Australian Payments Plus

Committee Secretary
Senate Standing Committee on Economics
PO Box 6100
Parliament House
Canberra ACT 2600

19 January 2023

Lodged via the APH Portal

Inquiry into Digital ID Bill 2023 and the Digital ID (Transitional and Consequential Provisions) Bill 2023

Dear Committee,

Australian Payments Plus (**AP+**) welcomes the Inquiry into Digital ID Bill 2023 and the Digital ID (Transitional and Consequential Provisions) Bill 2023 (**the Bills**).

Australian Payments Plus (AP+) brings together Australia's three domestic payment rails, BPAY, eftpos and the New Payments Platform (**NPP**), into one integrated entity. AP+ builds and operates Australia's national payment and data infrastructure.

AP+ is a committed supporter of the Digital ID Taskforce and this is important legislation that will allow Australians the choice to enhance the privacy and security of their personal information, thereby making Australian identities harder to steal. **ConnectID**, a TDIF-accredited Digital Identity exchange, is a key part of the Australian owned national infrastructure that AP+ operates. ConnectID is an identity verification solution with uses across governments, financial services, telecommunications, utilities, retail, travel, hospitality, and payments. ConnectID is designed to support and complement government and private sector identity initiatives and to be a hub in the Digital ID System to address the growing issues of unnecessary oversharing of data, identity theft and data breaches.

To best achieve the objectives of the proposed reform, AP+ wishes to offer eleven recommendations on the draft legislation reflecting our experience as a Digital ID exchange operator and from lessons learnt overseas.

Most importantly, the future Australian Digital ID System will contain participants (e.g., banks, government agencies and others) who will operate in both the accredited and non-accredited environments, and there is therefore a need to ensure clarity in the reach and operation of the obligations in the legislation outside the accredited environment of the Australian Digital ID System. Ensuring clarity in how far the obligations stretch outside the Australian Digital ID System is critical – without further clarity in the Bills and explanatory materials, a considerable disincentive to participate in the Australian Digital ID System will be legislated meaning accredited entities who wish to also offer services outside the accredited environment will face a substantial cost and operational disadvantage. Critically, the benefits of consumer choice, consumer control, data minimisation and greater national resilience against identity fraud may not be fully achieved.

To explain, many accredited entities will continue to offer other services to their customers outside a Digital ID Service. For example, banks (and federal/state government agencies) may offer their customers a Digital ID service, but that Digital ID is not the only product or service the bank or agency provides to their customer. As drafted, the legislation places limitations on an accredited identity provider's ability to provide services that it already provides to customers - such as the daily (and highly regulated) services provided by an individual's bank where the confirmation of identity may be required to authorise a banking action. The

proposed legislation potentially restricts some legitimate and in the case of banks, very highly regulated interactions, with their customers, for example, in the collection of certain attributes (s41), biometric information (s45) and marketing (s52).

Without amendments to the Bills, the benefits of consumer choice, consumer control, data minimisation and greater resilience against identity fraud will not be achieved as the Digital ID System will lack the necessary public and private sector participation to achieve the benefits of interoperability.

AP+ therefore makes eleven recommendations to achieve the intent of the Digital ID Bills.

This AP+ submission:

AP+ has a keen interest in the legislation which enables the next iteration of the Australian Digital ID System. A successful national Digital ID ecosystem will yield the privacy and security benefits for all those Australians who choose to use a Digital ID solution to better protect their identity.

We have structured this AP+ submission as follows:

> ***Covering letter***: Outlines key issues regarding the scope and potential reach of the Bills which AP+ believes need to be addressed before the legislation proceeds.
>
> ***Attachment A***: Recommendations for each of the key issues outlined in this cover letter and the necessary changes sought before the legislation is passed. We have also included additional recommendations on other aspects of the proposed Digital ID system.
>
> ***Attachment B***: Additional comments on sections of the draft legislation.

Summary of key concerns regarding the draft legislation

Scope and reach of the legislation

Clarity on when the legislation will and will not apply to accredited entities is critical to the operation and success of the Digital ID System. For the reasons outlined above, AP+ has focused our recommendations on clarifying the definition of "accredited service", however we recognise that other consequential amendments may also be necessary.

> **Definition of accredited service:** AP+ strongly recommends that amendments be made to the legislation and explanatory materials, to provide the necessary clarity around the definition of "accredited service" and how obligations in the Bills, ID Rules and Accreditation Rules will apply for accredited entities who provide services both inside and outside the proposed Digital ID System.
>
> It is currently unclear what obligations apply:
>
> 1. to accredited entities only when they are providing accredited services inside the Digital ID System.
>
> 2. to accredited entities when they are providing services (which are accredited services) outside the Digital ID System – e.g., through non-accredited channels.
>
> 3. to accredited entities at all times, including when providing non-accredited services – e.g., banks or government agencies providing regular (non-identity) services to their customers/citizens.

