25 05 2020

Secretariat
Inquiry into Future Directions for the Consumer Data Right
The Treasury
Langton Crescent, Parkes ACT 2600
data@treasury.gov.au

Westpac Place
Level 19, 275 Kent St
Sydney NSW 2000
westpac.com.au

Re: Inquiry into the Future Directions for the Consumer Data Right

Dear Sir/Madam

Thank you for providing an opportunity for comments on the issues paper 'Inquiry into Future Directions for the Consumer Data Right' (**the issues paper**).

Westpac Group (**Westpac**) supports the introduction of a Consumer Data Right (**CDR**) in Australia and we agree that the passage of the legislation in 2019 paves the way for an even more convenient, competitive and customer-centric financial services sector. We support placing customer data in the hands of the customer and enabling them to better control and direct where their data is transferred in a safe and secure way.

Westpac continues to make good progress towards the scheduled go-live date. We have been working very hard to meet the testing requirements that the Australian Competition and Consumer Commission (**ACCC**) had set out and appreciate the constructive and flexible approach the ACCC has taken to managing the overall delivery. We consider that thorough functionality and penetration testing of the ecosystem will continue to be crucial before customer data is allowed to flow through it.

Westpac has sought to lead the delivery of CDR across the industry and has worked collaboratively and consistently with the ACCC and Data61 to ensure the Rules and Standards are finalised to progress implementation. We believe that, if executed well, the regime has strong commercial possibilities.

We therefore welcome this second review and expect that an expanded CDR – if executed well – will further enhance the benefits to customers. We have directed this submission to this 'key focus' of the issues paper.

> Westpac supports enabling customers to better control and direct where their data is transferred in a safe and secure way. The sensitive nature of this proposed reform, involving as it does the transfer of data between parties, including third party write access – underlines the caution needed. We recommend that the first stage of the CDR is bedded down before expanding the scope.
>
> Critically, if write access is eventually enabled, particularly for payment initiation, there must be very robust security protocols as well as clear protections for customer data and customer funds.

Any expansion of the CDR should proceed on the basis of three key principles:

1) Security – if write access is enabled, particularly for payment initiation, the security protocols need to be even more robust for the system to be trusted by all parties and for data to be kept secure;
2) Reciprocity – all players should be required to compete on an equivalent basis to ensure the stability of the CDR ecosystem; and
3) The right time to expand CDR – this will be dependent upon the current CDR roadmap and other critical developments (*e.g.* digital ID, consent frameworks *etc*.).

Summary of Recommendations:

Recommendation 1: In a 'third party access' environment, authorisation (granting of consent) should have multi-factor authentication and all write actions should be authenticated (*e.g.* enter a One Time Password every time a payment is sent).

Recommendation 2: The existing protections should be reflected in any amendments relating to write access, *i.e.,* participants should not be held liable for unauthorised or fraudulent modifications provided they comply with their own obligations under the regulations and additional protections should be introduced given the liquidity risks of non-Authorised Deposit-taking Institution participants. Similarly to the current regulatory regime where the Accredited Data Holder (ADH) or Accredited Data Recipients (ADRs) could be held directly liable to the consumer, the consumer should have the ability to directly claim against the third party provider including in the event of fraudulent or inappropriate drawing on the account. Further, there should be a meaningful capital and/or insurance requirement for third parties, well above the existing requirements for read-only.

Recommendation 3: Deep and broad consultation within the banking sector and with CDR participants must occur in order to develop proposed consent taxonomies.

Recommendation 4: The two regimes (digital identity and CDR) should be dealt with separately but it is imperative that they are interoperable.

Recommendation 5: Accreditation at any level – including for intermediaries and third parties – should at the very least meet the same high standards around security, privacy and the need for consumer consent as currently exist under the regime, with the expectation of additional more stringent requirements for those seeking write-access. Different accreditation obligations may be useful to distinguish between the different risk profiles associated with different activities, however there should be no relaxing of obligations concerning security, privacy and consumer consent.

