This document contains GBG Australia Pty Ltd and Vix Verify Pty Ltd's response to the Digital Identity Consultation.

GBG is a global leader in identity data intelligence. Our solutions help organisations quickly validate and verify the identities and locations (addresses) of their customers. Our products combine access to an unparalleled breadth of data from over 150 global partners with GBG's market-leading technology, used by some of the best-known organisations around the world. Our innovative technology can verify and authenticate the identities of people globally, helping organisations to improve digital access, protecting them from fraud and creating fast, secure and seamless customer experiences that build trust. We specialise in layering multiple data sets through API based services to provide organisations confidence on the quality of data they are matching against and the robustness of the decisions that they make. We have more than 30 years' experience in technology innovation and are at the forefront of the digital economy.

In Australia, we were the first private sector organisation to access the Australian Federal Government Document Verification Service (DVS) comparing identifying information with a government issued record. Our products and services enable our customers to prevent and detect fraud and to meet their compliance obligations.

We are grateful for this opportunity to provide input on the Digital Identity consultation and we would be delighted to discuss any of the points in this response with the Australian Digital Transformation Agency at any time or to provide our views on how data can benefit the Australian digital economy.

We are submitting high level responses to certain questions only at this stage, with a view to providing more detailed feedback once the draft legislation is published.

GBG responses:

Question 4: Are the proposed obligations on relying parties described reasonable? Should there be any additional obligations?

We broadly agree with the requirements on relying parties and we agree that the legislation should not regulate the services that they provide once an individual has verified their identity. However, to avoid duplication, we recommend limiting any notification obligations to fraud or security issues which do not constitute a notifiable breach under the Privacy Act 1988.

Question 6: Does the Legislation need to include a definition of Digital Identity information, or is it preferable to rely on the definitions of personal, sensitive, or protected information in other Commonwealth Acts?

We are agnostic as to whether a new definition is developed or whether definitions in existing Commonwealth Acts are relied on. However, what is critical is that existing definitions, for example in the Privacy Act 1988, are updated where necessary to encompass technology and/or digital identity attributes that have been developed since the relevant legislation was enacted.

Question 8A: What factors should be considered in the development of the liability framework?

We agree that Participants should not be liable in circumstances where they have complied with the rules and requirements of the system. We also think it is important that Participants are not penalised twice for the same issue and, as such, the liability framework should not contemplate penalties in circumstances where a Participant is subject to a compensation claim under a section 52 Privacy Act declaration. It is also important that the liability framework takes into account the limited ability for

private sector Participants to negotiate liability terms with government bodies which act as data providers and that it apportions liability accordingly.

Question 8C: What remedies and/or redress should be available to aggrieved Participants and Users for loss or damage suffered as a result of their use of the system?

Perhaps the most equitable remedy (given the other potential liability claims a Participant or User may face under existing legislation such as the Privacy Act 1988), would be for Participants or Users who are found to have knowingly breached the system rules and requirements to suffer an increase in the charges payable by them to continue to use/access the system? This could follow an insurance premium type model.

Question 9A: Should the proposed privacy and consumer protections listed above be enshrined in primary legislation?

In our view, given the existing privacy protections in the Privacy Act 1988, it would be overly cumbersome and reduce the ability to make changes in a timely manner if the privacy and consumer protections were enshrined in primary legislation. Including these protections in the operating rules or policies should suffice, particularly if there are consequences for Participants and Users for knowingly breaching them under the liability framework.

Question 10A: Should the Legislation include rules around the extent of choice available to users to verify their identity?

We do not think this would be appropriate. The role of legislation should be limited to the digital identity framework itself and should not prescribe the mechanisms available to verify identity. That should remain a decision for the relevant relying party. Consumers still ultimately retain control as, if they do not agree with the mechanism selected by a relying party, they can purchase the relevant goods or services from a different relying party.

Question 10B: Should any types, or all types of relying parties be obliged to provide an alternative identity verification mechanism and what exceptions should be available?

As per answer 10A above, this should be a decision for the relying party to make. The legislation should not impede relying parties from making appropriate commercial decisions, based on their size, industry and risk appetite.

Question 11B: Should a public register of Attributes be maintained?

Based on the information in the consultation paper, we cannot see the benefit of creating a public register and do not think it would be positively viewed by consumers, given the likely privacy concerns. It would also be difficult to administer such a register, ensure it was stored and accessed in a way that meets privacy requirements and is kept up to date.

Question 14A: Should the Legislation specifically provide a mechanism requiring an individual's consent before the User transacts with a relying party?

Question 14B: Should the Legislation specifically provide an opt-out mechanism enabling individuals to opt out of the system after they have created a Digital Identity?

Yes, we would support both mechanisms being enshrined in legislation as we think it would be clearer for all parties and would remove any ambiguity.

Question 16: How should the Legislation cover situations where a person lacks capacity, is not capable, is too young or lacks interest or motivation to engage personally with the system?

If an individual lacks legal capacity and has a nominee appointed under law, such as a guardian or attorney, then it is appropriate that the system permits such guardian or attorney to represent that individual. However, we do not think it is the role of legislation to try to cover circumstances where an individual lacks "interest or motivation" to engage with the system. The rules and requirements of the system which will bind Participants, Users and relying parties should provide sufficient safeguards to such individuals without the need to cater specifically for them in legislation. An additional safeguard is the voluntary nature of the system.

Question 17: Should the requirement for a PIA remain in TDIF accreditation requirements or should it be required in the Legislation or Operating Rules?

We believe that it is sufficient and in accordance with the Privacy Act 1988 for PIAs to remain a TDIF accreditation requirement.

Question 30: Should the Legislation specify whether and how audit logs from the system can be used in court as evidence? If so, what should the Legislation say?

Our view is that audit logs from the system should be treated in the same way as any other electronic source from government websites.

Question 32: Should the Legislation specifically provide that additional administrative decisions relating to the system be subject to merits review?

Yes, this would make sense if a specialised review body (with appropriate digital identity knowledge) conducted any such merits review.