Proposed phased expansion

AP+ is a committed advocate for the Digital ID System. AP+ does not however support the proposed phased approach to the sequential expansion of the Australian Government Digital Identity System (**AGDIS**), particularly as ConnectID is purposely designed to help transform the way Australians manage and protect their identity to help address the growing issue of identity theft and data breaches. Strengthening Australia's resilience to cyber threats and identity fraud at an ecosystem level will only be achieved once there is full interoperability within the Digital ID System, including the AGDIS. Data minimisation is a key objective for both ConnectID and the Digital ID System, and this benefit for Australians will only be achieved when there is ubiquity in the use of Digital IDs, strengthening the resilience of identities against theft by reducing unnecessary oversharing of data.

Overseas experience shows a successful national digital identity ecosystem relies on interoperability and mutual recognition of digital credentials between the public and private sectors, which in the case of the AGDIS is the proposed 'Phase 4'. The proposed phasing removes the ability for consumers to use their preferred identity provider from day one. Australians should have the choice to leverage their existing trusted relationships and choose their preferred Identity Provider, so they have the choice to securely interact with all relying parties across the public and private sector.

The proposed phasing also causes uncertainty for businesses who may wish to become accredited. The undefined timelines will discourage entities from undertaking the necessary (and costly) accreditation groundwork required ahead of joining the Digital ID System. This will slow the uptake and adoption of Digital IDs and hinder the development of a vibrant and secure digital economy.

High cost of accreditation and duplicative regulatory burden

The cost of the proposed accreditation process and duplicative regulatory burden may be a disincentive for wider participation. The requirement for at least six external assessments (a privacy assessment and privacy impact assessment; protective security assessments including both pen test and ISO 27001 accreditation; fraud, and usability/ accessibility including WCAG accreditation) will make it hard to get a critical mass of participants. These are very important obligations which AP+ supports, but it is the case that many of these assessments and accreditation are obligations that already exist for regulated entities like banks. AP+ recommends that mutual recognition of existing standards, licences and regulations be adopted and limit the requirement for external assessments to where the requirements of the ID System exceed those existing standards or regulations.

Lessons from overseas

AP+ launched ConnectID with banks and other trusted providers, as experience from overseas shows that bank participation in a Digital ID ecosystem is critical to establishing trust and adoption (Norway, Sweden and Canada being good examples). In Norway, 4.3 million Norwegians have chosen to use a Digital ID (BankID), representing nearly 80% of the population, of those, 99% use their Digital Identity to access a range of both government and private sector services an average of 220 times a year – this almost daily use of identity verification solutions drives adoption and builds systemic cyber resilience. ConnectID is an open marketplace for trusted and authorised identity providers including banks (large and small), and non-bank entities who have been accredited under TDIF and also meet the necessary ConnectID security and privacy obligations.

A Digital ID System built on trust, transparency, consumer control, personal choice and privacy; and is an essential part of Australia's National Strategy for Identity and is a key pillar of the 2023-2030 Cybersecurity Strategy to build Australia's resilience to cyber threats and identity fraud at an ecosystem level. AP+ are committed to this important reform that will benefit all Australians who choose to use a digital ID.

I thank the Committee for their time and consideration, we are available to answer any questions.

Yours sincerely,

[redacted]

Lynn Kraus
Chief Executive Officer,
Australian Payments Plus

Encl.

Attachment A: 11 AP+ recommendations for amendments to the draft bills

Clarity around the scope of legislation and the definition of Accredited Service

It is currently unclear how obligations in the draft Bill, ID Rules and Accreditation Rules will apply to accredited entities who provide services both inside and outside the proposed Digital ID System.

This creates uncertainty for prospective providers and will limit participation in the Digital ID System from private and public sector organisations.

It is currently unclear what obligations apply:

1. to accredited entities *only* when they are providing accredited services inside the Digital ID System.

2. to accredited entities when they are providing services (which are accredited services) outside the Digital ID System – e.g., through non-accredited channels.

3. to accredited entities at all times, including when providing non-accredited services – e.g., banks or government agencies providing regular (non-identity) services to their customers/citizens.

AP+ recommends (Rec 1):

That the Committee recommends amendments to the legislation and explanatory materials to address the need for greater certainty around the definition of "Accredited Service" and how the Bills, Rules and Accreditation Rules are intended to operate for accredited entities who provide services both inside and outside the Digital ID System.

Particular focus should be on:

a) where the accredited entity provides services (which are Accredited Services) outside the Digital ID System or AGDIS, and

b) where the drafting restricts other legitimate (and in the case of banks, highly regulated) interactions with their customers beyond the scope of their Digital ID service.

Proposed phased expansion

AP+ is a committed supporter of the work of the Digital ID Taskforce and an advocate for an Australian Digital ID System. AP+ does not however support the proposed phased approach to the sequential expansion of the AGDIS, particularly as products like ConnectID are now available. Strengthening Australia's resilience to cyber threats and identity fraud at an ecosystem level will only be achieved once there is full interoperability within the Digital ID System, including AGDIS.

Without change to the proposed phased approach, the broader economic and productivity benefits of the Digital ID System are not likely to be realised until 'Phase 4', which is when there is interoperability and mutual recognition of digital credentials between public and private sector.

