16 July 2021

Mr Jonathon Thorpe
General Manager
Digital Identity
Australia

Email: digitalidentity@dta.gov.au

Dear Mr Thorpe

Re: Digital Identity Legislation: Positions Paper

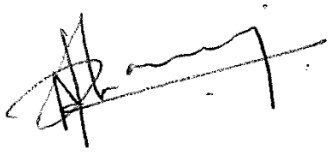
The Australian Financial Markets Association (AFMA) welcomes the opportunity to comment on the Digital Identity Legislation positions paper. AFMA's membership consists of over 110 financial market participants that together provide the whole range of financial services to both the public and private sectors and employ some of the most sophisticated technological, information and security resources.

Banks have long been the largest investors in identity management technology and services. Robust digital ID systems have tremendous value in the provision and security of digital financial services. Bank-developed digital IDs have been and are expected to continue to be some of the most frequently used ID services in the world and we understand a number of our members are developing solutions.

We welcome the development of a whole-of-economy digital identity system that supports innovation, interoperability, consumer choice and is markets-based. Our comments below elaborate our response to the proposals, and we trust they are of assistance.

Please feel free to contact us for more information via the Secretariat.

Yours sincerely



Nikita Dhanraj
Policy Manager

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7907 Email: secretariat@afma.com.au Web: www.afma.com.au

The structure and scope of legislation

Rational approach to legislation

A legislative environment that is conducive to innovation and the fast-growing needs of business and consumers is necessary for improving the competitiveness of the Australian economy. AFMA welcomes the aim to provide certainty via legislation whilst remaining flexible enough to allow for technological developments and innovation over time. We also appreciate it is not intended to apply to all digital identities and digital identity systems in Australia.

However, we flag that legislation should be principles-based and aim to achieve specific outcomes rather than prescribing approaches to developing practices to reach those outcomes.

We caution that the experience by industry of the Consumer Data Right should be considered to avoid the high-cost outcomes of that scheme, and its associated heavy demands on Government resources.

To ensure flexibility, process designs and operational solutions under the Trusted Digital Identity Framework (TDIF) should be the product of industry standards and operating rules that do not need parliamentary sanction to amend. These rules should be co-designed by public-private collaboration to ensure they align with industry best practice, support innovation and can be modified efficiently to meet changing needs. More detailed matters of the technological development of digital identity schemes, business models and ownership provisions can be addressed through contractual arrangements.

The contractual arrangements in payments systems should be considered in this regard. The scheme rules of each payment system function as a contract between members of that payment system and between each member and the operator of the payment system. While legislation, common law and industry codes guide the development of contracts, the nature of each scheme, including the benefits and risks to each party, depend on the content of their principal contracts. In recognition of certain contractual arrangements, legislation in turn implies certain basic warranties and terms in consumer payment facility contracts. For instance, the ASIC Act implies into any such contract a warranty that the services will be provided with due care and skill.[1]

We also note that private identity providers (IDPs) may service some transactions through a TDIF-mandated exchange (or by other means to a TDIF relying party), while at the same time servicing many other private transactions. We support that the latter type of transactions should not be captured merely as a consequence of being on the Participant Register.

Definitions

AFMA agrees that the distinct information included in a Digital ID would be useful to clearly identify and to ascertain which information will be subject to the legislation and rules. This would provide

[1] ASIC Act 2001 – Section 12ED

direction to participants on the specific identity requirements for building their systems' frameworks, technology and policies.

We support that the definition will reference personal or sensitive information as defined in the existing Privacy Act as this would allow digital identity systems that do not operate under the proposed legislation to give consumers the same level of privacy protection.

We note the potential plans to list the core attributes in the TDIF rules as non-exhaustive examples of digital identity information (family name, given name and date of birth). However, we caution against any bespoke prescription as the information that comprises digital identity information will evolve over time. Given this and in the interest of maintaining consistency between the digital identity legislation and the Privacy Act, the legislation should aim to elaborate on how the Privacy Act is applied in the digital identity system.

In terms of defining the digital identity system, we support a more technology-neutral approach. We caution that the proposed description of the system by referencing the identity exchange managed by Services Australia in the definition of system, risks including a particular technological approach. This approach also risks setting the provision of identities around one government-operated exchange in contrast to others that might exist in the private sector.

Regulatory oversight of the system and TDIF Accreditation system

AFMA notes the legislation aims to ensure that TDIF-accredited bodies can rely on accreditation to build trust in their systems without being subject to the entirety of the legislation. We support this proposal of TDIF accreditation, as it takes a rational approach to lowering inefficient legislative burdens.

