implemented due to increasing scams, identity theft and other cyber security threats. We appreciate the opportunity to review your report prior to publication.

In your report you make 4 recommendations and I confirm that the Agency accepts all recommendations and will take action to implement them.

The Agency's response with proposed actions is set out in Attachment A to this letter.

If you wish to discuss this or any aspect of the Agency's response, please contact Chris Birrer, Deputy Chief Executive Officer Payments and Integrity, [redacted]

Yours sincerely

[redacted]

Jarrod Howard
26 July 2024

Services Australia is committed to protecting people from identity theft and scammers. We welcome the Ombudsman's investigation. The investigation provides us with helpful recommendations for how we can further strengthen the security of the myGov platform, the role of member services to uplift security and provides us with certainty that we are on the right path with a number of measures we already have underway.

Services Australia operates myGov within an increasingly sophisticated cyber threat environment. Services Australia identifies and responds to more than 300 scams per week impersonating myGov. This reflects coordinated fraud activity operating in an opportunistic and systematic way to identify and exploit perceived vulnerability in government online services, such as myGov. There are a range of external factors that contribute to overall systematic fraud risks of digital services including:

- the cyber threat landscape has deteriorated substantially since myGov was first designed and implemented in 2013
- geopolitical events overlaid by the prevalence of sophisticated, organised, financially motivated criminal groups have caused a rapid rise in the number of data breaches, scams, and the amount of fraud committed utilising the internet, and
- financially motivated crime targeting internet-based services is widespread and is undertaken against all industry groups. The prevalence of citizen data and online platform credentials available for purchase on the dark web means malicious actors have access to a range of personal information to assist in undertaking fraud.

Services Australia is committed to ensuring we identify issues, threats and risks quickly and deliver effective measures to protect myGov and our customers.

myGov is among the first government services to introduce passkeys as a sign in option. Passkeys offer strong protection against phishing and are used by international services such as Apple, PayPal, Google and Microsoft. Using a passkey and turning off signing in with a password makes it harder for scammers to access myGov accounts using stolen usernames and passwords. Services Australia urges all customers to set up passkeys and protect their personal information.

myGov supports secret questions as a sign in method to ensure people who do not have or own a mobile phone can access digital government services. We understand some customers may share a device, use a computer in a library or use our self-service terminals in our national network of service centres, agents and access points. This is particularly important for financially vulnerable customers.

In addition to dedicated measures, we have implemented and will continue to implement to strengthen the myGov platform for the benefit of customers and all member services. We will continue to work with member services to better enable us to deliver more connected government services. This includes seeking opportunities to share information across linked member services, which would improve customer outcomes across all channels and reduce the risk of fraud.

We accept the four recommendations and two suggestions put forward by the Ombudsman. We plan to implement these in collaboration with myGov member services to ensure myGov remains trusted, safe and secure.

Following is a table setting Services Australia's responses to the Commonwealth Ombudsman's report, Keeping myGov Secure.

Recommendation	**Entity response to recommendations/suggestions**	**Action entity proposes to take and expected timeframes for implementation of recommendations/suggestions**
	Please indicate your response to each recommendation/suggestion. If you do not accept a recommendation/suggestion, please provide reasons.	**Please provide particulars of any action you propose to take to implement the recommendation/suggestion and expected timeframes for implementation, including justification for the timeframes.**
Recommendation 1: Consistent with its responsibilities for driving improvement in fraud control practices, we recommend Services Australia: a. assess existing PORO processes across the myGov ecosystem to identify and document shared risks and work with member services to agree and implement appropriate controls	☒ **Accepted** ☐ **Not accepted** If not accepted, please provide reasons:	**Recommendation 1a:** **Proposed action:** I. Review current PORO processes across the myGov ecosystem to identify shared risks. II. Develop a risk management and mitigation plan (including controls) for shared risks with each member service. III. Ensure all new member service onboardings follow the endorsed onboarding process (updated March 2024), which mandates [a new member service undertaking] a risk assessment and developing a risk management and mitigation plan. **Expected timeframes:** I. December 2024 to conduct the review. II. January 2025 for risk management and mitigation plans developed in collaboration with existing member services following the review of current PORO processes.

