Tuesday, 10 October 2023

Senator the Hon Katy Gallagher
Minister for Finance

Uploaded through the Department of Finance portal.

Dear Minister

Digital ID Bill and Rules

Chartered Accountants Australia and New Zealand (CA ANZ) welcomes the opportunity to provide its views to inform the Minister of areas of concern in the Digital ID Bill and Rules.

Our key areas of concern are outlined below with detailed feedback provided in Appendix A in the template for responses to the questions raised in the Guide to the Digital ID Legislation. We raise these areas of concern on behalf of the more than 136,000 financial professionals we represent who will rely on digital IDs to meet statutory obligations relevant to the services they provide. More details about CA ANZ can be found in Appendix B.

Varying, suspending and revoking accreditation

The draft Digital ID Bill 2023 (the Bill) and Digital ID Rules 2024 (the Rules) are silent on what happens to an individual's information when a participating party's accreditation is suspended or revoked. Further, there is currently no obligation for any participant nor the Digital ID Regulator (the Regulator) to inform Australians relying on the services of an accredited party that they can no longer, temporarily, or permanently, rely on those services.

The Bill and the Rules should require a participating party to notify its users of any change in their accreditation status, what will happen to the personal information held by the participating party and provide contact details if an individual has further queries.

Changes in name and changes in control of corporations

The Bill and the Rules are silent on how participating parties advise individuals using their services of a change in name or control of that entity. It is therefore unclear how individuals can trust that a 'new' entity is valid and is an accredited entity.

The Bill and the Rules should require a participating party to notify its users of any change in their name or control, noting the existing name and new name, when it comes into effect and contact details if an individual has further queries.

Further, the Bill only requires notice to the Regulator when there is a change of control. The incoming entity would therefore not go through the application for accreditation process, thereby bypassing an assessment by the Regulator if that entity is a fit and proper person. We consider this creates an unacceptable risk in the digital ID ecosystem.

The Bill and the Rules should require an incoming entity to apply for accreditation prior to taking control of an accredited entity.

Compliance assessments

We consider compliance assessments, not penalties, to be the critical tool to deter non-compliance by accredited parties. However, the Bill does not provide sufficient strength to compliance assessments.

The Bill allows the Regulator to require an entity to undertake a compliance assessment but does not allow for a rolling program of assessments. The Bill allows for such an assessment to be undertaken by, or on behalf of, the Regulator or by an independent assessor arranged by the entity. We strongly object to allowing the entity being assessed to appoint its own assessor as we consider, irrespective of the independence requirement, this to be an apparent conflict of interest.

The Bill and Rules should allow for a rolling program of compliance assessments which can only be undertaken by, or on behalf of, the Regulator.

Interaction with other laws

The Bill and Rules have considered existing privacy legislation to ensure the specific protections added for digital IDs build on, but do not duplicate, existing regulatory frameworks.

The implementation of the digital ID regime should also consider how a digital ID interacts with other regimes and seek changes to legislation where using a digital ID would be beneficial. For example, how digital IDs can satisfy customer due diligence in the anti-money laundering and counter-terrorism regime and how digital IDs can be relied on to access services using data transferred through consumer data right channels.

Conclusion

We welcome the establishment and expansion of the Australian Government Digital ID framework and will continue to work with the Government to ensure Australians can trust the framework to keep their personal information secure. Please do not hesitate to reach out to Jill Lawrence [redacted] to explore our feedback in greater detail.

Sincerely,

Simon Grant FCA
Group Executive
Advocacy and International Development

Karen McWilliams FCA
Sustainability and Business Reform Leader
Advocacy

Appendix A

Australia's Digital ID System

Key questions on the Digital ID legislation and Digital ID Rules

Your name	Jill Lawrence
Your organisation	Chartered Accountants Australia and New Zealand
Your email	[redacted]

Page # of guide	Question	Your response
14	What other types of Digital ID service should be included in the legislation, either now or in future?	**No comment**
14	Does the Minister's rule-making power to include new services over time provide appropriate flexibility to add new types of Digital ID services? If not, why not?	**No comment**