Recommendation 6: To balance the need to encourage competition with the need to ensure that the competitive landscape is not distorted and for all participants to compete and innovate, we recommend:

- accreditation criteria that include, at a minimum, an obligation for ADRs to also provide write access to their equivalent data sets in order to develop a product or service, where the consumer has consented to write access or where write access is permitted; and

- to ensure the barriers to entry are not too high, an exemption to the obligations of reciprocity for small business and start-ups that meet each of the following: (a) have an annual turnover of less than $10 million in the most recent previous financial year; and (b) have fewer than 100 full-time equivalent (FTE) employees; and (c) less than $3 million total debt to all credit providers, on a group-wide basis.

Recommendation 7: Expansion of the CDR to write access should not be legislated until a full post-implementation review of the current program has occurred – this should only take place once Phases 1 and 2 of the current program have been embedded.

Recommendation 8**:** To ensure that write access provisions do not pose a risk to the financial system, we recommend that the existing Know Your Customer (KYC) rules should be retained where write access is allowed for the purposes of opening an account on behalf of a customer.

Recommendation 9: Any write access ecosystem must guarantee, through appropriate consent and liability frameworks, at least the same strong privacy protections and fraud protections that the current read access environment provides.

Recommendation 10**:** Every field should be assessed against a risk matrix before write access is permitted on its own or in combination with other fields.

Recommendation 11**:** Any addition of payments within an expanded CDR should mandate the process needed to authenticate the transaction on the customer's behalf, but not the mechanism – the industry should be permitted to innovate.

Recommendation 12**:** The liability framework should be robust and third parties operating new 'payments' technologies within a write access regime should bear the liability. Aligned to our comments on accreditation, there should be a higher bar for those seeking write-access than those seeking read-only access to ensure a safe and efficient ecosystem.

1. Security

As we have previously noted, loss of funds due to fraud is one thing but a stolen identity or the impact of other breaches to customer privacy, including personal safety, can be permanent and debilitating. It is therefore essential that the move towards a CDR occurs in a manner that ensures customers are protected while still meeting their appetite for data-sharing. The risk is much higher when money can be moved in real-time, so the security and liability rules need to be commensurately stronger.

The security of the ecosystem is the lynchpin to the success of the CDR, as Deloitte has noted following a survey of 2007 retail bank consumers:

> For the Consumer Data Right to work effectively people will need to trust their bank (the data holder), the party receiving the data (the accredited data recipient) and the government accreditation process. When trust is missing from any one of these players, people are less willing to share data.[1]

Further, their survey revealed that:

> ...when we look at relative levels of trust, we trust the four major banks more than we trust any of the other types of organisations to keep our money safe.[2]
>
> *and*
>
> Digital banks, despite being regulated and supervised like other banks, were trusted by only 10% of people, and distrusted by 29%.
>
> …Technology companies, often seen as the source of potential competition for banks, have the lowest net prudential trust score. They were trusted by only 9% of people, and distrusted by 32%.[3]

We would argue that these findings underscore the need to ensure that the CDR ecosystem is robust – in other words, there should be no relaxation of standards in the name of lowering the bar to entry, given the risk to consumer trust in the system.

Attached to this submission is an Appendix (**Appendix 1**) which outlines some additional security controls from the current baseline to protect data in read and write access. Below we address some aspects of the policy framework which must be addressed as part of an expanded, secure CDR.

1.1 Liability and fraud

We agree, as stated in the Issues Paper, that:

> By establishing a framework that introduces standardisation, systems which support trust between participants, *clear liability* and providing access to data necessary to create innovative products and services, the CDR has the potential to create the conditions for an Australian digitised ecosystem to grow[4]. (our emphasis)

Clear liability frameworks will be critical to maintain trust in the network if third party access is permitted.

---

[1] Deloitte 2019 *Open banking: switch or stick? Insights into customer switching behaviour and trust,* p. 23
[2] Deloitte 2019, p. 14
[3] Deloitte 2019, p. 15
[4] Farrell, S. 2020, *Inquiry into Future Directions for the Consumer Data Right, Issues Paper*, The Treasury, p. 3

In 2019, Westpac responded to 1460 unique phishing sites which attempted to convince customers to disclose their banking passwords, and 116 unique banking-specific malware that attempted to compromise one of our brands. Each of these involved material effort on the part of the attacker, in expectation of a return. This underscores the need for customers to fully understand the risks of allowing third parties to access their accounts.

