



Digital ID - Redress Framework for the Australian Government Digital ID System

ACCC Submission

October 2025

Executive Summary

1. The Australian Competition and Consumer Commission (**ACCC**) welcomes the opportunity to provide a submission on the proposed redress framework for incidents involving accredited services of accredited entities within the Australian Government Digital ID System (**AGDIS**). This submission provides key insights and recommendations to support the development of a fair, transparent and efficient redress framework designed with the consumer at its core.
2. The ACCC supports the recommendation of establishing an appropriate redress framework by 30 November 2025 as required under section 88 of the *Digital ID Act 2024* (Cth) (**the Act**) for the AGDIS.
3. Our submission supports a strong consumer focus, whereby consumers are provided with **accessible, consistent** and **clear** support and resolution pathways, and a presumption of notification model.
4. The ACCC has outlined concerns regarding the scope of the framework, the lack of detailed minimum requirements for published policies and query the impact of not notifying consumers.
5. To the maximum extent possible the redress framework should draw on established and successful benchmarks and frameworks for dispute resolution, including the *Benchmarks for Industry Based Dispute Resolution Schemes* and Australian standards.

Introduction and role of the ACCC

6. The ACCC is an independent Commonwealth statutory agency that promotes competition, fair trading, protection of consumers' rights and product safety for the benefit of consumers, businesses and the Australian community. The primary responsibilities of the ACCC are to enforce compliance with the competition, consumer protection, fair trading, and product safety provisions of the *Competition and Consumer Act 2010*, regulate national infrastructure and undertake market studies. The ACCC's purpose can be summarised as 'making markets work for consumers, now and in the future'.
7. Under the Act, the ACCC commenced its role as the Digital ID Regulator on 30 November 2024.
The ACCC's role as the Digital ID Regulator includes:
 - accrediting entities that provide digital ID services under the Digital ID legislation
 - approving entities to participate in the AGDIS, and
 - promoting compliance with the Act, including compliance and enforcement activities in relation to the Act and associated rules and standards.
8. The ACCC has interest in the development of an appropriate redress framework in the AGDIS both in its capacity as Digital ID Regulator, which includes responsibility for protecting the integrity of the AGDIS, and as the competition and consumer regulator.

Scope of the Redress framework

9. We consider any good redress framework should have the following guiding principles:
 - a consumer focus
 - clear support and resolution pathways
 - be based on a presumptive model.
10. The scope of the proposed redress framework is limited to identity service providers (**ISPs**) and attribute service providers (**ASPs**) that are a participating entity or an entity whose approval to participate has been suspended or revoked. The proposed redress framework does not apply to identity exchange providers (**IXPs**) or participating relying parties (**PRPs**) in the AGDIS.
11. According to the Explanatory Statement, this aligns with the intent of section 88 of the Act whereby the redress framework relates to incidents that occur in relation to accredited services of accredited entities in the AGDIS. As ISPs and ASPs provide direct accredited services to individuals to access services in the AGDIS, they will be expected to assist users with incidents.
12. While we understand this position, we are of the view that PRPs need to play a part in the redress framework to ensure impacted consumers with established trusted contact details are adequately supported.
13. We propose the redress framework should be expanded to *cover PRPs participating in the AGDIS for incidents that occur in relation to accredited services of accredited entities.*

The rationale for expanding the redress framework include:

 - aligning with rule 4.2 of the *Digital ID Rules 2024 (Digital ID Rules)* where all participating entities are required to report a cyber security or digital ID fraud incident that has or is reasonably suspected to have occurred in the AGDIS
 - reinforcing that all participating entities must report a relevant incident in the AGDIS
 - providing consumers with assurance that if they report an incident, that entity will escalate to the appropriate accredited service provider for incident management and resolution
 - consideration of the likely consumer relationships and contact points existing with the PRP.
14. We propose that at a minimum PRPs be included in the redress framework in relation to Part 4 of the Exposure Draft, in requiring entities to provide reasonable assistance to help consumers affected by incidents.
15. We also propose that strong consideration be given to include PRPs in relation to Part 5 of the Exposure Draft, to develop and publish policies relating to incidents and complaints, in the law review 2026 program.

A consumer using a digital ID to access a service in the AGDIS may see the PRP as their first point of contact if they encounter issues, rather than the accredited service provider.