Recommendation	Entity response to recommendations/suggestions	Action entity proposes to take and expected timeframes for implementation of recommendations/suggestions
	Please indicate your response to each recommendation/suggestion. If you do not accept a recommendation/suggestion, please provide reasons.	**Please provide particulars of any action you propose to take to implement the recommendation/suggestion and expected timeframes for implementation, including justification for the timeframes.**
b. consider establishing baseline PORO requirements which must be met by all member services.		III. As required – for new member services. **Recommendation 1b:** I. The Agency will consider establishing baseline PORO requirements as part of its review of current PORO processes referred to above. **Expected timeframes:** I. December 2024 to conduct the review in line with outcome 1a (I). January 2025 should the outcome of the review determine baseline PORO requirements should be established. **Justification for timeframes:** Consultation with 17 State and Commonwealth member services will be required.
Recommendation 2: a. We recommend Services Australia implement additional security controls such as two factor authentication across its three member services, for all	☒ **Accepted** ☐ **Not accepted** If not accepted, please provide reasons:	**Recommendation 2a:** **Proposed action 1:** I. The Agency will implement additional security controls for high risk transactions across Centrelink, Medicare, and Child Support. This will include:

Recommendation	Entity response to recommendations/suggestions	Action entity proposes to take and expected timeframes for implementation of recommendations/suggestions
	Please indicate your response to each recommendation/suggestion. If you do not accept a recommendation/suggestion, please provide reasons.	**Please provide particulars of any action you propose to take to implement the recommendation/suggestion and expected timeframes for implementation, including justification for the timeframes.**
high risk transactions, including linking a member service account to myGov and updating contact and bank account details.	Recommendation 2 a – Digital Operations	a. additional security around updates to bank accounts; and b. obfuscation of bank account details in the online platforms in the online platforms for Centrelink, Medicare, Child Support (as well as the Centrelink payments service in myGov). II. The Agency will review and update its online processes for PORO and linking for Centrelink, Child Support and Medicare to ensure sufficient and consistent verification steps are in place to link Agency services to myGov. See response to Recommendation 2b for non-digital channels. **Expected timeframes:** These measures will be delivered in increments by June 2025. **Justification for timeframes:** ICT work is required across the three programs of Centrelink, Medicare and Child Support, across the two digital channels of Online Accounts and mobile apps including co-design with customers.

Recommendation	Entity response to recommendations/suggestions	Action entity proposes to take and expected timeframes for implementation of recommendations/suggestions
	Please indicate your response to each recommendation/suggestion. If you do not accept a recommendation/suggestion, please provide reasons.	**Please provide particulars of any action you propose to take to implement the recommendation/suggestion and expected timeframes for implementation, including justification for the timeframes.**
b. Services Australia should ensure that a high standard of security settings for high risk transactions applies consistently across all available service delivery channels for its member services.		**Recommendation 2b:** **Proposed action 1 (for myGov):** The Agency has commenced development of a myGov security dashboard. This initiative will deliver myGov users with a visual presentation of their current security settings and will prompt them to take action such as uplifting their sign-in settings to either Passkeys or Digital ID to better secure their account. **Expected timeframes:** We anticipate delivering three iterations of this measure by June 2025. **Justification for timeframes:** This measure was announced as part of the 2024/25 budget. Our digital product design framework involves prototyping and testing with myGov users before technology development commences.

