27 May 2022

Ms Elizabeth Kelly PSM
Statutory Review of the Consumer Data Right
The Treasury
Parkes ACT 2600

By email: CDRstatutoryreview@treasury.gov.au

Dear Ms Kelly,

Statutory Review of the Consumer Data Right

COBA appreciates the opportunity to provide a submission to the Statutory Review of the Consumer Data Right (CDR).

COBA is the industry association for Australia's customer owned banking institutions (mutual banks, credit unions and building societies). Collectively, our sector has $155 billion in assets and 4.5 million customers. Customer owned banking institutions account for around two thirds of the total number of domestic Authorised Deposit-taking Institutions (ADIs) and deliver competition and choice in the retail banking market.

Implementation of the CDR has been, and continues to be, a significant compliance challenge for COBA members, diverting scarce resources from other critical business priorities.

However, over time, and assuming the implementation challenges can be overcome, we do see the CDR as having huge potential to benefit consumers and drive competition in banking and potentially in other markets.

Out of the eight ADIs currently active as Accredited Data Recipients, three are mutual banks. COBA member Regional Australia Bank was the first ADI to be accredited as a data recipient, ahead of the major banks and other domestic banks.

Key responses to Review:

Question One: Are the objects of Part IVD of the Act fit-for-purpose and optimally aligned to facilitate economy-wide expansion of the CDR?

The objects are fit for purpose.

Question Two: Do the existing assessment, designation, rule-making and standards-setting statutory requirements support future implementation of the CDR, including to government-held datasets? Question Three: Does the current operation of the legislative settings enable the development of CDR-powered products and services to benefit consumers? Question Five: Are further legislative changes required to support the policy aims of CDR and the delivery of its functions?

Issues with the implementation of the CDR in banking indicate that the operation of the legislation settings and the rule-making and standards-setting requirements could be improved to support future implementation of the CDR, development of CDR-powered products and services to benefit consumers and to support the policy aims of CDR and the delivery of its functions.

The aggressive and dynamic implementation program for CDR in banking has produced significant compliance challenges for ADIs. These include postponement of other projects that are more important for customer service, competitiveness and risk management.

These issues can be addressed by changing the CDR framework to provide:

- A reasonable and orderly release schedule of rules, standards and other requirements.
- An improved exemptions process.
- A central location for rules, decisions papers and guidelines.
- Better co-ordination between all regulators and policymakers (ACCC, Data Standards Body, Treasury & Office of the Australian Information Commissioner).
- A timely, accessible and effective testing environment.

Question Four: Could the CDR legislative framework be revised to facilitate direct to consumer data sharing opportunities and address potential risks?

As noted in the Issues Paper, direct to consumer data sharing could potentially enable sensitive data to be shared outside the system. This data would not be subject to the same protection as data shared with an accredited data recipient who would have secure systems in place to read the personal data of the consumer. This raises the risk of undermining confidence in the CDR. Therefore, any revision of the framework to facilitate direct to consumer data sharing should be approached with great caution.

A hugely important factor in planning for the future expansion of the regime is the rising threat to cybersecurity. The functioning of Australia's banking system is dependent on a secure cyber environment. Our members are highly aware of the risk posed by the evolving nature of cybercrime and responding to this risk is a high priority for our sector. Our members dedicate considerable resources towards maintaining and developing defences, and ensuring they are compliant with existing cyber security obligations under the various frameworks.

Observations about implementation of CDR in banking

Scott Farrell's 2017 Review of Open Banking in Australia identified four key principles:

- Open Banking should be customer focussed. It should be for the customer, be about the customer, and be seen from the customer's perspective.
- Open Banking should encourage competition. It should be done to increase competition for the banking products and services available to customers so that customers can make better choices.
- Open Banking should create opportunities. It should provide a framework on which new ideas and business can emerge and grow, establishing a vibrant and creative data industry.
- Open Banking should be efficient and fair. It should be effected with security and privacy in mind, so that it is sustainable and fair, without being more complex or costly than needed.

In COBA's view, implementation of Open Banking, i.e. application of the CDR to the banking sector, has not captured the attention of consumers, has not increased competition and has been complex and costly.

Many COBA members have questioned the high priority the Government has maintained for CDR implementation, given the lack of consumer demand and a very crowded regulatory change schedule for banking.

Regulatory interventions divert scarce resources away from other priorities for regulated entities, such as investment in product innovation, better service and risk management.