Further, the proposed phasing removes the ability for Australians to choose their preferred identity provider from day one. The phased approach also does not consider lessons learnt from abroad as the experience of overseas jurisdictions shows that bank participation in Digital ID is critical to establishing trust and adoption.

AP+ recommends (Rec 2):

That the Committee recommends the Government remove the concept of phasing from the draft Bill to promote interoperability and provide consumers with choice and control over their preferred identity provider from day one.

AP+ would also welcome the opportunity to work with Government on a proof of concept to enable interoperability and mutual recognition of digital credentials between public and private sector. Initially such work could be a single use case. For example, Services Australia and the Reserve Bank of Australia (RBA) using Digital IDs from both public and private sector providers to more efficiently authorise and process disaster relief payments in real time whilst also helping to reduce fraudulent access to this support.

High cost of accreditation

The cost of the proposed accreditation process will likely be a disincentive for full private sector participation. The requirement for at least six external assessments (a privacy assessment and privacy impact assessment; protective security assessments including both pen test and ISO 27001 accreditation; fraud, and usability/ accessibility including WCAG accreditation) will make it hard to get a critical mass of participants beyond large well-resourced participants. Further, many large institutions (public and private) are already subject to significant regulation, standards and oversight, and the products of these existing similar regulatory obligations should be leveraged wherever possible to minimise duplication of effort and encourage participation.

AP+ recommends (Rec 3):

That the Committee recommends that mutual recognition of existing standards, licences and regulations be adopted, and limit the need for external assessments only where requirements of the ID System exceed those existing standards or regulations.

Obligations in the draft legislation

1. The Digital ID Bill attempts to create a nexus between many of the obligations and participation in the Digital ID System – for example s31 refers to providing the accredited services or doing things incidental or ancillary to those services. However, AP+ believes the current drafting is too broad especially for accredited IDPs, for example, the collection of certain attributes (s41) biometric information (s45) and marketing (s52). Regulated entities like banks or government agencies have existing practices and obligations (including existing identity verification processes) while providing a product or service to an individual. The reach of the proposed Digital ID framework may work contrary to these other legislative obligations. The AP+ concern is that obligations in the Bill overreach into some of these regulated business activities where that entity becomes an accredited identity provider.

AP+ recommends (Rec 4):

That the Committee recommends the legislation is amended to ensure participants who offer more than just Identity Verification services to a customer continue to have the ability to retain information in support of other legal or permitted purposes. For example, retention of proof of identity verification for mortgage applications and other processes including fraud prevention and anti-money laundering obligations.

2. The Bill and Rules require participating accredited entities and participating relying parties not to refuse to provide or accept services to/from other participating accredited entities or participating relying parties. An entity can apply to the Minister for an exemption to the interoperability

obligation. AP+ believes that the circumstances under which the Minister can grant an exemption are too broad and lack the necessary clarity to provide some certainty for industry to invest and grow in the Digital ID System with confidence.

AP+ recommends (Rec 5):

That the Committee recommends that an amendment is made to remove the power for the Minister to grant exemptions from interoperability. In the alternative, clear criteria should be established on which the Minister must base their decision to grant an exemption to the interoperability obligation. A successful national digital identity ecosystem relies on interoperability and the mutual recognition of digital credentials across and between the public and private sector.

3. The other powers granted to the Minister to make various rules and impose obligations impacting IDPs is also broad. Each of these powers should have clear criteria which the Minister must give consideration to when making a decision. AP+ raises this issue as we seek to adopt the lessons learnt from the rollout of the Consumer Data Right (CDR).

AP+ recommends (Rec 6):

That the Committee recommends the other powers granted to the Minister and the Digital ID Regulator to make various rules and impose obligations impacting IDPs should also require clear criteria which the Minister and/or Digital ID Regulator must give consideration to when making a decision.

Indigenous Australians and their access to conventional forms of identification or other documentation

Regarding section 41 in Chapter 3—Privacy, Division 2—Additional privacy safeguards.

The legislation should not prohibit the ability to collect, use or disclose the attributes of an individual who identifies as Aboriginal or Torres Strait Islander. Like all other aspects of the Digital Identity System that choice should also remain with the individual, via consent.

AP+ makes this recommendation as the legislation should not restrict accredited entities offering the ability for individuals to be able to reflect their cultural identity in certain digital representations.

There are positive practical use cases for “proof of Aboriginality” as an attribute, including:

- Demonstrating Aboriginal or Torres Strait Islander status for access to concessions such as education, government, banking and health, whilst also helping to reduce fraudulent access to those concessions.
- Proving representation in native title access discussions.
- Voting for elected representatives in Indigenous bodies.
- Facilitating employment opportunities for first nations people.

AP+ draws attention to the work of *Hold Access*, an Indigenous Corporation which is supported by ConnectID, NAB, the Red Cross and others. Hold Access, via their Digital ID product (Wuna) is closing the gap on First Nations Australians digital identity. Indigenous Australians and their access to conventional forms of identification or other documentation to access mainstream public and private services is an ongoing challenge in Australia which Hold Access seek to solve via their ID product Wuna.

Hold Access is exploring how they can support the ability for Indigenous Australians (if they so choose) to have a Digital ID that also preserves aspects of their indigenous cultural identity in the digital world.

