Commonwealth Bank

Can

Commonwealth Bank of Australia
ABN 48 123 123 124

18 January 2019

Manager
Consumer Data Right Team
Structural Reform Group
The Treasury
Langton Crescent
Parkes ACT 2600

Via email: data@treasury.gov.au

Commonwealth Bank welcomes the opportunity to respond to Treasury's draft Privacy Impact Assessment (PIA) of the Consumer Data Right (CDR) regime.

As Treasury notes, data sharing is already prevalent throughout the economy. However, the CDR may amplify the risks inherent in data sharing because of the scale, speed and immediacy of data sharing under the regime.

Commonwealth Bank endorses the approach of the CDR in creating a framework that, if properly implemented, will afford consumers greater privacy, security and confidence in sharing their data.

The integrity of the CDR regime will be underpinned by the nature of how consumers consent to sharing their data – specifically that such consent is express, informed, clear, current, specific, unbundled and time specific, together with the legal and technical protections surrounding the disclosure, use, and security of that data, as held and disclosed by trusted participants.

General Comments

The business of protecting a citizen's right to privacy is heavily reliant on the cyber security capabilities of any given organisation.

Commonwealth Bank invests heavily in protecting our customers' confidential banking data. As the RBA noted in its most recent Financial Stability Review, regulators and financial institutions have become much more focussed on cyber risk in recent years. The RBA quoted an IMF estimate that direct losses from cyber-attacks could be as large as nine per cent of total bank net income globally.[1]

While much work has been done already to progress the Consumer Data Standards (**Standards**) and Consumer Data Right Rules (**Rules**) for the CDR regime, the Privacy Impact

[1] RBA, October 2018, "Financial Stability Review", p.56

Commonwealth Bank of Australia
ABN 48 123 123 124

Assessment is timely and should in turn be used to inform the technological solutions and regulatory settings that underpin the regime.

Commonwealth Bank recommends that once the Privacy Impact Assessment is finalised, there should be an additional review of decisions that have already been made or are currently under consideration. Such decisions include:

- The customer authentication framework that will be adopted, and the uplift in security that would be afforded by adopting a decoupled model (InfoSec Standards Working Group).
- The granularity of consent that a customer may wish to provide (Consumer Experience Working Group).
- The Accreditation standards that will be enforced for accredited data recipients (ACCC Rules framework).

Recommendation 1

Once the Privacy Impact Assessment is finalised, an additional review of decisions already made – or currently being considered – in relation to the Rules and Standards, should be undertaken.

Protecting data and confidential information is very different to protecting physical assets. Whereas the loss of an asset can often be easily measured and remedied, the loss of data can result in a range of damages, including psychological distress, a heightened threat that online accounts will be compromised, and impacts due to unauthorised disclosure of information which cannot be remediated, such as loss of revenue and goodwill, and damage to reputation.

The regulatory and enforcement regime that underpins the CDR should not rely too heavily on legal measures that seek to punish malicious actors in response to incidents. When faced with determined malicious actors, significant penalties may not be effective where such actors are capable of avoiding identification or are operating beyond the practical reach of Australian regulators.

The regime should instead focus on actions and regulatory settings that will help prevent incidents and limit the severity of incidents once they have occurred. The Privacy Impact Assessment highlights the importance of consumer education and behavioural economics in preventing the misuse or leakage of confidential data; additional measures should include real-time threat monitoring and sharing of threat intelligence, the adoption of appropriate technical standards to prevent data loss, and accreditation standards that are appropriately robust.

Commonwealth Bank of Australia
ABN 48 123 123 124

Privacy Impact Assessment Recommendations

Commonwealth Bank supports all of the nine recommendations in the Privacy Impact Assessment. Additional comments on specific recommendations are outlined below:

Recommendation 1: Commonwealth Bank strongly endorses the incorporation of behavioural research into the design of the CDR. Consumer research should continue to be conducted periodically to reflect shifting consumer preferences and behaviours as well as measuring the effectiveness of proposed risk mitigations on consumer attitudes towards data sharing.