16	Is the Regulator's power to impose conditions on accreditation an appropriate mechanism to balance the need to provide for unique characteristics of accredited entities with the need for a consistent set of Rules for the Accreditation Scheme? If not, how can the Regulator's power to impose conditions on accreditation be improved?	**No Comment**
16	Is the application for accreditation process appropriate, or should other matters be included or some excluded?	**Whilst we consider the overall process to be appropriate, we raise two matters which in our opinion have been given undue consideration in determining a fit and proper person.** **Rules: Part 2 – Fit and proper person considerations** **5 Mandatory relevant matters** **While the matters listed are appropriate, we seek a limited previous period to look for (d) disqualification from managing corporations and (e) a history of insolvency or bankruptcy.** **We note the limited previous period of 10 years for (a) being found guilty of a serious criminal offence. This implies that mismanagement and insolvency are considered more egregious events than serious criminal offences.** **Both disqualification and insolvency events happen at a point in time and should not be taken into consideration for the life of an individual or an entity. We recommend instead that the Regulator must have regard for (d) and (e) only if they have occurred within the previous 7 years. This is in line with other timeframes within the insolvency ecosystem including eligibility for a small business restructure and the period of time a credit bureau can retain a record of bankruptcy.**

17	Are the maximum penalties for failure to meet accreditation requirements sufficient to deter accredited entities from not meeting their obligations? If not, what maximum penalties would be an appropriate deterrent?	**We consider a better tool to deter non-compliance is the proactive, rapid enforcement of accreditation requirements.** **The quantum of penalties as a deterrent should be considered alongside the likelihood of a breach by an entity being detected.** **There are some examples of ACCC enforcement that indicate that the quantum of penalties is often not a sufficient deterrent alone. Of concern is the premise that, particularly for large, profitable, businesses, penalties may simply be considered as a cost of doing business or they consider there is a low risk of being caught.** **Proactive, regular monitoring with rapid enforcement to address non-compliance can act as a deterrent and will increase the chance of non-compliant parties being caught.** **Compliance assessments should be undertaken on a rolling basis and only by, or on behalf of, the Regulator.**
21	Are the additional privacy safeguards sufficiently robust, clear and practical?	**Yes**
21	Is the rule making power to allow disclosure of biometric information to enable sharing of verifiable credentials (under specified circumstances) an appropriate exception to the restriction on disclosure of biometric information?	**Yes**
21	Is the maximum penalty for a breach of a privacy safeguard sufficient to deter accredited entities from interfering with a person's privacy? If not, what maximum penalty would be an appropriate deterrent?	**We consider a better tool to deter non-compliance is the proactive, rapid enforcement of accreditation requirements.** **The quantum of penalties as a deterrent should be considered alongside the likelihood of a breach by an entity being detected. Compliance assessments should be undertaken on a rolling basis and only by, or on behalf of, the Regulator.**

23	What is the appropriate age at which a young person should be able to create their Digital ID? What factors should be considered?	**We refer to the Government's response to the review of the Privacy Act where they have agreed in principle to proposal 16.1 that a child is an individual who has not reached 18 years of age.** **Similarly, proposal 16.2 that an entity must decide if an individual under the age of 18 has the capacity to consent on a case-by-case basis.** **We are concerned that persons under the age of 18 may not be able to provide informed consent where express consent is required under the Bill or Rules. For example, disclosure of personal attributes to a relying party or the use and disclosure of personal information to conduct testing.** **We further note that a relying party cannot make creating and using a digital ID as a condition of providing, or giving access to, a service.** **Therefore, it is unclear what the use case would be for allowing children, persons under 18 years of age, to set up a digital ID.** **Should children be given access, further protections are required.**
25	What other steps could the Government consider taking to ensure the AGDIS is ready for use by private sector relying parties and accredited entities?	**The Government must ensure that the Regulator is adequately funded and resourced to undertake a rolling compliance assessment program of participating parties and, where non-compliance is identified, to take rapid enforcement action.** **Please refer to our responses to Questions on pages 17 and 21 above.**
25	What factors should the responsible Minister consider prior to deciding to approve the AGDIS expanding into another phase?	**A key lesson to be taken from the implementation of the Consumer Data Right (CDR) is to ensure the system functions as intended before it is expanded. In the case of the CDR, even today, data transmitted over CDR channels in banking cannot be relied on as some data is duplicated and fields are missing or misrepresented.** **Prior to approving another phase, the responsible Minister must ensure that existing participants are compliant with accreditation requirements, that participants are trusted by individual Australians that are choosing to obtain a digital ID and interrogate disputes and how they were resolved to identify if there are systemic issues.**