Some links to the work underway by Hold Access:

https://news.nab.com.au/news/nab-digital-next-how-hold-access-is-bridging-the-gap-for-first-nations-australians-in-a-digitalised-economy/

https://www.humanitech.org.au/resources/hold-access/

> ***AP+ recommends (Rec 7)**:*
>
> That the Committee recommends the legislation be amended to not blanket restrict the ability to collect, use or disclose the attributes of an individual who identifies as Aboriginal or Torres Strait Islander. Like all other aspects of the Digital Identity System that choice should remain with the individual.
>
> Further, that the Committee recommends the restriction in s41 on disclosure of restricted attributes, should ideally be qualified so that it does not capture necessary incidental disclosure, noting that the Office of the Australian Information Commissioner (OAIC) has previously commented on incidental disclosure in photos (e.g. of people wearing traditional ethnic dress) or names can convey race or religion.

Proposed Data Standards Chair

The legislation adopts the concept of a Data Standards Chair, this concept is taken from the rollout of the Consumer Data Right (**CDR**). As with any new economy wide innovation there were challenges with CDR and the industry having to navigate the competing demands of Treasury, the CDR Data Standards Body (DSB) and the ACCC.

AP+ considers the proposed governance model is too complex and does not adopt the lessons learnt in the CDR rollout. The 2022 independent review[1] of the Consumer Data Right by Elizabeth Kelly PSM is a useful starting point. While that review stopped short of recommending immediate changes to the CDR's complex mix of regulators, it nonetheless identified a number of challenges including insufficient coordination and delineation of roles.

> 'Finding 2.3: *The Review heard from participants that their experience in the CDR has been compliance focussed to date. Concerns were raised by participants about complex and overly prescriptive rules and standards that have prevented them from focusing on developing new products and services. As the system develops and matures, including through the introduction of action initiation, consideration should be given to ways that implementation can reduce the complexity associated with rules and standards for participants.*'

AP+ considers that the method for setting standards in the Digital ID System should be designed to avoid the issues of 'overly prescriptive rules and standards' that have impeded the development of CDR. Importantly, the development of standards should be demand driven, i.e., driven by the Digital ID Taskforce and/or participants and not driven by the availability of resources within the data standards body to initiate change and iteration for change's sake. AP+ would welcome the Digital ID Taskforce applying the governance and oversight lessons learnt from CDR.

[1] Federal Treasury Report, Statutory Review of the Consumer Data Right, Report, 2022. Available at: https://treasury.gov.au/sites/default/files/2022-09/p2022-314513-report.pdf

AP+ recommends (Rec 8):

That the Committee recommends that the Digital ID Taskforce do not adopt the CDR approach to data standards. That the Digital ID Taskforce takes the lessons learnt from CDR and design from first principles: the role, function, authority, oversight, audit and control of the Digital ID Data Standards Chair and their work. The Digital Identity and Authentication Council of Canada (DIACC) is one model that has seen success.

The Data Standards Chair should be required to engage in genuine co-design on standards with participants in the AGDIS (and subject matter experts), including a focus on the adopting of international standards, rather than bespoke design.

Further, that the Committee recommends that the Data Standards Chair should report to the head of the Digital ID Taskforce.

Cyber Resilience

The definition of cyber security incident in the exposure draft is very broad, as the draft definition includes 'attempts' to gain access to systems, even if these attempts are blocked and unsuccessful.

Large organisations such as banks and government agencies are subject to, and successfully repel, hundreds of thousands of cyber-attacks daily. The reporting of these failed attempts serves no purpose and may overwhelm the regulator with useless information.

To be clear, AP+ supports all efforts to ensure greater cyber resilience in the Digital ID system and elsewhere across the economy. However, we consider that further analysis is needed to ensure the obligations for ensuring cyber resilience (including reporting) are appropriate and aligned with other significant pieces of legislation and regulation which are also tasked with ensuring information security and cyber resilience.

AP+ recommends (Rec 9):

That the Committee recommends that the obligations in the Bills be amended to remove the reporting of "attempts". Further, that the obligations and reporting timeframes proposed in the exposure draft should be aligned with those in other significant pieces of legislation (covering cyber and data breaches) such as the Privacy Act (Cth) and the Security of Critical Infrastructure Act (Cth) and APRA Prudential Standard CPS 234 Information Security**.**

Interaction of the Digital ID System with other legislation.

Privacy Act: AP+ note that on 28 September 2023, the Government responded to the Attorney-General's report on the review of the Privacy Act 1988 (Cth) by indicating that, of the 116 proposals made, it agreed with 38 of them and a further 68 in principle. Where the Government agreed in principle, it indicated that further engagement with organisations and a comprehensive impact analysis is required before it makes a final decision on the proposal.

AP+ recommends (Rec 10):

The proposed changes to the Privacy Act are individually and collectively likely to have a significant impact. AP+ is concerned however, that the changes will negatively alter the balance in the relationship between an accredited IDP and relying parties and that the proposed changes to the Privacy Act will conflict with obligations in the Digital ID legislation. AP+ would welcome the Committee recommending that the Digital ID Taskforce take a greater role in the Privacy Act Review

such that conflicts with the Digital ID laws and rules are avoided and the views of participants in the Digital ID System are duly considered as the reforms to the Privacy Act are progressed.

