20 October 2022

Productivity Commission
5 Year Productivity Inquiry: Australia's data & digital dividend
Via email: productivity.inquiry@pc.gov.au

Dear Commissioners

Thank you for the opportunity to contribute to the Productivity Commission's inquiry into how digital technology and data can be used to improve Australia's productivity.

COBA is the industry association for Australia's customer owned banking institutions (mutual banks, credit unions and building societies). Collectively, our sector has over $160 billion in assets, around 10 per cent of the household deposits market and around 5 million customers.

Our 57 members range in size from less than $200 million in assets to around $15 billion in assets – all significantly smaller than most of our ASX-listed peers. Customer owned banking institutions deliver competition, choice and market leading levels of customer satisfaction in the retail banking market.

This submission reflects the experience of the customer owned banking sector on a range of matters canvassed in the report, including data sharing and integration, digital data and cyber security skills, and the need for improved policy and regulatory coordination.

Key points

Infrastructure

- Ubiquitous, high quality affordable broadband is critical for both banks and their customers, and we support any infrastructure sharing and funding arrangements that aims to achieve universal service.

Data sharing and integration

- Building consumer trust and safeguarding data collected will be critical to unlocking benefits of data sharing and integration, but a clear purpose for collecting and sharing - including the anticipated benefit – still needs to be identified and considered against the cost and burden of collection.

Skills

- Skills bottlenecks – which can arise from the mandatory imposition of novel, sector wide technology obligations – should be anticipated and avoided.
- Australians need better scams and fraud awareness skills - businesses need to better understand how to effectively disrupt a scam that is underway, and to increase community education.
- Improving digital literacy across all segments of the community is a valuable goal.
- The value of Open Banking needs to be clearly communicated to consumers.

Suite 403, Level 4, 151 Castlereagh Street,
Sydney NSW 2000

Suite 4C, 16 National Circuit,
Barton ACT 2600

Customerownedbanking.asn.au

Cybersecurity

- Customer owned banks are already investing heavily in technology, including to meet regulator-driven investment requirements in cybersecurity, reporting and data analysis capacity, and AML/CTF vigilance.
- Enhancements to automated software security reporting could assist greatly to keep consumers and businesses safe online.
- Consumer products should have inbuilt malware and intrusion detection within the operating system or when connected to the internet.

Improved regulatory coordination

- To address scams, the government should establish a taskforce, comprised of regulators, banking representatives, payment providers, law enforcement officials, utility providers, relevant federal policy agencies and political representatives, to:
    - Establish a framework for combatting scams via a strategy paper, similar to the Australian Cybersecurity Strategy 2020 and the Ransomware Action Plan 2021
    - Establish themes and best practice for consumer messaging
    - Establish and lead a workplan to measure and track the prevalence of scams and cybercrimes and any reductions
- Treasury should implement a pilot regulatory initiatives grid like that seen in the United Kingdom, to assist regulators and policymakers to coordinate regulatory change and assist industry to plan and map out responses to regulatory change.

A more detailed response to each recommendation direction and information request is provided below.

Recommendation direction and information request 3.1 Investing in regional digital infrastructure

COBA member banks provide services across Australia and around half are headquartered outside capital cities. Ubiquitous, high quality affordable broadband is critical for our banks and their customers. We support any infrastructure sharing and funding arrangement resulting in the provision of universal service.

Recommendation direction and information request 3.2 Creating new data sharing and integration opportunities

Building consumer trust and safeguarding data collected will be critical to unlocking benefits of data sharing and integration. At the same time, a clear purpose for collecting and sharing - including the anticipated benefit - should be identified.

Collecting data in a shareable way can be time-intensive, costly and burdensome to those who have collected the data and become obliged to share it. A refinement process is also critical to ensure data collection is targeted and proportionate to avoid the costs of unnecessary collection and sharing.

Our sector's recent experience with the reportable situations regime demonstrates the risk of overcollection without a clear purpose. This regime has applied to Australian Financial Services (AFS) Licensees and Credit Licensees since 1 October 2021. The lodgement of data was designed to provide intelligence to the Australian Securities and Investments Commission (ASIC) to identify emerging trends of non-compliance and allow subsequent intervention.

The single biggest challenge in meeting the new obligations has been the absence of a materiality threshold for a breach. It means that licensees are required to report to ASIC breaches that have

resulted in no material harm to a customer, which could be for example citing a higher interest rate in advertising material.

COBA members have identified practical issues with reporting, and the regime has generated significant compliance costs. To date there is no evidence that this significant cost to banks is providing a benefit to the regulator or consumers.

ASIC has yet to publish a report on the first year of findings of the reportable situations from data it has received, but is already consulting on changes to refine the regime (including issues raised prior to the regime beginning).

Recommendation directions and information request 3.3 Developing digital, data and cyber security skills

Like many sectors, customers owned banks can have difficulty filling skills gaps needed across the business, and we welcome any systemic efforts to address them. The following should be considered as priority considerations in addressing skills gaps and shortages.