It is important that in seeking to make switching easier for customers, we do not inadvertently create new opportunities for data theft or fraud. Recent data from Deloitte indicates:

> Customers who switch providers of their financial services products are more likely to be better educated and have a higher income. They're also more likely to be tech-savvy and Millennials (Gen Y).
>
> Switching is not difficult for most products. It is not as difficult as people perceive. Once someone has switched, they also realise it's not as difficult as they might have thought.[5]

The education of consumers is therefore critical - customers need to be aware at every point that their data is being transferred from one party to another. Given the consumer will be engaging with the third party provider (in a write access scenario) we assume that similarly to the current regulatory regime where the Accredited Data Holder (**ADH**) or Accredited Data Recipient (**ADR**) could be held directly liable to the consumer, the consumer should be able to directly claim against that third party provider including in the event of fraudulent or inappropriate drawing on the account.

Further, where third parties have the power to move money around via write access, whether by holding it similarly to non-Authorised Deposit-taking Institutions (**ADIs**) or simply directing it, it is our view that additional financial security from third parties should be required (in addition to the existing requirements for insurance and guarantees which are limited to consumer losses relating to a breach of the CDR regulations), to provide equivalent protection to the capital requirements or other financial guarantees as are required of financial institutions with similar powers, as otherwise the liquidity risk of permitting these activities to occur may outweigh the benefits.

Recommendation 1: In a 'third party access' environment, authorisation (granting of consent) should have multi-factor authentication and all write actions should be authenticated (*e.g.* enter an One Time Password every time a payment is sent).

Recommendation 2: The existing protections should be reflected in any amendments relating to write access *i.e.* participants should not be held liable provided they comply with their own obligations under the regulations and additional protections should be introduced given the liquidity risks of non-Authorised Deposit-taking Institution participants. Similarly to the current regulatory regime where the Accredited Data Holder (ADH) or Accredited Data Recipients (ADRs) could be held directly liable to the consumer, the consumer should have the ability to directly claim against the third party provider including in the event of fraudulent or inappropriate drawing on the account. Further, there should be a meaningful capital and/or insurance requirement for third parties, well above the existing requirements for read-only.

[5] Farrell, S. 2020, p. 5

1.2 Consent taxonomy

The issues paper notes the potential to develop a 'consent taxonomy', "using standardised language for consents across providers and sectors"[6], presumably envisaging the Government's commitment to extend the CDR to cover data sets and data holders for energy and telecommunications.

The current systems for obtaining and recording consent vary widely between organisations, and often rely on legacy or proprietary systems. Accordingly, developing an agreed consent taxonomy across a banking sector, or multiple industry sectors, is likely to present a significant challenge.

Notwithstanding the challenge of developing a 'consent taxonomy' across sectors, it could assist in standardising the delivery of customer instructions. If correctly implemented, it could also lead to efficiencies and reduce risks across. However, given the inevitable differences in language used by individual providers, this would require significant consultation to ensure the correct references are chosen.

Recommendation 3: Deep and broad consultation must occur in order to develop proposed consent taxonomies.

1.3 Digital Identity

There is an important relationship between the CDR and Digital Identity. The CDR requires a customer to be authenticated to establish consent but determining that the individual establishing an identity is who they say they are is a further step. In order for the CDR to be safely expanded to write access, a portable digital identity solution, or solutions, is a necessary pre-condition.

Westpac is supportive of the development and enablement of portable digital identity in Australia as it could lead to significant improvements in customer experience, shared Know Your Customer (**KYC**) processes and detecting payments fraud. At their core both CDR and digital identity involve the flow of customer attributes driven by informed customer consent. However, there are also differences between the CDR framework and requirements for effective, interoperable digital identity solution(s) in Australia.