For example, if a consumer sees abnormal transactions on their Centrelink statement and believe their digital ID has been compromised, they are unlikely to distinguish between a technical ISP issue or a PRP service issue. Consumers simply want their problem resolved. Regardless of who the consumer approaches first, they should be provided with appropriate support and direction to facilitate the swift and effective resolution of their issue. It is therefore essential that requiring PRPs to have procedures in place to handle and escalate such matters, be included in the legislation.

Consumers must have confidence that when they experience technical issues using the AGDIS, there is a clear pathway that they can access to resolve their issue. This aligns with the intent of proposed rule 4A.5 (2)(b) of the Exposure Draft.

Consumer focus and clear support and resolution pathways

16. It is vital that consumers are empowered with **accessible, consistent and clear** information for when they have been impacted by a cyber security or digital ID fraud incident and what pathways are available to remedy the situation.
17. We believe the proposed redress framework contains a greater focus on investigation and resolution of technical issues, rather than a consumer-centric focus. For example, it is not clear whether “technical issues’ will be defined sufficiently broadly to encompass the range of consumer disputes that may arise.
18. We welcome the inclusion of requirements on entities to develop and publish policies relating to the identification, management and resolution of incidents, and policies relating to complaints made by consumers, which provides transparency of process and procedures to consumers.
19. We also understand the need to strike a balance between being too prescriptive and allowing entities to leverage existing policies that are applicable to their digital ID services. However, we are of the view that the proposed framework appears to lack clear support and resolution mechanisms for the consumer.
20. Requirements for policies and procedures should be more explicitly defined, with the establishment of minimum standards in the redress framework to guarantee consumers receive consistent and reliable levels of support. We therefore recommend consideration of the following. The framework should:
 - provide an outline of the support available to consumers, for example internal or third-party support to:
 - coordinate assistance from relevant parties to use or access services using alternative means (especially relevant to entities excepted or exempted from voluntariness under section 74 of the Act)
 - provide recommendations regarding which organisations, such as the police, financial institutions or relevant government agencies should be notified of the incident
 - provide guidance on steps to recover a compromised digital ID or create a new digital ID, if required.
 - define the process for complaint resolution, for example:

- provide a clear and accessible end-to-end complaint process to inform consumers of what to expect, including acknowledgement of the complaint, timelines and points of contact, as multiple parties may be involved in resolving the issue
 - if consumers are dissatisfied with the outcome, what further recourse is available, including who to contact and how
 - utilise existing benchmarks for complaints resolution including the *Benchmarks for Industry Based Dispute Resolution* and relevant Australian standards.
- include financial redress options (to be developed and administered in the medium term)
 - seek to return the consumer to the position they were or would otherwise have been in, either financially or otherwise.
21. We suggest referring to established redress models from sectors like telecommunications and banking which have sound consumer escalation pathways for complaints and external dispute resolution schemes.

Notification to affected consumers should be on a presumptive model

22. We have previously expressed concern with allowing entities to decide whether to notify or not notify a consumer of a cyber security or digital ID fraud incident that impacts them.
23. We maintain the view that if trusted contact details are established by the entities, and notification will not adversely impact other consumers or the operation of the AGDIS, then there should be an express requirement in the redress framework for consumers to be notified.
24. We appreciate that our feedback has been taken into account and the draft rules were expanded to include additional matters to be considered by entities when assessing whether it is appropriate to notify. Working together with rule 4.2(3)(g)(ii) of the *Digital ID Rules 2024*, we are comforted that there is oversight in place to ensure entities justify their decision to the System Administrator, when it decides not to notify a consumer even when trusted contact details are held.
25. Despite this, we still question whether not mandating notification when trusted contact details have been confirmed and no other adverse outcomes have been identified, diminishes the consumers' ability to seek support or redress under the framework, or prevent them from taking protective action against possible scams.

Conclusion

26. The ACCC acknowledges the complexity of designing a consumer redress framework under the AGDIS, with the time pressures involved. As such, the ACCC recommends serious consideration be given to the factors above when progressing this important regulatory reform in 2026.
27. The ACCC looks forward to continuing to work with the Department of Finance and our government counterparts on the implementation of this legislation and progressing this important regulatory reform for the Australian community.