AML/CTF Act: AP+ supports the Government's commitment to simplify and modernise Australia's Anti-Money Laundering and Counter-Terrorism Financing (**AML/CTF**) regime. The AP+ view is that an interoperable national digital identity ecosystem is a critical component of a resilient economy. It follows that a successful national digital identity ecosystem relies on a robust and modern AML/CTF regime and has the potential to be an effective additional measure to identify, mitigate and manage money-laundering and terrorism financing risks and alignment will also protect Australian identities.

AP+ has a recommended change to the AML/CTF Act and Rules to facilitate the adoption of a digital identity capability across the economy by ensuring alignment between AML/CTF requirements and the Digital ID System.

> ***AP+ Recommendation (Rec 11):*** That the Committee recommend that the AML/CTF Act and Rules be amended such that:
>
> > a) data or a verified identity provided by an accredited IDP is considered 'reliable and independent electronic data' or a 'reliable and independent digital identity' for an AML/CTF Reporting Entity to satisfy the electronic safe harbour provisions; and
> >
> > b) that the Committee recommend that the AML/CTF Act and Rules be amended to align with the Digital ID legislation; in particular, to enable digital identities which meet a particular level of assurance under the Digital ID Bill and Accreditation Rules (e.g., Identity Proofing Level of 2+ and above), be deemed to fully satisfy the safe harbour provisions of the AML/CTF Act.

There are also other sector-specific regulations which the Government could consider modernising - notably the '100-point check' for new customers in the telecommunications sector, identity verification requirements for legal and accounting services, and the Australian Registrars' National Electronic Conveyancing Council (ARNECC) regulations for property transfers. Reforms to these regulations to enable the use of Digital ID for identity verification would improve identity resilience and also remove regulatory costs.

Attachment B: Detailed comments on the Digital ID Bill 2023

Reference	Wording	AP+ recommendations
Section 3: Objects (1)(a)	… verifying their identity in online transactions with government and businesses…	AP+ recommends that the wording of contained in Objects(1)(a) be amended to reflect the reality that Digital IDs are also used in face-to-face situations, and not just online.
Section 9: Definitions	***accredited service***, of an accredited entity, means the services provided, or proposed to be provided, by the entity in the entity's capacity as a particular kind of accredited entity	AP+ strongly recommends critical amendments to address the need for certainty around the definition of "accredited service" and how the obligations in the Bill, Rules and Accreditation Rules will apply for accredited entities who provide services both inside and outside the Digital ID System. It is currently unclear what obligations apply: to accredited entities only when they are providing accredited services inside the Digital ID System. to accredited entities when they are providing services (which are accredited services) outside the Digital ID System – e.g., through non-accredited channels. to accredited entities at all times, including when providing non-accredited services.
Section 9: Definitions *identity exchange provider*	***identity exchange provider*** means an entity that provides, or proposes to provide, a service that conveys, manages and coordinates the flow of data or other information between participants in a digital ID system.	The word 'conveys' assumes certain types of data flow which may not be applicable in all cases. Therefore, we query whether the definition of identity exchange provider is broad enough to capture ConnectID as ConnectID does not 'convey' data. This minor ambiguity could be resolved by amending the drafting to read: "...conveys, manages ~~and~~ **or** coordinates the flow of data or other information between participants in a digital ID system.
Section 9: Definitions *identity service provider*	identity service provider	AP+ raises the question whether the definition of "identity service provider", should be amended to ideally exclude identity exchange providers? We raised this question as an identity exchange provider that, as part of that exchange, "distributes" authenticators may inadvertently be caught by the definition of identity service provider.
Section 9: Definitions	***cyber security incident*** means one or more acts, events or circumstances that involve: (a) unauthorised access to, modification of or interference	The definition of cyber security incident is very broad, as the proposed definition includes "attempts" to gain access to systems, even if these attempts are blocked and unsuccessful.