Digital Identity has important connections with Anti-Money Laundering and Counter-Terrorism Financing (**AML/CTF**) laws, KYC requirements specified within those laws, and other aspects of financial crime. Compliance regimes for AML/CTF regulation are implemented by each Reporting Entity, as defined in the AML/CTF Act. It is important that digital identity frameworks and associated standards are developed by industry in consultation with key stakeholders including AUSTRAC and the RBA.

Importantly, the first Farrell Review acknowledged that supporting documentation provided by an individual as part of identity verification significantly raises the risks of identity theft[7]. Risks related to fraud and unauthorised access to the customer's accounts are significantly increased by the provision of certain

[6] Farrell, S. 2020, p. 5
[7] Farrell, S. 2017. *Open Banking – Customers choice convenience confidence*, The Treasury, p. 34

identifying information to a third party, including the customer's date of birth or copies of a passport/driver's licence information.

ADIs should not be required to share information supporting an identity verification assessment directly with the customer. If ADIs were required to supply personal information about a customer (*e.g.* identify information such as a Date of Birth) inside a digital channel, such as an online banking system, this would become another vehicle for identity theft (and increase the attractiveness of online banking as a target for malicious actors). An additional uplift in security would be required at a significant cost to the organisation.

To reduce these risks, Westpac has been taking active steps over a number of years to remove personal and identifying information from online banking due to the increased use of screen-scraping and the ability for fraudulent parties to access this personal information to take over a customer's identity. On this basis, we strongly recommend that this type of data not be required to be shared under the proposed expansion.

We note there is a pending amendment to the AML/CTF Act (Part 2, Division 7) that is expected to allow a Reporting Entity to rely on the applicable customer identification procedure that was previously carried out by an unrelated Reporting Entity.

The first Farrell Review recommended against the inclusion of value-added data because it would discourage investment in analysis and transformation and accordingly undermine competition to generate innovation and increased customer choice[8]. The Government has confirmed this approach via its designation instrument which includes an exclusion for materially enhanced information. In our previous submissions on this topic, we have noted that the line between that 'materially enhanced' information[9] and 'simple' forms of derived data is not entirely clear.

However, in our view identity verification assessments information would be considered enhanced because algorithms or analytics are used to achieve that output making the information significantly more valuable than the source material. A KYC process involves the production of materially enhanced data, and it is equally important that competitive neutrality is maintained.

Established organisations should not be expected to subsidise or absorb business costs on behalf of other data participants in data-sharing initiatives, particularly those entities that cannot provide an equivalent identity verification service. We note that there are significant developments in the digital identity space in Australia, including the development of interoperable industry standards through the Australian Payments Network and several domestic and international solution providers have expressed interest in accreditation through the framework.

Given there is considerable work being undertaken on digital identity by both industry and Government and this includes the development of alternative solutions and interoperable accreditation standards and

> *Recommendation 4:* The two regimes (digital identity and CDR) should be dealt with separately but it is imperative that they are interoperable.

[8] Farrell, S. 2017, Recommendation 3.1, p. 35

[9] As confirmed by the ACCC in the Rules Framework any inclusion of derived data would not include materially enhanced data, see also fn 9.

solution design, it would be more logical that these develop independently except to the extent required to ensure interoperability.

1.4 Tiered accreditation

As stated in earlier submissions, Westpac supports a tiered accreditation model to ensure the regime is set up safely and for success. Appropriate security requirements and accreditation will be critical for intermediaries not to introduce systemic risk. To ensure a safe and efficient ecosystem, here should be a higher bar to accreditation for those seeking write-access than those seeking read-only access.

Accreditation for read and write access will require separate and distinct security and technical requirements. Equally the liability framework to support accreditation for write access will require similarly distinct requirements, recognising that banking data includes not only customer personal information but financial data, so it is imperative that this information is adequately protected to avoid the introduction of systemic risk into the Australian financial and payments systems.