Recommendation	Entity response to recommendations/suggestions	Action entity proposes to take and expected timeframes for implementation of recommendations/suggestions
	Please indicate your response to each recommendation/suggestion. If you do not accept a recommendation/suggestion, please provide reasons.	**Please provide particulars of any action you propose to take to implement the recommendation/suggestion and expected timeframes for implementation, including justification for the timeframes.**
		Proposed action 2 (for Centrelink, Medicare and Child Support delivery channels): The Agency is developing an Enterprise Customer Authentication Tool (ECAT) to support telephony and face to face service delivery channels. ECAT will use a risk-based approach to authentication, where 'high risk' transactions, such as unlocking an online account, issuing a linking code, or updating a bank account will require a higher level of authentication. We anticipate the strengthened measures ECAT introduces will reduce the risk of fraudulent updates to phone numbers, email, and addresses made in staff facing channels. Authentication measures, like the adoption of passkeys and Digital ID, will enhance protection of a customer's myGov account. **Expected timeframes:** Completion of Phase One development by 30 June 2025 ECAT's complete implementation by 31 December 2025.

Recommendation	Entity response to recommendations/suggestions	Action entity proposes to take and expected timeframes for implementation of recommendations/suggestions
	Please indicate your response to each recommendation/suggestion. If you do not accept a recommendation/suggestion, please provide reasons.	**Please provide particulars of any action you propose to take to implement the recommendation/suggestion and expected timeframes for implementation, including justification for the timeframes.**
		Justification for timeframes: It is envisaged that the ECAT ICT build will be completed by 30 June 2025. ECAT will be required to manage the diverse complexity of an individual's PORO across Centrelink, Medicare and Child Support. This will need to be implemented across all three programs at the same time. This represents the largest change to authentication and PORO processes in a decade. After completion of Phase One, implementation, roll-out and staff training and preparedness is expected to take up to six months.
Recommendation 3: We recommend Services Australia establish formal processes for managing all shared risks across the myGov ecosystem, including identifying, assessing and documenting shared risks, periodically assessing the effectiveness of agreed controls, and	☒ **Accepted** ☐ **Not accepted** If not accepted, please provide reasons:	**Proposed action:** Engage and collaborate with member services to develop a formal process for managing shared risk across the myGov ecosystem. This work will be undertaken in parallel with the work being done for Recommendation 1a. **Expected timeframes:** October 2024

Recommendation	Entity response to recommendations/suggestions	Action entity proposes to take and expected timeframes for implementation of recommendations/suggestions
	Please indicate your response to each recommendation/suggestion. If you do not accept a recommendation/suggestion, please provide reasons.	**Please provide particulars of any action you propose to take to implement the recommendation/suggestion and expected timeframes for implementation, including justification for the timeframes.**
responding to indications that risk assessments should be updated.		**Justification for timeframes:** Time required to engage and collaborate and conduct risk assessments with 17 State and Commonwealth government member services.
Recommendation 4: We recommend Services Australia seek external legal advice about options to facilitate a greater level of information sharing across linked member services and support member services to act proactively to reduce fraud risk or other unlawful activity while meeting their other legislative obligations.	☒ **Accepted** ☐ **Not accepted** If not accepted, please provide reasons: Fraud and Identity Assurance	**Proposed action 1:** The Agency recognises that section 16A allows it to disclose information under the *Privacy Act 1988* as reflected in the myGov Member Services Handbook v 5.0, dated March 2024, which was provided to the Ombudsman. The Agency also recognises that this provision does not provide a general exception to program-specific secrecy provisions. The secrecy provisions and their application to protected customer information needs to be considered on a case-by-case basis. The Agency has received $2.4 million over two years (MYEFO 2023-24) to undertake research, evaluate the legislation landscape for myGov and to inform the future development of the platform.

Recommendation	Entity response to recommendations/suggestions	Action entity proposes to take and expected timeframes for implementation of recommendations/suggestions
	Please indicate your response to each recommendation/suggestion. If you do not accept a recommendation/suggestion, please provide reasons.	**Please provide particulars of any action you propose to take to implement the recommendation/suggestion and expected timeframes for implementation, including justification for the timeframes.**
		This activity reflects the Government's response to Recommendation 3 of the myGov User Audit and will also inform the advice required to facilitate information sharing as recommended. **Expected timeframes**: 30 December 2024 to undertake preliminary research. **Justification for timeframes:** As agreed with Government. **Proposed action 2:** As announced in the 2024/25 Budget (Strengthen myGov Fraud Prevention) the Agency has commenced development of new capability which will enable a greater level of information sharing between myGov member services that are linked to a myGov User's account. The myGov Incident Response System (MIRS) aims to provide faster, more accurate and auditable sharing of information between the myGov platform and linked member services.

