CHOICE

SUBMISSION TO THE DEPARTMENT OF FINANCE

DIGITAL ID BILL AND RULES

OCTOBER 2023

[redacted]

The Australian Consumers' Association is a not-for-profit company limited by guarantee. ABN 72 000 281 925 ACN 000 281 925

About Us

CHOICE is the leading consumer advocacy group in Australia. CHOICE is independent, not-for-profit and member-funded. Our mission is simple: we work for fair, just and safe markets that meet the needs of Australian consumers. We do that through our independent testing, advocacy and journalism.

Consumers in digital markets will benefit from a trusted, accessible and robust national Digital ID system. By providing consumers with an option to authenticate their identity in a secure and convenient Digital ID system, consumers can be better protected from threats of scams, identity theft, and data misuse, and will increase their trust in online products and services.

Conventional online verification processes leave consumers in Australia vulnerable to harm. Consumers are often required to provide digital copies of identity documents to businesses, often transferred through unsecured systems and indefinitely retained. Consumers seeking an alternative option may be required to authenticate their identities in person, which may be complicated, inconvenient or inaccessible for some consumers. Some business models also rely on collecting consumer data and offer little or no alternatives, as CHOICE found in its investigation into third-party rental platforms.[1]

However, a Digital ID system must be implemented with appropriate safeguards. Although Digital ID can neutralise a number of risks to consumer data, inadequate regulation and poor implementation can create new risks of exclusion and discrimination, data monetisation, and catastrophic data breaches.

To achieve these goals, CHOICE recommends the Federal Government:

1. establish a national Digital ID system to protect consumers;
2. empower the ACCC as the interim Digital ID Regulator;
3. prioritise consumer protections and obligations on participating businesses in standards set in the Accreditation Rules;
4. require and adequately resource consumer consultation in future developments of accreditation and data standards;
5. provide consumers alternative means to authenticate their identity;
6. limit exemptions to interoperability and strengthen the Digital ID Regulator's ability to refuse exemptions;
7. provide resourcing for economy-wide consumer education and advocacy on the use of Digital ID trustmarks;
8. consider the future use of different trustmarks for accreditation-only entities and entities also participating in AGDIS;

[1] CHOICE, 2023, *At What Cost? The price renters pay to use RentTech,* https://www.choice.com.au/consumer-advocacy/policy/policy-submissions/2023/april/renttech-report

9. prohibit Digital ID providers from charging consumers a fee to create or deactivate a Digital ID and prohibit relying parties from passing on fees to consumers;
10. review proposed penalties for breaches of the Digital ID Bill to align with consumer expectations and other privacy related regulatory regimes;
11. introduce statutory rights to consumer redress, including appropriate and accessible dispute resolution process;
12. implement reforms to the Privacy Act such as
    a. personal redress through a statutory tort for invasion of privacy and a direct right of action,
    b. introducing a fair and reasonable use test, and
    c. stricter controls on overseas data flows; and
13. introduce an unfair trading prohibition in the Australian Consumer Law.

A well-designed national Digital ID system can protect consumers

Consumers in Australia will be better protected from identity theft and data misuse harms under a well-designed national Digital ID system. A major harm experienced by consumers is through data breaches. A report by the Office of the Australian Information Commissioner (**OAIC**) on recent notifiable data breaches found that 60% of breaches exposed identity information, such as data of birth, passport details, and driver licence details.[2] A recent survey by the OAIC also found that almost half of all Australians had been involved in a data breach in the preceding year, and three-quarters had subsequently experienced harm; almost a third had to replace identity documents.[3] Unsurprisingly, only 12% of consumers have trust in businesses to use their data responsibly and in their interests.[4]

A national Digital ID system should aim to minimise the number of sensitive identity documents transmitted and stored across the economy. CHOICE supports the establishment of this system through a robust accreditation scheme and through the Australian Government Digital ID System (**AGDIS**). CHOICE also supports the government's phased approach to the Digital ID system that integrates state/territory