Third Party data management arrangements will vary. They may assist in the collection of CDR data or offer end-to-end services that collect and use CDR data. In either scenario, third parties must be accredited to ensure appropriate handling and use of consumer data. We agree that different accreditation obligations may be useful to distinguish between the different risk profiles associated with different activities, however there should be no lesser obligations in terms of security, privacy or consent. It is possible to have data sharing systems that are privacy and security-protective by design and by default.

Recommendation 5: Accreditation at any level – including for intermediaries and third parties – should at the very least meet the same high standards around security, privacy and the need for consumer consent as currently exist under the regime, with the expectation of additional more stringent requirements for those seeking write-access. Different accreditation obligations may be useful to distinguish between the different risk profiles associated with different activities, however there should be no relaxing of obligations concerning security, privacy and consumer consent.

2. **Reciprocity**

Westpac has always strongly supported the Government's position that there should be reciprocal obligations, *i.e.* the principle that 'equivalent transaction data' be shared by data participants to ensure the robustness of the regime. This principle should be extended to any requirement to provide for third party write access. This is particularly important given the CDR is intended to be economy-wide and is consistent with the objective of establishing a robust and innovative data industry in Australia.

Westpac supports the Government's objectives – giving customers the ability to access and share their data with third parties will lead to more product choice, and greater convenience. It will also enable new players to enter the market and facilitate innovation and data driven products. However, there are significant risks of market distortion.

We have previously noted that allowing incumbent, data-rich companies to take advantage of the unequal playing field created by regulation, is a form of regulatory arbitrage. All providers should be able to access the same or equivalent data and compete via their insights and analytics to make innovative products and services, thereby maximising benefits to consumers.

Recommendation 6: To balance the need to encourage competition with the need to ensure that the competitive landscape is not distorted and all participants to compete and innovate, we recommend:

- accreditation criteria that include, at a minimum, an obligation for ADRs to also provide write access to their equivalent data sets in order to develop a product or service, where the consumer has consented to write access or where write access is permitted; and
- to ensure the barriers to entry are not too high, an exemption to the obligations of reciprocity for small business and start-ups that meet each of the following: (a) have an annual turnover of less than $10 million in the most recent previous financial year; and (b) have fewer than 100 full-time equivalent (FTE) employees; and (c) less than $3 million total debt to all credit providers, on a group-wide basis.

3. The right time to expand CDR

There are key contingencies for write access to work, *e.g.* where there is standardised data capture and processing, it is possible to achieve write access. As data sets and complex processes associated with many products vary quite significantly between banks, it is difficult to standardise interfaces for many actions, including closing accounts, switching between products or mortgage origination. The more complex the data set, the more difficult the task across multiple ADIs. In addition to the security and liability concerns raised above, we outline some other key developments which will assist on the pathway to further expanding CDR.

The first Farrell Review concluded that the CDR legislation should not preclude the possibility of providing write access in the future. However, that it should only be considered after a post-implementation review of the assessment of the success of read access[10]. We agree with this and suggest that whilst it will be helpful to consider the key opportunities and constraints in this process, timing and policy decisions to proceed with write access should not proceed before such a post-implementation assessment. With the build for read access still underway, and a further build necessary for write access, we could not see write access being viable before 2023 at the earliest.

Recommendation 7: Expansion of the CDR should not be legislated until a full post-implementation review of the current program has occurred – this should only take place once Phases 1 and 2 of the current program have been embedded.

[10] Farrell, S. 2017., p. 109

3.1 Use cases, rules and standards

We have previously noted that the industry's ability to meet implementation timeframes is contingent on the finalisation of the data and security standards. This is equally applicable to any expansion of the CDR. The Rules and Standards should expand in a focussed and progressive way by considering the costs and benefits of each scope expansion at an ecosystem level. The most appropriate way to do this initially is to focus on enabling those use cases which have been already identified.

Clear, concise and effective consent needs to be provided for all use-cases and is something which is required by the current regulatory regime. While competition will naturally drive innovation in use-cases, an expanded CDR must define service offerings and a mechanism to ensure the evolution of use-cases over time are captured by the Act, as well as Rules and Standards.