Where the regulatory intervention is novel, technical and elaborate, with multiple regulators, multiple layers of requirements and complex sequencing of rules and standards, it is even more important to optimise consultation for all relevant stakeholders and provide adequate transition periods.

COBA members are strongly committed to protecting the security of customer data and this has been their top priority in working towards compliance with CDR obligations. COBA members are determined to preserve the customer trust they have built up over decades.

Some COBA members, along with other non-major banks, have obtained extensions of time to comply with CDR obligations in the form of formal exemptions provided by the CDR regulator, the ACCC. Other COBA members and non-major banks engaged with the ACCC on individual roadmaps to compliance.

Implementation of CDR is a significant and complex technology transformation project occurring against a backdrop of a global pandemic and many other non-CDR regulatory change projects. This has proved challenging to all stakeholders, including banking institutions, their key technology suppliers and the ACCC as lead regulator.

Halfway through the first year of CDR implementation with the major banks, responsibility for CDR policymaking was shifted from the ACCC to Treasury.

This is a new, highly-technical reform in a new regulatory space. More than 12 months after CDR commencement for major banks, the ACCC was still in the process of developing tools to assist banking institutions to test their CDR solutions, such as mock registers, mock data holders and mock data recipients.

The commercial marketplace for CDR compliance solutions is developing rather than mature.

The ACCC in 2021 needed to provide additional resources to improve the performance of its Conformance Test Suite which is a crucial part of the process for banking institutions to validate their CDR solutions.

The CDR regime comprises legislation, rules, standards and guidance, but the regime is not limited to technical issues of data transfer and security: "*As well as requirements for Application Programming Interfaces (APIs) – in the form of common standards for the APIs that will be used to share machine readable data between CDR users – responsible design of protocol for the exchange of consumer data under CDR requires sensitivity to human contexts of data sharing, including consideration of consumer vulnerability, inclusive user interfaces, and alertness towards privacy implications and other ramifications of automation*."[1]

Given the complexity of such a novel and evolving regulatory regime and the need for certainty and clarity, all these elements must be subject to adequate consultation and completely settled before regulated entities can commence implementation.

The nature and context of implementing CDR underlines the importance of regulators taking a pragmatic approach to enforcement during early stages. High priority must be given to ensuring data is secure and that consumer confidence in data security is maintained.

In April 2022, the Minister then responsible for CDR announced that the Morrison Government had decided to give non-major banks an additional three months to implement joint account data sharing under the CDR.

[1] Consumer Policy Research Centre CDR Report 1

Minister for the Digital Economy, Senator Jane Hume said: “Implementation of CDR in the banking sector has continued to progress, with consumers able to choose to securely share banking data with accredited third parties to access better value products and services. That is why, when non-major banks informed me they needed more time to enable joint accounts to become part of the Consumer Data Right, I agreed to a short extension.”

The Explanatory Statement to this relief instrument said: “The new commencement date of 1 October 2022 gives non-major ADIs sufficient time to build the information technology infrastructure required to comply with obligations that had been scheduled to commence on 1 July 2022.

“Non-major ADIs have outlined significant difficulties in meeting these obligations for a range of reasons including:

- the need for careful design to ensure compliance with the requirements,
- skills shortages in this specialised field, and
- a high dependency on external suppliers who have also been impacted by skills shortages exacerbated by the pandemic.”

In making the case for this relief, COBA argued that its members are challenger institutions in a market dominated by four major players and the key to improving the competitive position of our members in CDR terms is capacity to become data recipients. COBA argued that, in the absence of relief, the aggressive and dynamic implementation timetable would increase the risk that CDR implementation will harm rather than enhance the competitive capacity of smaller banking institutions compared to the major banks. We noted that the continuing compliance pipeline of overlapping commencement dates has reduced the capacity of many of our members to even consider becoming an accredited data recipient.

In addition to the reasons noted in the Explanatory Statement, other factors creating the compliance challenge are:

- complexity of requirements, demanding significant work to break down and assess the pathway forward,
- need for extensive testing to ensure performance and to avoid any adverse impact on underlying core systems,
- pace of introduction of new CDR requirements,
- rules delivered with a due date but without all of the required supporting material (e.g. standards and guides),
- multiple changes occurring in parallel, and
- competing demand for limited resources given multiple urgent non-CDR projects.

CDR implementation projects compete for resourcing against projects to strengthen ADIs against cyber risk. APRA and ASIC both nominate the threat of cyber attacks as significant and enduring.