Relying party on-boarding

We note the paper allows relying parties to apply to the Oversight authority to on-board to the system without TDIF accreditation. We do not support this proposal. Accreditation will be an important measure for enforcing standards around data management and preventing misuse of data. Consequently, dynamic accreditation will be necessary for de-accreditation in the case of negligence or a data breach by a relying party.

The paper states a number of potential obligations on relying parties. In light of our concern above, we note there are several noteworthy gaps, which should be considered for inclusion as additional obligations, including:

- Standards on storing data;

- Requirement to delete ID data that a customer requests; and
- Requirement to purchase cyber insurance to cover the risk of a data breach.

Participant Register

AFMA supports that accredited participants should be required to check a relying party's status on the register before sharing data with them. In an effort to minimize the risk of consumer harm, we suggest the status be updated in real-time.

For example, consider a situation where a participant becomes aware of a data breach by a merchant on a Monday morning. If the register is updated daily, the participant will be able to send customer data to the relying party until the following day when the status is updated, and the merchant is de-accredited. In this example, a one-day period exposes consumers to potential harm.

Oversight Authority

AFMA notes that the Oversight Authority with roles including accreditation, enforcement of compliance and administration of sanctions will face conflicts of interest that need to be carefully managed. We are supportive of the separation of the policy making functions to be held within departments advising the Minister. We support that rulemaking by the Minister should sufficiently draw on private sector expertise and industry practices to meaningfully reflect the interests of participants in the system. Consideration should be given to how any residual conflicts can be structurally addressed where possible.

Data and Data Breaches

AFMA supports the need for a consistent approach by Government agencies, departments and schemes to the sharing and use of data. We endorse an approach that empowers data subjects in a manner that is consistent with the CDR regime. We agree that the scope of data sharing between Participants needs to be clarified.

AFMA welcomes the proposal that any notification to the Oversight Authority should simply be a copy of the notification to the OAIC under the Notifiable Data Breach threshold assessment, which are similar to CPS 234 Information Security requirements, and that inquiry and investigation powers should remain solely with the OAIC. We agree that the Notifiable Data Breach (NDB) scheme in Part IIIC of the Privacy Act provides a well-defined process applicable to APP entities and consistency with it should be upheld for non-APP entities covered by the Digital Identity legislation.

For APP entities who will also be subject to the proposed Bill, notification of data breaches or cyber security incidents under the NDB scheme will be subject to an assessment to be conducted in less than 30 calendar days. AFMA supports that it is important that the proposed Bill does not add another layer of complexity that may affect these timeframes.

Governance – Advisory Boards

AFMA notes legislation will enable the Minister to appoint an independent Oversight Authority as a statutory officeholder to regulate the non-privacy-related provisions of the Legislation. AFMA supports establishing one advisory board, with subdivisions to advise on technical areas. We highlight that the board should seek to consider and balance various industry issues and concerns when providing advice to the Oversight Authority.

To support transparency, AFMA holds that decisions of the advisory board should be published, including occasions where the board fails to reach consensus on specific matters. Additionally, decisions of the Oversight Authority should reference advice provided by the advisory board, and where decisions contradict that advice, the Oversight Authority should provide a rationale for departing from the advice provided.

We note that non-accredited participants will not be governed by the Oversight Authority. In the interest of more clarity, the industry would benefit from understanding how accredited and non-accredited entities connect with each other.

Governance – Step-in powers

The paper provides that the Oversight Authority should have "step in" powers to allow it control the off-boarding Participant's exit process where the it reasonably determines necessary for the integrity and security of the system. AFMA notes that this should be fulfilled by a dynamic registry that is attached to an exchange, as IDPs will not see which relying parties are requesting data.

Privacy Impact Assessments

AFMA does not support the mandatory requirement of an external provider for Privacy Impact Assessment (PIA). Many firms have built considerable internal capability and frameworks to allow PIAs to be conducted in-house. The OAIC's own guide to PIAs does not require that they be conducted independently, and suggests it is helpful to make use of various 'in-house' experts available, such as the privacy officer or equivalent. A requirement for mandatory external providers would create inefficiency by unnecessarily adding to costs without benefit.

Privacy and Consumer safeguards

AFMA strongly supports that the privacy protections provided in the Privacy Act should take precedence and the digital identity legislation should reference the content of the Privacy Act and elaborate its application. As noted above, not all digital identity schemes will be captured by the

proposed digital identity legislation. The Privacy Act provides protections around biometric personal information and sensitive information which should allow similar provisions anticipated in the proposed legislation.

The highly complex and costly to implement outcomes of the Consumer Data Right in relation to privacy are to be avoided. A single consistent Privacy Act based approach is preferred.

