Australian Banking Association

17 December 2020

Department of Senate
PO Box 6100
Parliament House
Canberra ACT 2600
via email: fintech.sen@aph.gov.au

Dear Senator Bragg

Senate Select Committee on Financial Technology and Regulatory Technology

The Australian Banking Association (**ABA**) is pleased to make this submission to the Senate Select Committee on Financial Technology and Regulatory Technology (***the Committee***) in respect to the Issues Paper released in November 2020 (**Issues Paper**).[1] The ABA has previously considered several matters raised in the Issues Paper; including issues relating to data security, Consumer Data Right (**CDR**), Digital ID, and privacy. Therefore, this submission will take the opportunity to bring to the Committee's attention that policy work.

1. Data Security

FinTech is a term given to the functionality that banks have been at the forefront of developing for decades – telephone banking, internet banking, EFTPOS, BPAY, NPP are examples. ABA members actively develop or support independent third-party technology solutions so that customers can access new, secure, and competitive banking products. Australians are increasingly choosing to undertake their banking via their bank's digital banking channels, making Australian banks the largest developers and users of FinTech. The FinTech solutions which banks implement are done so in accordance with the Australian Prudential Regulation Authority (**APRA**) and the Australian Securities and Investments Commission (**ASIC**) security requirements.

The significance of financial services has been identified by the government in designating it a critical infrastructure sector. The proposed amendments to the *Security of Critical Infrastructure Act 2018,* would require owners of critical assets in this sector to maintain a rigorous all-hazards approach to manage the security and resilience of their assets. Further, specific regulation would apply to data processing and storage service providers in recognition of the critical nature of this service in its own right, highlighting the significance of data protection and technology security in the banking system.

Therefore, when considering the regulatory setting to enable FinTech[2] it must be borne in mind that FinTech will operate within the context of banking as critical infrastructure, with significant regulatory requirements for banking systems and data. The ABA strongly recommends that any considerations which will liberalise the banking value chain by enabling execution of some functions by non-bank entities or individuals must first be passed through the lens of the objectives of the Reserve Bank and financial regulators so that security, safety, and privacy standards are maintained.

[1] Select Committee on Financial Technology and Regulatory Technology, Second Issues Paper, (Link)
[2] Per the Committee's intention to ensure 'the settings are optimal to encourage and support Australian FinTech and RegTech businesses.' Source: Select Committee on Financial Technology and Regulatory Technology, Interim Report, Sept 2020p. xiii (Link)

Australian Banking Association

2. Consumer Data Right

In respect to the CDR, the Issues Paper seeks comment on obligations of entities as Accredited Data Recipients and options for the future inclusion of further sectors in the CDR. The ABA has made several submissions which address these points. For brevity, three pertinent points will be outlined in this submission.

First, on the question of future sectors for designation, the ABA is of the view the CDR should be permitted to develop in accordance with consumer and market demand. The current process for the designation of future sectors is opaque. The ABA has previously recommended that the Department of Treasury 'undertake public consultation on potential sectors to be considered for sector assessment. This will support a demand driven expansion of the CDR.'[3]

Second, in respect to the question of a competitively functioning CDR, the ABA holds reservations about the way in which the siloed and sequential development of the CDR through the sectoral designation process will slow the development of the nascent data economy. The ABA has consistently recommended that data reciprocity must be invoked for a truly competitive CDR to evolve. The ABA submission to the *Inquiry into Future Directions for the Consumer Data Right* recommended: 'All participants who are prepared to use consumer data via the CDR regime should be required to reciprocate, irrespective of whether those entities are within a designated sector. The principle of reciprocity will ensure all participants are incentivised to deliver the right outcome for consumers.'[4]

Finally, the ABA supports the Committee's recommendation 'the Australian Government establish a new national body to consolidate regulatory responsibilities in relation to the implementation of the Consumer Data Right.'[5] Whilst an effective governance structure may not resolve all issues within the CDR, if done correctly, it will enable a more efficient process for the escalation and resolution of issues. The ABA notes there will soon be five[6] government or overseeing authorities that participants will need to navigate in determining what to build for the CDR. The CDR will be the responsibility of the Department of Treasury (CDR Rules, Sector designation), the ACCC (CDR Enforcement), the Data Standards Body (the CDR technical standards), the Office of the Australian Information Commission (Privacy Regulator), and AFCA (consumer complaints). It is inevitable that the CDR will be challenged in achieving its full potential without a single point of accountability to drive the growth and future direction of the CDR.

Appropriate evolution of the CDR

Some of the recent draft Rules proposed by the ACCC have the potential to negatively impact on the security of consumers banking data. An example is the draft CDR Rules[7] which provide the ability for unaccredited individuals and entities (referred to as Trusted Advisers) to access a consumer's banking data. Trusted Advisers are not required to attain CDR accreditation, nor are they obliged to adhere to the bank data security requirements per APRA's CPS234.[8] The ABA opposes this particular weakening of the controls and security in the CDR. Consumer confidence is key to the success of any initiative in the data economy, if consumer trust is lost, then the ambitions of the CDR will not be achieved.