[2] OAIC, 2023, "Notifiable Data Breaches Report: July to December 2022", https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-july-to-december-2022
[3] OAIC, 2023, *Australian Community Attitudes to Privacy Survey 2023*, https://www.oaic.gov.au/__data/assets/pdf_file/0025/74482/OAIC-Australian-Community-Attitudes-to-Privacy-Survey-2023.pdf
[4] CHOICE Consumer Pulse June 2023 is based on a survey of 1,087 Australian households. Quotas were applied for representations in each age group as well as genders and location to ensure coverage in each state and territory across metropolitan and regional areas. Fieldwork was conducted from 7th to 22nd of June 27, 2023

digital IDs and enables the use of myGovID in private sector services before integrating private sector Digital IDs. This phased approach will build consumer confidence in the system and facilitate consumer literacy of the system. Further, CHOICE welcomes the additional privacy safeguards in the Digital ID Bill 2023 (Cth) ('**Digital ID Bill**') such as the prohibition of one-to-many biometric matching, the requirement for express consent, prohibition on data profiling, and restrictions on marketing.

CHOICE also supports the government's proposed regulatory framework for the Digital ID system, including the appointment of the Australian Competition & Consumer Commission ('**ACCC**') as the interim Digital ID Regulator, and the OAIC as the regulator for privacy protections in the Digital ID legislation. The ACCC is best suited to this role due to its expertise in consumer protections, including in digital markets. The OAIC is best suited to have oversight over privacy regulations in the legislation, particularly as many of these regulations should be considered in conjunction with the *Privacy Act 1988 (Cth)* ('**Privacy Act**'). The ACCC and OAIC should be appropriately resourced to fulfil its Digital ID functions without compromising its other regulatory roles.

Consumers must have confidence that accreditation means robust standards have been met

Consumers will only benefit from a Digital ID system that is built on safe, reliable, and transparent accreditation standards. Holding accredited businesses to robust standards will also build consumer trust in the Digital ID system. Technical standards in the Accreditation Rules should comply with international best practice, and usability and accessibility requirements should ensure all consumers can access the same quality of Digital ID service regardless of the provider they use. Consumers should also be able to trust in the security and retention of their stored data as a data breach in a Digital ID service could have catastrophic effects, particularly if irreplaceable biometric information is breached. CHOICE notes the consultation on Accreditation Rules concludes after the close of the Digital ID Bill and Rules consultation, and urges the Federal Government to prioritise consumer safety and fairness in its consideration of the Accreditation Rules.

The Digital ID system must avoid the failings of the Consumer Data Right (**CDR**) scheme to benefit consumers and increase consumer adoption and trust in the system. As noted by the Consumer Policy Research Centre (**CPRC**), CDR was designed to give consumers greater control over their own data, but allowed non-accredited entities to gain access as

well.[5] The Digital ID's accreditation scheme should be designed to ensure only trusted and authorised businesses engage with consumers or their data, rather than give unaccredited entities weaker obligations. CPRC also noted that CDR overly relied on disclosure and consent, rather than requiring businesses to act safely and fairly.[6] Due to the highly complex and technical nature of Digital ID, it is vital that accreditation standards protect consumers from harms instead of relying on consumers to consent to potential harms.

Another failing of the CDR that should be avoided in Digital ID is with consumer representation. Consumer representatives were and are insufficiently consulted in the CDR and its evolution, nor was any consumer consultation appropriately resourced by the government as most consumer advocacy organisations are not-for-profit organisations with limited resources. An obligation to consult with consumer advocacy organisations was also recommended by the OAIC.[7] For the Digital ID System, the Data Standards Chair responsible for data standards beyond the Accreditation Rules should also be required to consult with consumer representatives, and this consultative role should also be appropriately resourced by the Federal Government.