Recommendation 2: Commonwealth Bank supports these reporting requirements. Such requirements should also include: a) length of time to resolve specific complaints; b) data that will assist participants in the cyber insurance market, including number of breaches; number of customers affected; estimated monetary cost per breach; and the broad category of the data breach. The availability of cyber insurance to Data Recipients will be an important factor in helping businesses respond effectively to remediate the impact to consumers in the event of a data breach. Cyber insurance could help ensure that a Data Recipient has the wherewithal to pay for prompt notification of consumers affected by an unauthorised disclosure of CDR data, enabling those consumers to take timely, proactive steps to mitigate or prevent any potential harm.

Recommendation 3: Commonwealth Bank has begun to consult with organisations representing vulnerable consumers via our Customer Advocate's community roundtable. Recommendations from these consultations include ensuring that consent: a) is written in plain English; b) allows adequate time and opportunities for customers to consider the nature of their consent; c) allows for consumers to review their consent over time.
Commonwealth Bank recommends that further consumer testing be conducted to measure the extent to which consent and the purposes for which data is used under the CDR is properly understood.

Recommendation 7: Consumer education materials should be developed in conjunction with industry to ensure there is consistency in communications to consumers. Materials should help develop consumer awareness of potential phishing risks and, in time, provide examples of phishing risks connected to CDR, to help mitigate the risk to consumers.

Risk Assessment

The Risk Assessment covers 38 scenarios, of which four have a 'High' risk rating, an additional 18 have a 'Medium' risk rating and 16 have a 'Low' risk rating.

These risk ratings appear to be lower than expected given industry experience. To understand the reasoning behind some of the risk ratings, industry participants would benefit from further detail of the methodology used for the risk assessment. For instance, a scenario for

which may result in a Low or Medium risk severity for a major financial institution may be rated much higher for an organisation with fewer staff and less resources.

It should also be noted that the cumulative risk rating to consumers of such scenarios is much higher than each in isolation. For instance, if a customer is tricked into handing over their online banking credentials to a non-accredited data holder, the likelihood that their data will be used in a way that is inconsistent with their consent or disclosed to other malicious parties is greatly increased. Daisy-chaining of data greatly exacerbates both the likelihood and severity of consumer detriment.

Response to Specific Scenarios

Phishing scenarios (Scenarios 1.1, 3.1, 3.2)

These scenarios cover instances of phishing, in which a cyber-criminal poses as either a Data Holder or Data Recipient in order to socially engineer a consumer into providing them with personal and/or financial data. Phishing attacks which exploit the CDR regime are very credible and would result in considerable consumer detriment.

The likelihood of cyber criminals seeking to exploit Open Banking as an opportunity for phishing campaigns is high. Cyber criminals have proven themselves to be highly adaptive and quick to take advantage of new developments.

In calculating the likelihood of the phishing scenarios, there is an overreliance on the efficacy of some Risk Mitigation Strategies listed the PIA. For instance, Australian legislation, such as the Privacy Act,the Criminal Code, and the Trade Practices Act, have not proven to be an effective deterrent to international cyber criminals, who operate anonymously beyond the reach of domestic law enforcers and regulators.

Commonwealth Bank agrees with, and strongly endorses, Treasury's identification of consumer education about the phishing threat associated with the Open Banking regime as a key strategy for mitigating the phishing risk.

The final form of authentication flow in the Standards (currently being developed by Data61 as the Data Standards Body) will influence the likelihood of the phishing attacks occurring under the CDR. Some models of authentication provide greater opportunities for exploitation through phishing than others. Commonwealth Bank favours a de-coupled approach over re-direct approach for this reason.

The PIA does not give sufficient weight to the impact that a phishing attack would have on an individual in calculating the Risk Severity of some scenarios. A cyber-criminal is likely to attempt to maximise the value of stolen data; as a result, once personal details or credentials have been compromised through phishing, criminals may attempt to conduct a wide range of

malicious activities including identity theft, impersonation, diversion of funds and the resale of that data.

In addition, Commonwealth Bank does not agree with the implication of the statement in the Privacy Impact Assessment that "there are also a number of currently unregulated approaches to data sharing, of which screen-scraping is one example ... the CDR is not a replacement 'pipe' but is instead intended to be a safer pipe" to existing data sharing practices.