The Issues Paper also seeks comment on prospects for the CDR, including regarding potential linkages. Consideration should be given to expanding the CDR regime to the Australian Taxation Office (**ATO**). Under such an arrangement, those applying for credit products may elect to share data such as their PAYG income tax or BAS information with credit providers. Potential borrowers could provide consent to credit providers to access this information from the ATO, instead of being required to source and supply their individual pay slips or tax returns as part of an income verification process. This will help to streamline lending processes and quickly facilitate innovation, efficiency and competition.

[3] ABA Submission, Treasury Laws Amendment (measures for a later sitting) Bill 2020: amendments of the consumer data right (Link)
[4] ABA Submission to the Inquiry into Future Directions for the Consumer Data Right, 21 May 2020 (Link)
[5] Select Committee on Financial Technology and Regulatory Technology – Interim Report, September 2020 p.viii (Link)
[6] There are currently four active entities responsible for elements of the CDR.
[7] ABA submission on the proposed expansions to the CDR Rules 2020 (Link)
[8] At the time of writing this submission, the final Rules which include the treatment of the Trusted Adviser model had not been released.

Australian Banking Association

3. Digital ID

The Government has laid out a forward-looking vision for how digital identity services could be used to improve government service delivery and bolster privacy protections for citizens.[9] The Digital Transformation Agency is seeking to extend the Trusted Digital Identity Framework (**TDIF**) beyond federal government agencies, to state and territory agencies and the private sector. Collaboration between government and the private sector will be beneficial for all parties, including Australian consumers and businesses. Banks are actively exploring digital identity initiatives and are open to collaboration with the government towards a digital identity ecosystem.

The interests of the Australian economy will be better served if there is flexibility to innovate and respond to the needs of consumers and businesses, instead of establishing a single government digital identity scheme. Government can also achieve genuine collaboration with industry without legislation. As such, the intended scope and coverage of the proposed digital identity legislation should be limited to areas where parliamentary authority is explicitly required for the extension of the TDIF. Matters that go to the operation of solutions within the TDIF are best left to operating rules and industry standards. Prescribing such matters in legislation may hamper the development of future digital identity schemes or reduce the incentives for private sector to become participants of any government digital identity system.

In addition, where rules and standards are being created for digital identity solutions (whether or not they are TDIF-accredited), the Government should co-design these rules with the private sector to ensure that they align with industry best practice and do not hamper innovation.

The ABA has also recommended that Digital ID information should be dealt with under the *Privacy Act*, rather than establishing a bespoke Digital ID privacy regime that can diverge from the *Privacy Act* over time.[10]

4. Overall regulatory framework for Digital Economy policy

The ABA's recent submission to the Attorney-General's Department review of the Privacy Act highlighted concerns with the number of overlapping government data-economy reforms and initiatives currently underway. If not co-ordinated or consistent in approach the multitude, complexity, and reach of each of the proposed reforms present a significant risk to Australia achieving a clear and consistent regulatory structure for the data economy. The ABA noted in the submission to the review of the *Privacy Act* (Cth) *1988*: the following initiatives:[11]

Consultation	Government Department/Agency
Privacy Act Review	Attorney-General's Department
Cyber Security Strategy 2020	Department of Home Affairs
Inquiry into the Future of the CDR	Department of Treasury
CDR Rules Version 2	Australian Competition and Consumer Commission
Data Availability and Transparency Bill	Office of the National Data Commissioner
AI Action Plan for all Australians	Australian Government Department of Industry, Science, Energy and Resources
Digital Identity	Digital Transformation Agency

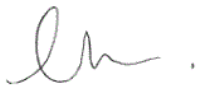
[9] See for instance Minister Stuart Robert's speech to the Digital Transformation Agency Digital Summit 2020: "Digital government: delivering in the post-COVID world" (link)
[10] The ABA submission to the Digital Transformation Agency's consultation on digital identity will be available from late December on the ABA website.
[11] Source: ABA Submission to the *Privacy Act 1988* (Cth) Review (link)

Trusted Digital Identity Framework	Digital Transformation Agency
Review of Retail Payments	Reserve Bank of Australia
Review of the Australian Payments System	Department of Treasury
Australia's third National Action Plan	Office of the Australian Information Commissioner
Australia's second Open Government National Action Plan	Office of the Australian Information Commissioner

The ABA urges the development of an overarching strategy for data and information privacy to underpin the transition to a digital economy and provide a consistent framework for future reforms. Co-ordination will be critical to achieve the intended outcomes.

The data economy has the real and exciting potential to generate jobs and opportunities for servicing the needs of all Australians. Technology and digital capability are the mechanisms by which banking will continue to develop. Banking is built on the principles of prudence, safety, and security. It is imperative that those involved in the provision of banking services whether licensed as banks or non-bank FinTechs, are held to these same standards for the benefit of the economy and Australians.

Yours sincerely



Emma Penzo
Policy Director
Emma.Penzo@ausbanking.org.au