This emphasis by key regulators of the financial services industry recognises the increasing threat posed by cybercrime and the risk to data stored within financial service providers. Customer owned banks are investing heavily in technology, including to meet regulator-driven investment requirements in cybersecurity, reporting and data analysis capacity, and AML/CTF vigilance. Market and consumer-driven investment requirements include the need to update and replace legacy systems, cost reduction, risk management, partnering capacity, APIs and robotics, and meeting changing customer needs and expectations.

Negative impacts of the CDR data holder compliance challenge are:

- exacerbating the impact of the pandemic in terms of staff exhaustion, fatigue and burnout,
- unreasonable impact on the business of having to give top priority to the aggressive and dynamic CDR implementation timetable rather than other projects where there is actual current consumer demand,
- high costs due to skills shortages,

- postponement of other projects that the business considers more important for its customers and risk management,
- inability to devote resources to becoming a data recipient, therefore exposing the business to strategic risk as major banks gain yet another competitive advantage over smaller ADIs, and
- risk of reputational impact and/or regulator enforcement action from non-compliance.

These issues can be addressed by the following changes:

- An agreed release schedule that considers the rules, maintenance, information security and standards over a 2 or 3 year window, with only urgent security updates introduced outside of that, to allow ADIs to properly plan, budget and resource this work.
- Modifying the exemptions process to make exemptions more accessible so ADIs can deliver to individualised timelines that suit the cadence of their organisation's resources and environments with consideration to size and scale.
- Ensuring delivery timelines are more achievable and based on when all artefacts are delivered, not simply when the rules are passed.
- Having a central location for rules, decisions papers and guidelines.
- Better co-ordination between all regulators and policymakers (ACCC, DSB, Treasury & OAIC).
- Providing an accessible and effective testing environment.

The Consumer Policy Research Centre noted in 2021 that in such a large and complex implementation project, "large incumbents are better resourced to meet technical compliance – there is a risk they may dominate the ecosystem, nullify its impact on competition, and increase barriers to switching."[2]

'Open Banking'

In hindsight, perhaps 'Open Banking' was not the best term to promote CDR. Banking ranks well ahead of most other sectors in terms of consumer trust that information (and money) is safe and well secured. However, 'Open Banking' implies an open environment rather than a secure and protected one.

Clearly, consumer trust is crucial for CDR's success, as highlighted in the Consumer Policy Research Centre (CPRC) report commissioned by the CDR Data Standards Body (DSB): "*Trust is a complex issue that applies to consumer experience and perception of CDR in a variety of ways: trust that the system is secure; trust that the law will protect consumers while using it; and trust that businesses are delivering products and services that are safe, fair, and of good quality.*"[3]

A bank account is a valuable data asset, but consumers are more focused on ensuring this data remains securely protected than on exploiting the data for their own benefit. Optimising CDR will require a sustained effort to uplift financial literacy and data literacy.

As discussed in COBA's September 2021 submission to the CDR Strategic Assessment, consumer research indicates that awareness of Open Banking/CDR remains low and understanding of the benefits is even lower. Customers are unlikely to share data under CDR without a clear, demonstrable benefit to doing so. As such, increasing awareness of CDR is not as important as increasing understanding of the benefits for customers.

We encourage the Review to keep at the forefront of its considerations the key issues[4] for consumers. As noted in the CPRC report, the relative importance ascribed by consumers to key issues affecting their use of digital markets, data portability, and open banking vary, e.g. due to demographics and survey design, but the core themes are largely consistent.

[2] Consumer Policy Research Centre CDR Report 1

[3] Consumer Policy Research Centre CDR Report 1

[4] Consumer Policy Research Centre CDR Report 1

These are:

- trust and transparency
- comprehension and consent
- privacy and security
- fairness and accountability, and
- retaining control over their data.

COBA suggests that as the extension of CDR to other sectors and datasets is considered, the focus should be on a sustainable and safe expansion of the regime so that consumers' trust in the digital market is safeguarded. Further, the perceived benefits of sharing data and considering which datasets are secure and non-sensitive enough to share, should be measured against the uptake by consumers and cost on industry for making these datasets available.

Thank you for the opportunity to respond to this consultation. If you wish to discuss any aspect of this submission, please contact Luke Lawler (llawler@coba.asn.au) or Esther Rajadurai (erajadurai@coba.asn.au).

Yours sincerely

Michael Lawrence
Chief Executive Officer