	with a system, service or network; or (b) an unauthorised attempt to gain access to, modify or interfere with a system, service or network; or (c) unauthorised impairment of the availability, reliability, security or operation of a system, service or network; or (d) an unauthorised attempt to impair the availability, reliability, security or operation of a system, service or network.	AP+ supports efforts to ensure cyber resilience in the Digital ID System, however, considers that further analysis is needed to ensure the obligations for ensuring cyber resilience (including reporting) are appropriate and aligned with other significant pieces of legislation (and APRA Standards) which are tasked with ensuring cyber resilience. Large organisations such as government agencies and banks, are subject to and repel hundreds of thousands attempted attacks daily. The reporting of these failed attempts serves no purpose and will overwhelm the regulator with unusable information. AP+ considers that the reporting timeframes in the Bill should be aligned with those in other significant pieces of legislation (covering cyber and data breaches) such as the Privacy Act (Cth) and the Security of Critical Infrastructure Act (Cth).
Section 11: Meaning of restricted attribute of an individual		AP+ recommends greater clarity in the legislation and supporting explanatory materials such that there is certainty in the obligations for entities who are accredited providers operating both inside and outside the Digital ID System. With particular reference to s11, AP+ would welcome greater clarity in the legislation and supporting explanatory materials as to whether an accredited provider can pass a restricted attribute outside the Digital ID System? Further, AP+ would also welcome greater clarity in the legislation and supporting explanatory materials on whether the attribute remains restricted outside the Digital ID System?
Section 11: Meaning of restricted attribute of an individual **11 (1) (d)**	A restricted attribute of an individual means: (d) information or an opinion about the individual's membership of a professional or trade association.	One of the many future use cases for Digital ID is the onboarding of new employees by an employer, part of that process typically requires the employer (or their agent) to check qualifications. Professional memberships are a valuable personal and employment attribute – e.g., confirming an individual is a Registered Nurse or Chartered Accountant. Information about memberships is a statement of fact which an individual should be able to share (with consent) wherever they choose. Further many of these qualifications are already published and available on registers which are accessible by the public. A Digital ID System that facilitates and reflects the multiple uses of Digital ID is critical to driving uptake of Digital ID in the broader economy. Flexibility in the legislation is directly linked to the

		ability of the Digital ID System to deliver the economic and productivity benefits of Australian's being able to transact and verify ourselves using secure and trusted digital identity provider of their choice. Therefore, AP+ recommends the removal of memberships from definition of restricted attributes.
Section 19: Requirements before Accreditation Rules impose conditions relating to restricted attributes or biometric information of individuals	(2) In deciding whether to make the rules, the Minister must have regard to the following matters:	AP+ recommends that the section could be amended to include an additional consideration of whether the *disclosure* is actually required to achieve the purpose, or whether an ***attestation*** as to validity (e.g., passport, driver licence details) is sufficient.
Section 28(2): Digital IDs must be deactivated on request	The accredited identity service provider must, if requested to do so by the individual, deactivate the digital ID of the individual as soon as practicable after receiving the request	AP+ considers the drafting of this section too rigid to reflect all the permutations of a business/customer relationship and the requests an individual customer may possibly make. In practice it will be difficult for many IDPs to "deactivate" a Digital ID; particularly where that IDP provides other (non-ID) services to an individual. More typically, an ID service will be enabled for the customer (e.g., as a service inside their banking app or state government services app) and it is always within the individual's control whether to use the Digital ID (or re-enable use in the future) or not. It is likely that further controls could be implemented by the IDP at a customer's request and s28(2) should be amended to provide that flexibility. AP+ recommends the removal of S82(2) in its entirety or that the drafting be amended to read 'deactivate, disable, block or hold'. Further, consideration should be given to whether law enforcement agencies may have existing powers to direct IDPs to take certain actions which may conflict with the customer's request, in particular the deactivation obligation currently expressed in s28(2).
Chapter 3— Privacy	Chapter applies to accredited entities only to the extent the	As above, AP+ recommends amendments to address the lack of certainty around the definition of "accredited service" and how obligations in the

Section 31: Chapter applies to accredited entities only to the extent the entity 6 is providing accredited services etc.	entity is providing accredited services etc.	Bill, Rules and Accreditation Rules will apply for accredited entities who provide services both inside and outside the Digital ID System. It is currently unclear what obligations apply: to accredited entities only when they are providing accredited services inside the Digital ID System to accredited entities when they are providing services (which are accredited services) outside the Digital ID System – e.g., through non-accredited channels. to accredited entities at all times, including when providing non-accredited services.
Division 2—Additional privacy safeguards **Section 41:** Collection etc. of certain attributes of individuals is prohibited	information or an opinion about an individual's racial or ethnic origin.	The legislation should not restrict the ability to collect, use or disclose the attributes of an individual who identifies as Aboriginal or Torres Strait Islander. Further, the legislation should not restrict the ability to entities to offer the ability for individuals to be able to reflect their cultural identity in certain digital representations. There are numerous positive use cases which this capability would enable, including facilitating access to concessions such as education, banking and government services, while minimising fraudulent access to these concessions. AP+ draws attention to the work of Hold Access, an Indigenous Corporation which is supported by the Red Cross. Hold Access, via their Digital ID product (Wuna) is closing the gap on First Nations Australians digital identity. Indigenous Australians and their access to conventional forms of identification or other documentation to access mainstream public and private services is an ongoing challenge in Australia which Hold Access seek to solve via their ID product Wuna. ConnectID is also exploring how we could support the ability for Indigenous Australians (if they so choose) to have a Digital ID that also preserves the indigenous cultural identity of the individual in the digital world. Some links to the work underway by Hold Access in 2023: https://news.nab.com.au/news/nab-digital-next-how-hold-access-is-bridging-the-gap-for-first-nations-australians-in-a-digitalised-economy/