Consumers should not be excluded by or from Digital ID

All consumers that want it should have access to the protections from data-related harms that Digital ID provides. CHOICE recommends the Federal Government prioritise the following areas in the Digital ID Bill and subsequent implementation of the Digital ID system to ensure inclusive consumer participation in the Digital ID system:

(a) alternative methods for authentication,

(b) limiting exemptions to interoperability between private Digital IDs,

(c) promoting consumer confidence and literacy with trustmarks, and

(d) prohibiting charging consumers for using Digital ID.

[5] CPRC, 2022, "Submission: Statutory Review of the Consumer Data Right – Issues Paper", https://cprc.org.au/submission-statutory-review-of-the-consumer-data-right-issues-paper
[6] CPRC, 2022, "Submission: Statutory Review of the Consumer Data Right – Issues Paper", https://cprc.org.au/submission-statutory-review-of-the-consumer-data-right-issues-paper
[7] OAIC, 2022, "OAIC submission to the Statutory Review of the Consumer Data Right", https://www.oaic.gov.au/engage-with-us/submissions/oaic-submission-to-the-statutory-review-of-the-consumer-data-right

Alternative methods for authentication

Consumers should be free to choose an alternative method of authentication if they do not wish to use or can't use Digital ID. CHOICE welcomes assurances in the proposed legislation that participation in the Digital ID system should remain voluntary for consumers.[8] Government agencies such as the Australian Transaction Reports and Analysis Centre have recognised that various groups may have structural barriers to official identification, including Aboriginal and Torres Strait Islander people located remotely, people affected by natural disaster, and people affected by domestic and family violence.[9] As the Digital ID system accesses existing documentation, this will exclude people without official identification. Consumers who are less digitally literate, without access to digital technology, or with personal objections to Digital ID will also benefit from alternative methods for authentication.

CHOICE recommends that the Digital ID Rules require accredited entities in the Digital ID system to follow best practice standards on inclusive and accessible design. The Digital ID system is most effective when it strives to ensure all consumers can access its services.

Limiting exemptions to interoperability between private Digital IDs

Interoperability between Digital IDs is necessary to guarantee consumer choice and control over their own data. While interoperability is mostly guaranteed in the Bill, CHOICE is concerned with the exemption to interoperability if it is to "assist individuals who would otherwise be at a disadvantage in accessing the Australian Government Digital ID System."[10] This may limit consumer choice and data control for consumers with additional needs, and preferably all Digital ID platforms should have robust accessibility features. Further clarity is also needed on how an exemption for services by relying parties that "promote use of digital IDs if the service, or access to the service, was available through the Australian Government Digital ID System" will be interpreted by the Minister.[11] The Federal Government should remove exemptions to interoperability that

[8] Digital ID Bill 2023, s71
[9] AUSTRAC, 2023, "Assisting customers who don't have standard forms of identification", https://www.austrac.gov.au/business/core-guidance/customer-identification-and-verification/assisting-customers-who-dont-have-standard-forms-identification
[10] Digital ID Bill 2023, s75(3)
[11] Digital ID Bill 2023, s75(3)

may affect consumer choice of Digital ID when accessing government or business services.

Promoting consumer confidence and literacy with trustmarks

A Digital ID trustmark can promote consumer confidence in the security and validity of accredited Digital IDs. However, consumers will need time to identify or seek out trustmarks when using Digital ID services. Worse, consumers may be intentionally misled by deceptive services without accreditation. The Federal Government should adequately resource consumer education and awareness on trustmarks, including through consumer advocacy organisations. The Federal Government should also consider in the future whether different trustmarks are needed for accredited Digital ID providers and providers that are also participating in AGDIS.

Prohibiting charging consumers for Digital ID

As a system designed to keep consumers safe in digital markets, access to Digital IDs should be encouraged and facilitated. However, the Digital ID Bill allows accredited Digital ID providers to charge a fee in relation to the use of its ID services.[12] Charging a fee for creating or using a Digital ID may disincentivise adoption of Digital ID or be prohibitive for people who can't afford the charges, undermining the benefits of the system and putting excluded consumers at greater risk of data-based harms. Further, allowing an accredited entity to charge for Digital ID use in a private service while the same ID may be used for free in AGDIS may result in confusion. CHOICE recommends the Federal Government prohibit the charging consumers a fee to access Digital ID, as well as prohibiting relying parties from passing on fees onto consumers through additional costs.