While the CDR regime and models for sharing data will indeed be safer, at the very least the Government and regulators have an important role in educating consumers about unsafe practices. Beyond this, regulators should clarify whether accredited persons under the CDR should also be allowed to engage in unsafe data sharing practices, such as screen-scraping. Encouraging both safe data sharing practices and unsafe practices is likely to confuse consumers and heighten the risk of their data being misused as it may not be clearly apparent to consumers in a particular circumstance where they aren't exercising their CDR but are in fact providing credentials for the purposes of screen scraping.

Further, it is possible that accredited data recipients will leverage the CDR for the data which is within scope of the CDR regime and screen scrape data which is not. This permission doesn't appear to fulfil the policy intent of the Treasury given that this will result in a second category of data held by accredited data recipients about a single customer for which the CDR protections will not apply. Commonwealth Bank considers that this will cause confusion with consumers and is not clearly mitigated by the penalties for misleading and deceptive conduct.

Recommendation 2

A review of authentication frameworks should be undertaken to test the security protections they provide consumers. In particular, the ACCC and Data 61 should investigate whether a decoupled approach would reduce the incidence of successful phishing attacks.

Commonwealth Bank of Australia
ABN 48 123 123 124

Recommendation 3

CDR accreditation should be provisional on a party not engaging in unsafe data sharing practices, such as screen-scraping. In the event that an accredited data recipient is found to be engaging in unsafe data sharing practices, their accreditation should be suspended or revoked.
In addition, Government consumer education campaigns should reinforce the dangers of unsafe data sharing practices, such as screen-scraping.

External attack leading to compromise of a Data Recipient (Scenario 5.4)

The likelihood of an accredited data recipient's systems being compromised by an external attacker, enabling the attacker to access and use CDR data, will largely be a function of the cyber security capabilities of that accredited data recipient. Commonwealth Bank assesses that the likelihood of this type of attack would be higher than Treasury's assessment of 'Unlikely'.

In addition to mandatory data breach notification, threat monitoring and intelligence sharing arrangements between participants would also help participants to defend against cyber-attacks targeting consumer data.

Commonwealth Bank strongly endorses additional risk mitigation measures included in the ACCC's Rules Outline, released in December 2018. These will significantly mitigate the threat that consumers' data under the CDR will be compromised by cyber-criminals. Importantly, these include:

- The exemption from the obligation to share CDR data with an accredited person, if the data holder has reasonable grounds to believe that serious harm could be caused to an individual or to the integrity of the CDR system (Section 1.7).
- A requirement that data holders and accredited data persons hold appropriate cyber insurance to cover potential financial losses by consumers (Section 5.10).
- Regular audits of all accredited data Recipients by the ACCC and OAIC to ensure they are adhering to the requirements of accreditation (Section 9.9).

Commonwealth Bank considers that further detail regarding the exemption process is necessary in order to implement any related systems and processes; such as:

- If exemptions will be applied with respect to certain accredited data recipients, in order for authorisation of a valid request to be rejected (as section 1.8 of the Rules Outline suggests);

- Processes relating to notification by data holders of the reliance upon an exemption which has been set by the Rules (such as the serious harm exemption); and
- Suspension of accreditation and / or notification by ACCC or OAIC to CDR participants of the potential for serious harm arising from a request for disclosure of CDR data from a particular accredited data recipient, in order for other data holders to safeguard CDR data from disclosure and rely upon the exemption.

Commonwealth Bank recommends that, as the Rules Outline is translated into Standards, additional mitigation measures should enable immediate revocation of an accredited person's security certificate, to prevent the ongoing disclosure of CDR data in the event of that an accredited person's accreditation is suspended or revoked, including as a result of the application for an exemption by a data holder.

In addition, the Standards should be aligned with current cyber-security standards imposed on financial institutions, to ensure there is no 'weak-link' established among accredited data recipients. This should include a requirement that accredited data recipients ensure that data is encrypted at rest, once it has been received from a data holder.

Commonwealth Bank also recommends that data holders should be able to conduct security testing against accredited data recipients and perform ongoing fraud and security monitoring as additional safeguards. Data holders have the scale and resources to carry out these tests. In light of the global cyber skills shortage, accredited persons may not be able to develop these capabilities themselves. These steps are taken today as part of normal supplier and data partnership arrangements and are important in ensuring the appropriate security controls and protections are in place.