		https://www.humanitech.org.au/resources/hold-access/ Further, the restriction in s41 on disclosure of restricted attributes, should ideally be qualified so that it does not capture necessary incidental disclosure, noting that the Office of the Australian Information Commissioner (OAIC) has previously commented on incidental disclosure in photos (e.g. of people wearing turbans) or names (e.g. Mohammad) can convey race or religion.
Section 43(2): Disclosure of restricted attributes of individuals	An accredited entity must not disclose a restricted attribute of an individual to a relying party that is not a participating relying party if the accredited entity's conditions on accreditation do not include an authorisation to disclose the restricted attribute to the relying party.	AP+ strongly recommends critical amendments to address the need for certainty around the definition of "accredited service" and how the obligations in the Bill, Rules and Accreditation Rules will apply for accredited entities who provide services both inside and outside the AGDIS. S43(2) places restrictions on disclosure of restricted attributes where the accredited entity and the participating relying party are both inside AGDIS; but not clear on the application where a relying party is outside AGDIS. We recognise that many accredited entities will operate inside and outside AGDIS; and would seek to avoid a scenario where non-accredited entities may be at an advantage by not having restrictions on them. AP+ would welcome clarification in the legislation and explanatory materials that an accredited entity (IDP) can disclose a restricted attribute to a (non-AGDIS) relying party.
Section 44: Restricting the disclosure of unique identifiers	(2) The assigning entity must not disclose the unique identifier to any other entity other than: (a) if the unique identifier was disclosed to another accredited entity—the other accredited entity; or (b) if the unique identifier was disclosed to a relying party—the relying party.	AP+ has two concerns with the current drafting of s44. 1) Disclosure of the unique identifier to third party sub-contractor or service provider (Salesforce, CRM, HR Systems, etc) may be necessary in certain legitimate situations, and the current drafting prohibits that necessary action. AP+ recommends that disclosures of unique identifiers should be permitted in certain circumstances and in addition to clarifying amendments to the legislation, inclusion of these permitted circumstances in the explanatory materials will assist industry and government agencies meet their obligations. 2) AP+ queries whether this section also needs to be also expanded to enable disclosure (and on disclosure) of unique identifiers to enable interoperability between Digital ID systems (e.g.,

		Services Australia & ConnectID), not just "within a digital ID system" which is the current drafting.
Section 46: Authorised collection, use and disclosure of biometric information of individuals—general rules	An accredited entity is authorised to collect, use or disclose biometric information of an individual if: (a) the entity is an accredited identity service provider; and (b) the entity's conditions on accreditation authorise the collection, use or disclosure of the biometric information; and (c) the biometric information of the individual is collected, used or disclosed for the purposes of the accredited entity doing either or both of the following: (i) verifying the identity of the individual; (ii) authenticating the individual to their digital ID. (2) An accredited entity is authorised to collect, use or disclose biometric information of an individual if: (a) the biometric information is contained in a verifiable credential that is in control of the individual; and (b) the collection, use or disclosure complies with any requirements prescribed by the Accreditation Rules.	AP+ queries whether the addition of an 'and' or an 'or' is perhaps necessary in s46? As currently the obligations in s46(1) and s46(2) are separate and distinct. AP+ would welcome further clarity in legislation and the explanatory materials that will accompany the Bill and Rules such that it is clear that these restrictions only apply to an accredited entity in the course of providing an accredited service; e.g., where the collection or use of this information would be permitted in the course of providing other unrelated business services. AP+ notes that s46(2) is the only reference to verifiable credentials in the draft Bill. AP+ considers that this drafting may not be necessary, i.e., that the passing of biometric information under s46(1) should be technology-agnostic and apply to verifiable credentials. In the alternative, if verifiable credentials are to be excluded from s46(1), then s46(2) this setting would need to be reflected throughout the legislation).
Section 46(8): Authorised collection, use and disclosure of biometric information of individuals—general rules	(8) An accredited entity is authorised to retain, use or disclose biometric information of an individual if: (c) the information is retained, used or disclosed for the purposes of preventing or investigating a digital ID fraud incident; and	AP+ would welcome a clarification on the intended operation of s46(8). Our concern arises given the fact that fraud can happen anytime, but s48(1) requires the provider to destroy the information immediately after the verification is complete.
Section 48(1): Destruction of biometric information of individuals	48(1) the provider must destroy the information immediately after the verification is complete. (4) If an accredited entity retains biometric information of an	AP+ would welcome a clarification on the intended operation of s48(1). An accredited entity in compliance with s48(1) would not have the data to rely on s48(4) or disclose under s46(8).