The legislation should also account for the requirements around consent management in the Privacy Act. The Privacy Act requires personal information to be destroyed or de-identified once it is no longer needed for its permitted purposes and there are no other laws requiring its retention. Further, AFMA understands the current review process considers the right to erasure of a consumer's personal information reasonably shortly after requested. Such erasure rights could be a safeguard in addition to strengthened consent requirements by providing a mechanism for withdrawing consent if consumers are no longer comfortable with an Australian Privacy Principles entity collecting, using or sharing their personal information.

The paper appears contradictory on this matter. We are unclear if this is to be a law mandating a retention requirement (which would be relied on with regards to the Privacy Act) or whether it is just repeating the principle (APP 11.2) that the Privacy Act already covers.

We welcome that the paper acknowledges the Government is undertaking a review of the Privacy Act and support that legislation would recognise the potential changes being made to broader privacy protections as a result of the review. There should be sufficient clarity and no duplication in regard to data-related expectations. Updating the Privacy Act to be a single, known and consistent source is entirely the correct approach.

Further, we note the paper puts forth eight safeguards for the collection and management of biometric data. While the safeguards are sound in principle, we note that the industry may face some difficulties. For example, fraud activities would generally occur after biometric data is deleted and measures designed to assist investigators of fraud are likely to have little effect. AFMA supports further engagement with industry participants for better understanding of some of these practical challenges.

Need for consistent legislation and requirements

We note that lack of consistency in the legislative framework would cause operational and legal complexities and create unfavourable conditions for entry and participation in the digital identity system. Inconsistency can also make it hard to understand what protections are applicable to users' information. System-specific privacy protections and consumer safeguards risk creating multiple layers of legal and regulatory obligations over and above the requirements by the Privacy Act and the Consumer Data Right. For example, in Open Banking, there is a requirement that consent be informed, time-limited and specific to a purpose.

We strongly support a whole-of-economy analysis of existing requirements around these matters and potential alignments to them instead of newly enshrining similar provisions in law and risking costly duplication.

Transaction History Log

AFMA agrees that particular requirements around metadata should be clarified. Given this contradicts other requirements around retention and record keeping, it would be important to align with other legislative requirements.

The paper proposes that the rules will require identity exchanges on the Participant Register to provide Users with a centralised view of their metadata, specifically, the relying party's services the User has accessed; the date and time of access; and the categories or types of attributes passed to the relying party.

We do not support the proposal that the exchange should be collecting or presenting consents for the following reasons:

- It involves the exchange collecting personally identifiable information in a centralised way;
- It is not clear what user interface will be available to the user (e.g. would they have to download an additional application?); and
- It is not clear whether they can manage consents at the exchange level instead.

Penalties and Enforcement

We agree that the purpose of civil penalties is to ensure that Participants comply with their obligations to assist individuals in dealing with identity fraud and cyber security incidents. AFMA strongly supports that the penalty regime should not be set in line with penalties already in the system where these are disproportionate and punitive. Penalties in some regulatory areas no longer conform to the Murray Financial System reviews recommendation against extreme penalties.

AFMA draws the DTA's attention to the experience in the Australian regulatory context. We note that 'responsive regulation' within single agencies or authorities will be highly likely to fail. This is due to the inherent conflicts of interest in a single body that is responsible for investigation, prosecution, policy setting and industry support. It is critical that these functions be separated to avoid the progression of the 'responsive' model into a punitive regulatory stance. In the long term this is the most important element to get right to avoid the damage to the economy that punitive regulation can cause.

As noted above, the various functions of the Minister, the Oversight Authority, OAIC and other parties in the governance framework of the digital identity system should be structured in a way that appropriately manages conflicts between rulemaking, accreditation, enforcement of compliance, administration of sanctions and penalties. To that effect, AFMA suggests that any civil enforcement

proceedings should have the conflicts of interest managed by having these decisions reached at through independent deliberation modelled on the likes of the Director of Public Prosecutions (DPP).

Charging framework

AFMA agrees with the position that competitive neutrality principles would apply to ensure the government would not enjoy competitive advantages over private sector companies. We support competitive neutrality principles, specially also considering that charges should promote inclusion, enable affordability for Users and relying parties, and incentivise adoption.

The charging model should also provide clarity for private sector decision-making about investment in digital identity initiatives. AFMA holds that it should be established in alignment with existing Government policy to ensure that the commercial framework does not discourage investment in private sector solutions.

The paper states that Participants should be charged fairly, and charges set according to the value and complexity of the services provided. We welcome this as it acknowledges the need for charging to be adaptable and scalable to precisely account for market rates, feature enhancements, and changes in demand.

We support the ability of Providers to set prices based on market principles where provisions are not standardised (e.g. provision of certain credentials).