It may be beneficial to identify possible or desirable future use cases, having regard to emerging technology trends. For example, what kind of service efficiencies and user experiences could be achieved by technologies such as intelligent digital assistants using CDR APIs? By more clearly articulating desirable medium and long term outcomes, we can better plan and structure the immediate deployment of the CDR to achieve those objectives.

Further, the issues paper "The Consumer Data Right gives customers, including individuals *and business customers*, the right to safely access certain data about them…".[11] Given the broad nature of the proposed expansion of the CDR program, and the current status of the program, we recommend that business is not brought into an expanded CDR at this point, in keeping with the existing scope.

Recommendation 8: To ensure that write access provisions do not pose a risk to the financial system, we recommend that the existing Know Your Customer (KYC) rules should be retained where write access is allowed for the purposes of opening an account on behalf of a customer.

3.2 Write Access

In contrast to sharing 'open data' on a read-only premise, 'write access' is more complex and raises more significant concerns about the scope and sensitivity of the data, complexity of the processes involved (*e.g.* consent, authorisation and verification), privacy, security, liability, fraud, data accuracy and other impacts of data breaches on individuals. These risks exponentially increase where there is both 'read' and 'write' functionality (*i.e.* an ability for a third party to transact on behalf of the customer's accounts) as required in the UK.

As the UK experience has demonstrated, the need to resolve significant outstanding issues in a CDR regime cannot be underestimated. One participant in the UK has recently noted that "before we scale

[11] Farrell, S. 2020, p. 2

Open Banking further, we need to ensure we have a resilient and scalable platform for an ecosystem which will be the basis for financial services in the coming decades"[12].

It is essential that an individual's identity, data and finances are protected and trust in the financial system is retained. We welcome any attempt to bring the Australian standards closer to the applicable international standards. This allows for:

1) Increased security and efficiency of the ecosystem as it leverages the development of the international standards.
2) Australian fintechs and other start-ups to better transition to international markets; and
3) More choice for Australian consumers, as standards-alignment will make it easier for international players to enter the Australian market.

We agree that any write access should only be granted to 'authorised trusted third parties' but note that this is a concept that in itself must be very carefully defined (see above, 'tiered accreditation').

Recommendation 9: Any write access ecosystem must guarantee, through appropriate consent and liability frameworks, at least the same strong privacy protections and fraud protections that the current read access environment provides.

The issues paper flags that write access could have several aspects:

3.2.1 Enabling a customer to open a new account
Allowing the customer to not only assess their situation in a competitive market but act on that assessment may seem a natural expansion, but the implementation is likely to be complex and pose a much higher risk to consumers.

In an environment of increasingly large cyberattacks and data breaches, it is known that attackers are developing vast stores of compromised identity information and login credentials. API-enabled and automated or partially automated account creation gives rise to the risk that attackers could use stolen personal information to open accounts, potentially at scale. For example, an attacker could use stolen Proof of Identity to open a credit card account to which they then have access.

The ability for a customer to open an account with a different institution also depends upon a range of developments in Digital Identity which have not yet been settled (see above) in order to meet existing, KYC obligations. Westpac should not be required to verify (KYC) the party leveraging write access through the system (as we would with a signatory).

[12] Danske Bank's chief digital officer Søren Rode Andreasen quoted in FinExtra's "Open Banking year two: Insights from the CMA9" Accessed on 7/5/2020: https://www.finextra.com/newsarticle/35054/open-banking-year-two-insights-from-the-cma9

Further, with regard to current AML/CTF reporting requirements clarity will be required in the context of write access, particularly as it may be an organisation rather than an individual that is the person seeking access.

Recommendation 10: Every field should be assessed against a risk matrix before write access is permitted on its own or in combination with other fields.

3.2.2 Updating details

Westpac has a long standing commitment to ensure that there are protections for customers whenever their personal information is disclosed, *e.g.* to mitigate the risk of identity theft and phishing *etc*. and to minimise any impact to the individual if there is a data breach. However, we are concerned that the risks will be exponentially increased under a write-access environment, given actively fraudulent amendments to personal data can be pushed out and repeated much more quickly and to scale.