Commonwealth Bank proposes further discussion on how best to help consumers make educated decisions about with whom they share their data. One possibility is that accredited data recipients are awarded publicly accessible ratings that correspond to security posture in a similar manner that Canstar or other consumer comparison sites rate consumer services.

Recommendation 4

Commonwealth Bank recommends the Technical Architecture outlined in the Standards should enable immediate revocation of an accredited person's security certificate if accreditation is suspended or revoked.

To the extent possible, security standards under the CDR should be aligned with existing cyber security standards imposed on financial institutions. This should include a requirement that accredited data recipients ensure that data is encrypted at rest, once it has been received from a data holder.

Commonwealth Bank of Australia
ABN 48 123 123 124

Recommendation 4 (cont'd)

Data holders should be able to conduct security testing against accredited data recipients and perform ongoing fraud and security monitoring as an additional risk mitigation measure.

Insider working for an Accredited Data Recipient accesses Consumer data (Scenario 5.1)

Commonwealth Bank assesses that the likelihood of unauthorised access to consumer data by an insider at a Data Recipient is higher than 'Unlikely'. The Office of the Australian Information Commissioner reported that of the total breaches reported under the Notifiable Data Breaches (NDB) scheme between 1 July 2018 and 30 September 2018, 37 per cent were the result of human error (including unauthorised access by an employee, or unauthorised disclosure by an employee) and 57 per cent were the result of malicious or criminal attacks.[2]

One of the factors that may impact the likelihood of this scenario are the Identity and Access Management (IAM) controls at the accredited data recipient. Strong IAM controls, including applying the 'least privilege' principle to a user's access to data, will help mitigate this risk. The information security standards expected of accredited persons that are established in the Rules should mandate appropriate IAM controls.

Recommendation 5

Accredited persons be mandated to maintain robust Identity and Access Management (IAM) controls that may be audited by regulators to reduce the risk of unauthorised access to CDR data.

Insider at accredited data recipient discloses a person's CDR data (Scenario 5.3)

This scenario could include a malicious insider disclosing or selling a person's CDR data on a dark marketplace on the Internet. Accordingly, the Risk Severity should be higher than the current "Moderate" rating.

[2] OAIC, 2018, "Notifiable Data Breaches Quarterly Statistics Report: 1 July – 30 September 2018" available online at: https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/notifiable-data-breaches-quarterly-statistics-report-1-july-30-september-2018

Commonwealth Bank of Australia
ABN 48 123 123 124

Sophisticated external attacker interfering with data transferred between the Data Holder and data Recipient (Scenario 4.9)

The likelihood of this scenario occurring would be rare, since the current draft of the Standards include measures that would make the attack extremely difficult to execute. In particular, the Standards provide from Mutual Transport Layer Security (Mutual TLS) for backchannel communications between the data holder and data recipient. Mutual TLS provides a two-way secure channel for backchannel communications between the two parties, which would be technically extremely difficult to compromise.

Next Steps

Treasury noted that the current version of the Privacy Impact Assessment does not cover key elements of the CDR regime including:

- the nature of and processes for consent to disclosure, use, holding and collection;
- detail of deletion and anonymisation rights;
- restrictions and processes for transfers of data out of the CDR system;
- restrictions on direct marketing and on-sale of data;
- granularity of access permissions that the system will support; and
- granularity of use permissions that the system will allow.

Commonwealth Bank welcomes the opportunity to engage and contribute to future versions of the Privacy Impact Assessment. In addition to the topics listed above, it is also recommended that future Privacy Impact Assessments also review specific data sharing requirements for complex customers such as small and large businesses.

In addition, given that the most sensitive consumer data will be shared among data holders in a pilot from July 2019, Commonwealth Bank recommends that a separate privacy assessment and risk framework be developed as part of that pilot ahead of sharing with accredited data recipients from February 2020. As part of this process, Treasury and the ACCC should consider whether a tiered accreditation system would be appropriate for different categories of data, depending on their sensitivity.

Recommendation 6

Later versions of the Privacy Impact Assessment should consider the risk of privacy and confidentiality impacts on complex customers, such as business customers, including the appropriate authorisation framework and risk mitigations. Additional assessments should also review the framework for sharing the most sensitive consumer data, including whether a tiered accreditation system would be appropriate for accredited data recipients to get access to the most sensitive categories of data.