Recommendation	Entity response to recommendations/suggestions	Action entity proposes to take and expected timeframes for implementation of recommendations/suggestions
	Please indicate your response to each recommendation/suggestion. If you do not accept a recommendation/suggestion, please provide reasons.	**Please provide particulars of any action you propose to take to implement the recommendation/suggestion and expected timeframes for implementation, including justification for the timeframes.**
		As part of implementing MIRS, the Agency will seek further external legal advice regarding the myGov Fraud Data Sharing Framework and information sharing. This will ensure data sharing protocols remain current and continue to operate within legislative obligations. **Expected timeframes**: This measure was announced as part of the 2024/25 budget. We anticipate delivering MIRS across two iterations by June 2025. This will include obtaining further legal advice on information sharing.
Suggestion 1: We suggest Services Australia share learnings and information about its authentication and PORO approaches with other myGov member services to support them to build their capability.	☒ **Accepted** ☐ **Not accepted** If not accepted, please provide reasons:	**Proposed action:** The Agency will share regular updates at the 'myGov Operational Member Service Forum' about authentication and PORO across the myGov ecosystem. **Expected timeframes:** August 2024 meeting **Justification for timeframes:** Next scheduled monthly meeting.

Recommendation	Entity response to recommendations/suggestions	Action entity proposes to take and expected timeframes for implementation of recommendations/suggestions
	Please indicate your response to each recommendation/suggestion. If you do not accept a recommendation/suggestion, please provide reasons.	**Please provide particulars of any action you propose to take to implement the recommendation/suggestion and expected timeframes for implementation, including justification for the timeframes.**
Suggestion 2: We suggest Services Australia regularly reviews and updates its communications regarding potential myGov and member service account breaches, including security notifications, staff guidance and online content, to ensure people are supported to take real time action to mitigate breaches to their myGov and or linked member service accounts.	☒ **Accepted** ☐ **Not accepted** If not accepted, please provide reasons:	**Proposed action:** The Agency has a strong communication focus on educating the public about myGov account security features and awareness of scams. As the Agency implements new security functions in myGov, all communication to the public, operational material for staff and notifications sent from myGov will be reviewed and updated. These notifications include details about steps a myGov user can take to secure their account. Agency staff are provided with detailed internal resources so they can best support people who have concerns about fraudulent activity with their online accounts. **Expected timeframes:** Ongoing myGov security notification messaging, Telephony IVR messaging improvements and Digital Assistant content will be reviewed on an as required basis or by 30 September 2024.

Recommendation	Entity response to recommendations/suggestions	Action entity proposes to take and expected timeframes for implementation of recommendations/suggestions
	Please indicate your response to each recommendation/suggestion. If you do not accept a recommendation/suggestion, please provide reasons.	**Please provide particulars of any action you propose to take to implement the recommendation/suggestion and expected timeframes for implementation, including justification for the timeframes.**
		Web content, operational material about scams and account security will be reviewed and updated every 6 months, or sooner as required. **Justification for timeframes:** The Agency uses continuous improvement principles to respond to environmental changes. This includes regular reviews and updates to website and marketing communications in response to public scam activities or issues raised by customers through our Agency phone operations and social media accounts. These necessary steps take some time and if rushed may be ineffective.

Disclaimer

Use of the Coat of Arms

Contact us

Inquiries regarding the licence and any use of this report are welcome at:

Commonwealth Ombudsman

Level 5, 14 Childers Street

Canberra ACT 2600

Tel: 1300 362 072

Email: ombudsman@ombudsman.gov.au