There would also be impacts to our existing regulatory obligations in a write access environment:

- Westpac has an obligation to notify individuals when we collect new personal information directly or indirectly from an individual. Clarity is required as to whether a privacy notice should be provided to a customer every time new personal information is received from a 'trusted third party'. This could also serve as an anti-fraud mechanism, alerting customers and ourselves of activity, however there is also the risk of over notifying customers.

- We also have an obligation to ensure that all personal information we hold is accurate, up to date and relevant. There is a risk that technology provided by a trusted third party could be used to change personal information that is currently in dispute or to cover money laundering activities as examples. For example, a customer may be seeking an update to their credit report and would need to contact us first. There is a further risk that a third party API may be used to update personal information without agreement with us.

- A 'trusted third party' could, as an example, provide an app that enables individuals to delete their own data, making it more difficult to meet our retention obligations under various laws. Clarity is required whether write access includes removing or destroying details relating to a customer, noting that financial service organisations have strict obligations globally to retain personal data relating to individuals for various retention periods.

Where information is inaccurate, there is also a risk that reporting to Regulators, other third parties and processes using the personal data could be impaired.

3.2.3 Payment Initiation

Consumers currently have a number of ways of initiating payments (from cards in-store, in-app, using a wallet or online, to cash, to direct debits, to online banking with pay anyone, including real-time Osko and BPAY). With regard to payments and Open Banking in the UK, it has been observed that "while contactless payments are popular, cards will remain the preferred methods of payment, because it is

difficult to create an easier proposition, even with Open Banking"[13]. As noted above, the fraud controls today provide considerable protection for customer funds.

A write access regime that also includes payment initiation brings a customer's financial assets more directly within the responsibility of the third party. It is imperative that this information is adequately protected to avoid the introduction of systemic risk into the Australian financial and payments systems. Any payment initiation requirement on ADIs to accept payment instructions from a third party to debit our customer's account and to pay a fourth party (potentially via the New Payments Platform/Osko) must occur under strict liability and authentication protocols.

If the intent of the payment initiation is to be the final leg of a switching process, then restricting payments so that they can only be made between a customer's existing accounts would assist to avoid bad actors posing as trusted third parties (forth parties), as outlined above.

We do not consider it is necessary to mandate payments initiation, but rather allow this to be a competitive advantage which would add value to an institution's accounts.

Recommendation 11: Any addition of payments in an expanded CDR should mandate the process needed to authenticate the transaction on the customer's behalf, but not the mechanism – the industry should be permitted to innovate.

Recommendation 12: The liability framework should be robust and third parties operating any new 'payments' technologies within a write access regime should bear the liability. Aligned to our comments on accreditation, there should be a higher bar for those seeking write-access than those seeking read-only access to ensure a safe and efficient ecosystem.

Conclusion

As we have noted above, further expansion of the CDR ecosystem to write access should only be considered after read-access has been delivered, bedded down and a post implementation review has been completed.

In closing, we emphasise that to retain trust and confidence in the economy, the CDR framework must support the safe transfer and use of customer data, thereby protecting customer privacy and information. In the banking sector, customer information relates to their financial assets, so it is imperative that this information is adequately protected to avoid the introduction of systemic risk into the Australian financial and payments systems.

Should you have any further questions on this issue, please contact Jaimie Lovell, Head of Government Affairs, Consumer Division on 0450 132 858.

[13] FinExtra's "Open Banking year two: Insights from the CMA9" published on 13 January 2020, Accessed on 7/5/2020: https://www.finextra.com/newsarticle/35054/open-banking-year-two-insights-from-the-cma9

Yours sincerely,

Michael Choueifate
Group Head, Government and Industry Affairs

Appendix 1

We understand that the ACCC has engaged CyberCX to develop a Cyber Security strategy for the CDR which will address the register, governance, controls and monitoring and the wider ecosystem. We take this opportunity to reiterate the recommendations we made to CyberCX.