	individual in accordance with subsection 46(8) (about preventing investigating digital ID fraud incidents), the entity must destroy the information at the earlier of: (a) immediately after the completion of activities relating to the prevention or investigation of the digital ID fraud incident (as the case may be); and (b) 14 days after the entity collects the information	
Section 49:		As currently drafted, s49 does not appear to clearly permit retention of source records of biometric information against which an individual requesting verification will have their biometrics assessed. AP+ notes this may be intent of s48(2), but it is not clear. AP+ would welcome a clarification on the intended operation of this section.
Section 51: Personal information must not be used or disclosed for prohibited enforcement purposes	(1) An accredited entity must not use or disclose personal information that is in the entity's possession or control for the purposes of enforcement related activities conducted	AP+ would welcome a clarification on the intended operation of s51. Does the personal information included in s51 also include the profiling information mentioned in s50(1)(b), noting that s50(1)(b) does not have a carve out for enforcement activity?
Section 52: Personal information must not be used or disclosed for prohibited marketing purposes	(1) An accredited entity must not use or disclose personal information about an individual that is in the entity's possession or control for any of the following purposes: (a) offering to supply goods or services; (2) Subsection (1) does not apply to the disclosure of personal information about an individual if: (a) the information is disclosed to an individual for the purposes of: (ii) advertising or promoting the entity's accredited services; and	s52(1)(a) includes a broad prohibition on use or disclosure of information that is in the possession or control of an entity for the purposes of supply of goods or services. This prohibits accredited entities who are also relying parties from actually using the data for provision of goods and services in their core business. AP+ agrees that where a customer has opted out of marketing and/or communication, that choice should be respected, and personal information should not be used for marketing purposes. If the intention of this clause is to prohibit the use of personal information for marketing, where a customer has explicitly opted in for this marketing, then the clause does appear to be overly restrictive. s52(2)(a)(ii) may also have the effect of restricting an accredited entity's ability to market its (non-accredited) services to customers of those non-accredited services. For example, a bank or state

		government agency may be restricted in promoting its services to its own customers, where those customers have used that bank/agency as an IDP.
Section 58: Applying for approval to participate in the Australian Government Digital ID System	(1) An entity may apply to the Digital ID Regulator for approval to participate in the Australian Government Digital ID System if: (b) the entity is: (i) an accredited entity; or (ii) an entity that has applied for accreditation under section 14; or	AP+ would welcome a clarification on the intended operation of s58. We believe that s58 allows an entity to apply for both accreditation and AGDIS participation in parallel. AP+ would be supportive of that approach.
Section 62: Conditions on approval to participate in the Australian Government Digital ID System	(c) the entity must begin to participate in the Australian Government Digital ID System on the entity's participation start day;	AP+ would suggest that the drafting of s62(c)be altered to read: (c) the entity must begin to participate in the Australian Government Digital ID System on the **agreed** entity's participation start day; There are a number of practical operational reasons that make it prudent for all parties agreeing on a suitable start date. For example, public holidays, software freezes, other conflicting legislated start dates for other regulatory obligations.
Section 75: Notice before exemption is revoked	(3) Without limiting subsection (1), the Digital ID Rules may do any of the following: provide for the Minister, on application, to grant exemptions from the interoperability obligation;	A successful national digital identity ecosystem relies on interoperability and mutual recognition of digital credentials between the public and private sector. AP+ recommend that an amendment is made to remove the power for a Minister to grant exemptions from interoperability. In the alternative, clear criteria is established on which the Minister must base their decision to grant an exemption to the interoperability obligation.
Section 85: Digital ID Regulator	The Digital ID Regulator is the Australian Competition and Consumer Commission.	A minor point, perhaps the drafting could be updated to provide flexibility to change the Digital ID Regulator (without the need for an amending Act) as the AGDIS grows in size and importance, noting that the appointment of the ACCC as the Digital ID Regulator was seen as an interim approach.
Section 86: Functions of the Digital ID Regulator	The sharing of these functions between the Digital ID Regulator and Services Australia remains under consideration	When considering the functions of the Digital ID Regulator and Services Australia, one regulatory efficiency would be the enablement of certain relevant reporting directly to Services Australia instead of the Digital ID Regulator.
Division 4: Section 128: Power to require information or documents	(2) The Digital ID Regulator may, by written notice, require the entity: (a) to give to the Digital ID Regulator, within the period and in the manner and form specified	On its face, the section does not obviously exclude transaction information or personal information. AP+ queries whether this is an intentional exclusion.

	in the notice, any such information	
Section 130: Destruction or de-identification of certain information	(c) the entity is not required or authorised to retain the information by or under: (i) this Act; or (ii) another law of the Commonwealth; or (iii) a law of a State or Territory; or (iv) a court/tribunal order (within the meaning of the *Privacy Act 1988*);	s130 requires the destruction of information obtained through the Digital ID system that an entity is not required or authorised at law to retain. Many legal purposes for use of information are not "authorised" per se by law, so it is not clear when retention is permitted. AP+ would welcome a clarification in the legislation and explanatory materials on the intended operation of s130.
Section 142: Charging of fees by accredited entities in relation to the Australian Government Digital ID System	(1) An accredited entity that charges fees in relation to its accredited services that it provides in relation to the Australian Government Digital ID System must do so in accordance with the Digital ID Rules (if any) made for the purposes of subsection (2).	s142 includes an ability for the regulator to control fees. AP+ would welcome clarity in both the legislation and explanatory material regarding how these fee controls will relate to interoperable systems, e.g., ConnectID interfacing with the AGDIS. The Bill is currently drafted to cover services provided "in relation to the Australian Government Digital ID System", and AP+ recommends the drafting be amended to cover fees related to services provided ***within*** that system. This will avoid any price decisions established within AGDIS also inadvertently impacting services of an accredited entity outside AGDIS.