



28 August 2026

Select Committee on Cyber Security for Small to Medium Sized Businesses and Organisations
PO Box 6021
Parliament House
Canberra ACT 2600

Submitted to [APH submission portal](#)

Dear Select Committee,

TIO submission on the Inquiry into cyber security for small to medium sized businesses and organisations

Thank you for the opportunity to provide information to assist the Select Committee's Inquiry into cyber security for small to medium sized businesses and organisations.

The Telecommunications Industry Ombudsman (TIO) is a free, fair and independent external dispute resolution (EDR) service for individuals, small businesses and not-for-profits who have been unable to resolve their complaint with a phone or internet service provider.

We receive a growing volume of enquiries from people, small businesses and not-for-profit organisations who are unable to resolve problems with digital platforms. We regularly hear from people whose accounts have been hacked or compromised, most commonly social media and email, and are unable to regain access. For small business owners and not-for-profit leaders, this can disrupt advertising, communicating with customers and suppliers, access to business and customer information, and result in lost income and reputational damage. These complaints are currently outside our jurisdiction.

Government investment in cybersecurity resources has ensured small businesses and not-for-profits have access to best practice information on protecting digital infrastructure, account security, training employees, and troubleshooting incidents when they occur.

However, these measures do not compel digital platforms to provide practical customer support pathways to restore account access, reverse unauthorised charges, and access fair and timely support. Without stronger obligations on platforms to provide this necessary support, small businesses and not-for-profits are often unable to recover their accounts and restore their businesses when automated processes fail.

To improve cybersecurity for small and medium sized businesses and organisations, we offer the following recommendations:

Recommendation 1: Establish clear and enforceable internal dispute resolution (IDR) requirements for digital platforms.

Recommendation 2: Establish an external dispute resolution scheme for digital platforms by expanding the TIO's jurisdiction to handle both telecommunications and digital platform complaints as the Communications Ombudsman.

Small businesses and not-for-profit organisations need access to effective account recovery and dispute resolution pathways.

Research from the Consumer Policy Research Centre (CPRC) into Australian experiences online found that small businesses experience account hacking at a higher rate than individuals, 17 per cent compared to 9 per cent.¹ The research found that problems with hacked accounts were resolved to the consumer's satisfaction 56 per cent of the time, a higher rate than other digital service complaints, which could be attributed to the availability of government cybersecurity resources and support.²

However, these services do not place obligations on digital platforms to provide timely, transparent or human support. Digital platform users who approach the TIO for help consistently report difficulty accessing the help they need to fix their problem. They describe exhausting online forms, chatbots and email channels, receiving automated or generic responses, or being unable to speak to a person to resolve their complaint.

Case study: a small IT hosting business was affected by ransomware and poor incident communication.

Claire runs a business that provides IT cloud hosting services to clients. The company she leases her servers from had a security breach, which led to a ransomware attack. When she did not receive any incident updates from the server provider, Claire worked overtime to patch her security herself. The provider then took her servers offline to reboot them without notifying her, resulting in data losses and duplicated work.

Claire's client websites and data storage were impacted by the ransomware attack and the cloud server provider taking the system offline. She was frustrated that the provider did not properly communicate with her around their incident response, and she was concerned about the incident's impact on her business reputation.

**Names have been changed for privacy reasons.*

Case study: a community organisation lost its main public information channel

A community-run not-for-profit organisation relied on social media to provide news and updates for their local area. Their page was hacked and volunteers lost administrative control. They lodged complaints through online forms, chat, and provided identity verification, but never received a direct response from the social media company.

The organisation was concerned that they could no longer provide timely community and safety updates, and that hackers could post harmful or misleading information to their page. Unable to speak to a human or regain access to their account, and unsure what to do next, they contacted the TIO for help.

**Names have been changed for privacy reasons.*

¹ CPRC (2026) [Someone To Turn To](#) p.10

² Ibid, p.14

Recommendation 1: Establish clear and enforceable internal dispute resolution (IDR) requirements for digital platforms.

The ACCC's Digital Platforms Services Inquiry highlighted the need for dispute resolution and consumer protections, recommending the establishment of mandatory IDR standards and access to an independent ombuds scheme.³ Effective IDR standards should ensure accessibility, timeliness, accountability, the ability to escalate to a human representative, and transparency in decision-making.