Westpac recommends establishing additional security controls from the current baseline to protect data in read and write access. We also recommend a governance framework to ensure continual review and improvement to assist the system to meet developing external threats.

Each of these controls would result in greater trust in the ecosystem because incidents and anomalies would improve response times and ensure that security assurance would be tighter.

To better guarantee a robust system, Westpac would recommend:

1) *A 24x7 centralised Security Operations Centre (SOC) responsible for monitoring the RAAP (Register & Accreditation Platform) and coordinating responses to threats across the CDR ecosystem.*
   In considering the scope and nature of security monitoring, a 24x7 system would provide early visibility and timely response to security incidents in the ecosystem and reducing the window of exposure to external threats where cyber criminals could target unmonitored systems.

2) *Capability for real-time detection and flagging of anomalous/unusual behaviour at both customer and participant level (ADR, ADH). This should be mastered and monitored centrally to identify anomalous activity and trends early across the CDR ecosystem.*

   This would reduce participants' reaction time when incidents occur and better protect consumers, their money, data and identity. It would also ensure that participants do not operate in isolation, but rather coordinate to shut down security threats effectively and quickly.

3) *Strengthen the ongoing compliance requirements for ADRs via a program of ongoing and centrally managed security testing and audits activities.*

   The current self attestation model has benefits because it reduces the cost of entry into the ecosystem. However, the ACCC should be proactive in verifying what has been attested to – this will ensure the compliance with the standards and provide assurance to the overall security posture of all participants.

4) *A crisis management plan/framework to be implemented when the entire ecosystem, including participants, consumers and the Australian financial system at heightened or unsustainable risk (e.g. including the capability to stop all CDR transactions systems wide).*

   Should there be a significant threat level or indeed systemic issues with online fraud or identity theft detected, it is important that there is an established crisis management framework to rapidly address such risks and potentially shut down the system. Examples might be: multiple fraudulent registered ADRs or compromise of the register itself.

5) *Policy and protocols to manage security incidents and investigations across the ecosystem.*

   This would ensure that knowledge of incidents is shared between participants and that response are rapid, proportionate and consistent. This would include provisions to support the operational activities of Federal law enforcement agencies such as the Australian Signals Directorate and Australian Cyber Security Centre

6) *A framework for data holders to suspend access based on anomalous activity observed themselves through their own detection of anomalous/unusual behaviour.*

   This will reduce the impact of incidents as they occur as data holders will be able to react more quickly and ensure that distinct data holders react in a consistent way to incidents.

7) *Secure and confidential exchange of threat intelligence specific to the CDR ecosystem and a risk committee to discuss Fraud and Digital Security issues. The committee would compromise of subject matter experts to discuss trends and patterns of anomalous behaviour within the CDR ecosystem. Legal provisions should be in place to deter disclosure beyond CDR participants.*

   This will allow participants to share information on multiple levels, improve reactivity and collude to defeat new attack vectors and control risks as they arise. It will also allow participants to share information and cooperate to defeat new attack vectors and risks as they arise.

8) *A framework for secure and confidential exchange of threat intelligence specific to the CDR ecosystem.*

   Ensuring legal provisions are in place to deter disclosure beyond CDR participants.

9) *Limit (or prevent) the use of less secure practises of gathering customer information, e.g. screen scraping. Make provisions to transition from less secure data sharing practises towards the CDR ecosystem over time, and/or ensure that these practises are controlled by equivalent legislation to the CDR.*

   This will level the playing field and ensure that increased compliance risk is not a reason to avoid adopting the CDR for data sharing.

Additional comments on operations

In terms of accelerating the creation of a safe and efficient ecosystem of participants and service providers, the following could be considered:

1) Automated tests for both APIs and security infrastructure (as in the UK system)
2) A sandbox register and sandbox data holder is available for developers to use (as in the UK)
3) A more specific security blueprint, *i.e*. a ready-made security policy.
4) A downloadable library in various languages to handle the security layer interchange.
5) Cloud Infrastructure ‘recipes’ to create environments that will be automatically be certified as secure as long the manual portions of the recipe are met.