Strong enforcement is needed to protect consumers

Consumer trust and confidence in the Digital ID system is critical to its success. In addition to robust standards for accreditation, consumers rightly expect that breaches of Digital ID legislation and rules will be appropriately penalised to deter future noncompliance. Strong enforcement tools for regulators will also ensure that businesses without the adequate capacity to deliver safe and secure Digital ID services will be less likely to participate in the system. The Digital ID Bill includes powers for regulators

[12] Digital ID Bill 2023, s142

around accreditation, such as the revocation of accreditation, that may protect consumers from harmful practices.

However, to strengthen these enforcement tools further, CHOICE recommends the Federal Government increase the proposed penalties in the Digital ID Bill. Currently, the maximum proposed civil penalty for a breach of the Bill is 300 penalty units ($93,900) for offences such as the disclosure of restricted attributes or failure to destroy biometric information when required.[13] This is misaligned with civil penalties for breaches of credit reporting regulations in the Privacy Act that range between 500 and 2000 penalty units, and are vastly lower than penalties for entities committing serious or repeated interferences with privacy which begin at $50,00,000.[14] Due to the risks of data misuse, consumers expect that Digital ID businesses entrusted with sensitive consumer data should be held adequately accountable; while 300 penalty units may deter small businesses, it is unlikely to hold larger businesses to community standards.

There is currently no mechanism in place in the Digital ID Bill for individual redress. Consumers should be able to receive a remedy in the event of harm caused by a Digital ID provider which has failed to adhere to the Digital ID legislation. This would provide another strong incentive for compliance, in addition to civil penalties, as well as ensuring consumers are not unfairly suffering harm. A personal redress mechanism could be achieved by providing consumers using Digital ID a statutory right to compensation in appropriate circumstances. Consumers affected by harms to their privacy could also seek redress through a statutory tort for invasions of privacy or a direct right of action in the Privacy Act. The Federal Government should also prioritise establishment of appropriate and accessible dispute resolution schemes for consumers to exercise these rights.

Reforms to the Privacy Act and Australian Consumer Law will support Digital ID

Consumers are best protected from harm by a whole-of-economy approach to consumer protection. While a Digital ID system is a step in the right direction, the integrity of this system requires reforms in other areas of consumer protection. Strengthening and modernising the Privacy Act and Australian Consumer Law will protect consumers in digital markets and support the goals of the Digital ID system.

[13] Digital ID Bill 2023, s43; Digital ID Bill 2023, s48
[14] OAIC, 2023, "Chapter 7: Civil penalties — serious or repeated interference with privacy and other penalty provisions", https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-7-privacy-assessments

CHOICE welcomes the Federal Government's recent support for the majority of recommendations in the Privacy Act Review, and urges the Federal Government to implement reforms as soon as possible. These reforms will complement Digital ID legislation. For instance, the introduction of a fair and reasonable use test will require businesses to only collect and keep data that is essential to the provision of a good or service to a consumer. Alongside Digital ID, this will encourage businesses to adopt Digital ID as a convenient and safe method for authenticating a consumer's identity, and should restrict businesses from requesting additional information unnecessarily. Reforms to overseas data flows in the Privacy Act will also better protect consumers from Digital ID data stored overseas, as the Digital ID Bill only prohibits holding information outside Australia for accredited entities participating in AGDIS.

CHOICE also supports the introduction of a prohibition on unfair trading in the Australian Consumer Law. A prohibition on unfair trading will complement the use of trustmarks and provide the ACCC further ability to take enforceable actions against businesses misleading or deceiving consumers into the use of unaccredited or untrustworthy identification platforms, including through the use of deceptive patterns online.