26	How would phasing the rollout of the ADGIS affect the wider Digital ID services market in Australia?	**No comment**
27	Is the balance between voluntary use and the exceptions to voluntary use right? Are any additional exceptions appropriate?	**No comment**
27	Are the exemptions to the interoperability principle appropriate? Are any additional exemptions appropriate?	**No comment**
29	Are the protections for the Australian community within AGDIS appropriate, or are additional protections needed?	**We consider the protections in the Bill and Rules for the Australian Community to be insufficient.** **In particular, there are no protections for individuals using the services of a participating party when the party's accreditation is varied, suspended or revoked. Further, there are no requirements on the participating party, or anyone else, to inform the individuals using the services of that party of their change of status. There are also no requirements on how the participating party must ensure the continued security of an individual's information or what happens to that information if accreditation is revoked.** **Equally, where a participating party changes its name. While it is required to inform the Regulator, it is not required to inform its users. Similarly, where there is a change of control. The incoming body does not need to pass accreditation and instead merely gives notice to the Regulator that there has been a change of control. There are also no requirements to advise the customers of the existing participating party.** **For individuals using the services of such a party, how can they trust that the new name of their digital identity service provider is actually accredited?** **To ensure trust in the system, any change to the accredited party or the accreditation of a party should require immediate notification to the customers of that accredited party. That notice should outline the**

		change in circumstance, how it affects the information held about the individual and who the individual can contact for more information. **Further, to re-assure Australians that their personal information is securely protected by law, any entity seeking to stand as an accredited party offering accredited services must undertake the complete accreditation process.**
29	Are the protections for participants in the AGDIS appropriate, or are any additional protections needed?	**Please refer to our comments immediately above.**
34	Noting the pace of technological change and the need for Digital IDs to stay protected by the latest developments, how can Data Standards provide an appropriate balance between certainty for accredited entities while maintaining currency?	**No comment**
34	What would be an appropriate model for the Australian Digital ID Standards Chair and are there lessons that can be learned from the Consumer Data Right model?	**No comment.**

Appendix B

Chartered Accountants Australia and New Zealand (CA ANZ) represents more than 136,000 financial professionals, supporting them to build value and make a difference to the businesses, organisations and communities in which they work and live.

Around the world, Chartered Accountants are known for their integrity, financial skills, adaptability and the rigour of their professional education and training.

CA ANZ promotes the Chartered Accountant (CA) designation and high ethical standards, delivers world-class services and life-long education to members and advocates for the public good. We protect the reputation of the designation by ensuring members continue to comply with a code of ethics, backed by a robust discipline process. We also monitor Chartered Accountants who offer services directly to the public.

Our flagship CA Program, the pathway to becoming a Chartered Accountant, combines rigorous education with practical experience. Ongoing professional development helps members shape business decisions and remain relevant in a changing world.

We actively engage with governments, regulators and standard-setters on behalf of members and the profession to advocate in the public interest. Our thought leadership promotes prosperity in Australia and New Zealand. Our support of the profession extends to affiliations with international accounting organisations.

We are a member of the International Federation of Accountants and are connected globally through Chartered Accountants Worldwide and the Global Accounting Alliance. Chartered Accountants Worldwide brings together members of 13 chartered accounting institutes to create a community of more than 1.8 million Chartered Accountants and students in more than 190 countries. CA ANZ is a founding member of the Global Accounting Alliance which is made up of 10 leading accounting bodies that together promote quality services, share information and collaborate on important international issues.

We also have a strategic alliance with the Association of Chartered Certified Accountants. The alliance represents more than 870,000 current and next generation accounting professionals across 179 countries and is one of the largest accounting alliances in the world providing the full range of accounting qualifications.