In 2023, the Australian Government committed to undertake further work to develop internal and external dispute resolution requirements by calling on industry to develop voluntary internal dispute resolution standards by July 2024 as a first step.⁴ Two years later, there is no publicly available information about whether these standards have been developed or when they will be ready for use.

Recommendation 2: Establish an external dispute resolution scheme for digital platforms, by expanding the TIO's jurisdiction to handle both telecommunications and digital platform complaints as the Communications Ombudsman.

While services like the Australian Small Business and Family Enterprise Ombudsman (ASBFEO) can provide some assistance with digital platform problems, they can only help small businesses and family enterprises, and cannot compel platforms to provide information or deliver binding decisions. ASBFEO have noted that digital platform complaints are one of their fastest growing areas, placing growing pressure on their services.⁵

The Office of the Australian Information Commissioner (OAIC) plays an important role as Australia's privacy regulator however they are shifting towards systemic improvements and away from individual complaints.⁶ This coincides with a six to twelve month wait time for individual dispute resolution, making this an impractical avenue to resolve pressing privacy concerns.⁷

Establishing an ombuds scheme for digital platforms is a key recommendation of the ACCC's 2019 Digital Platforms Inquiry,⁸ and their Digital Platforms Services Inquiry Final Report.⁹ The Statutory Review of the *Online Safety Act 2021* echoed these recommendations as a key means of protecting people in Australian society.¹⁰ The Digital Platform Regulators Forum committed to exploring dispute resolution mechanisms for digital platforms as part of their 2026 work program.¹¹

³ ACCC (2025) [Digital platform services inquiry. Final report](#), p.20

⁴ Assistant Treasurer (2023) [Government's response to the ACCC's major competition and consumer recommendations for digital platforms | Treasury Ministers](#)

⁵ ASBFEO (2026) [Quarterly Report June 2026.pdf](#)

⁶ OAIC (2026) [Handling privacy complaints – a new approach for a new era](#)

⁷ OAIC (2025) [Annual report 2024-25](#)

⁸ ACCC (2019) [Digital platforms inquiry - final report.pdf](#), p.27

⁹ ACCC (2025) [Digital platform services inquiry. Final report](#), p.20

¹⁰ Rickard, D. (2024) [Report of the Statutory Review of the Online Safety Act 2021](#), p.8

¹¹ DP-REG (2026) [2026 DP-REG Work Program | The Digital Platform Regulators Forum \(DP-REG\)](#)

Expanding the TIO to take on this jurisdiction would strengthen the Australian government's online safety and cybersecurity reforms by giving consumers a trusted, independent and established avenue to individual redress.

Strengthening consumer safety improves trust.

The rapid evolution of online services and artificial intelligence has created a dynamic cybersecurity environment where traditional regulatory frameworks often struggle to keep pace. This lag can leave consumers exposed to further risks from opaque decision-making and inadequate resources when things go wrong.

The CPRC found that over half of Australians reported having lower trust online because of negative experiences resolving problems with platforms, and have stopped using the platform or service where they experienced the issue.¹² For small businesses and groups reliant on these platforms to reach their audiences, this decrease in trust risks reducing participation in the digital economy, as both entrepreneurs and consumers.

Consumers in Australia agree that it needs to be easier to make a complaint and have issues resolved with digital platforms. 82% of people surveyed by the ACCC believe there should be an independent EDR body to help resolve complaints with digital platforms.¹³ 83% of people surveyed by the CPRC were open to the TIO taking on that role.¹⁴

By implementing these recommendations and establishing a Communications Ombudsman, the government can create clear consumer standards for small businesses and not-for-profit organisations at every stage of a cybersecurity threat, across all platforms. This would strengthen the government's work in cybersecurity, online safety and consumer law reform, and give consumers a trusted place to turn when things go wrong.

Yours sincerely

Cynthia Gebert

Telecommunications Industry Ombudsman

¹² CPRC (2026) [Someone To Turn To](#), p.16

¹³ ACCC (2025) [Digital platform services inquiry. Final report](#), p.11

¹⁴ CPRC (2026) [Someone To Turn To](#), p.23