- *Skills bottlenecks should be foreseen and avoided*

The government policy timeframes for Open Banking (Consumer Data Right/CDR) milestones had ramifications for entire banking sector. One of the most significant for the customer owned banking sector was navigating the skills shortages to develop and implement CDR solutions. Many in the sector experienced a high dependency on external suppliers, who in turn were also impacted by skills shortages exacerbated by the pandemic.

Trying to acquire staff with the appropriate skills against competitors with much deeper pockets – who needed the same skills at the same time – was problematic. The ensuing war for talent in turn raised the overall cost of implementing Open Banking for the mutual sector.

Whilst this skills bottleneck was recognised and some compliance flexibility achieved when specifically requested, the overall experience was far from seamless for businesses who were trying to do the right thing and comply with regulation. Better understanding of the practical implementation of sector wide reforms and flexible compliance frameworks will go some way toward avoiding businesses- and ultimately, customers - incurring additional expense due to skills bottlenecks.

- *Australians need better scams and fraud awareness skills*

COBA provides fraud and financial crime advice to our member institutions. We are regularly liaising with customers and banks who have fallen - or in the process of falling - victim to a scam but do not believe this is the case until they have lost their money. Banks have sophisticated systems to detect and disrupt scams, and provide direct personal interventions, but this is often no match for sophisticated scammers who use psychological tricks to part Australians from their money.

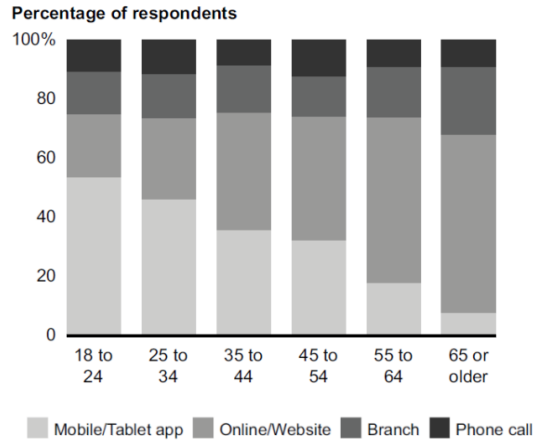
Whilst banks communicate regularly with customers about current threats, and ongoing general education and advice about fraud and scams, the ever-growing losses indicate that consumer skills are not adequate for keeping bad actors at bay. Research[1] undertaken for COBA in the lead up to Scams Awareness week in 2021 found that 8 in 10 Australians had been approached by a cyber-criminal in the previous two years, and of those affected a quarter did what was asked of them. The findings – based on an Essential Research poll of 1094 people – investigated the incidence of scams that ask people to click on a link such as 'missed delivery' text messages, hand over personal information such as bank account or credit card details, or send money or goods.

[1] https://www.customerownedbanking.asn.au/news-and-resources/media-releases/Scams-awareness-week-2021 accessed 4/10/2022

Scam disruption is a complex task with many stakeholders. Consumers have a critical role to play in helping reduce the prevalence of scam losses. Better understanding how to best disrupt scams when they are in play, and more broadly improved community education, is urgently needed.

- *Improving community digital literacy*

Digital channels are now the preferred banking channels across Australia, as the graph[2] below demonstrates. A significant number of people continue to use face-to-face banking transactions.



Source: Retail Banking & Insurance Survey (April 2021), n=5,082

The use of digital banking services will continue to increase as cash use decreases and more services are brought online. While there is strong consumer preference for digital channels, some COBA members have noted that regional and rural customers, elderly customers, customers with disability and customers from diverse cultural backgrounds are more likely to be excluded from the digital transition.

COBA members have programs to assist their customers with the digital transition, but there is a broader role for government in ensuring all Australians are able to join the digital transition and access a digital inclusion program that meets their needs.

Ultimately, if these customers are excluded from digital banking services, they are also likely to be excluded from other digital services in our society.

- *The value of Open Banking needs to be communicated to consumers*

A bank account is a valuable data asset, but consumers are still focused on ensuring this data remains securely protected than on exploiting the data for their own benefit. Consumer research indicates that awareness of Open Banking remains low and understanding of the benefits is even lower. Customers are unlikely to share data under the regime without a clear, demonstrable benefit to doing so. Increasing awareness of open banking is not as important as increasing understanding of the benefits for customers.

The relative importance ascribed by consumers to key issues affecting their use of digital markets, data portability, and open banking vary, but the core themes are largely consistent[3]. These are:

- trust and transparency

[2] The Customer Imperative in Financial Services, Bain and Company & Salesforce

[3] Consumer Policy Research Centre Stepping towards trust Consumer Experience, Consumer Data Standards, and the Consumer Data Right accessed 04/10/2022

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

Optimising the use of open banking will require a sustained effort to uplift financial literacy and data literacy. COBA has advocated that the focus should be on a sustainable and safe expansion of the CDR regime so that consumers' trust in the digital market is safeguarded.

Recommendation direction and information request 3.4 Balancing cyber security and growth

The functioning of Australia's banking system is dependent on a secure cyber environment. COBA 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.

The 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. APRA's 2021-25 corporate plan[4] says cyber threats continue to be a material prudential risk, with increasing frequency and sophistication of cyber-attacks having the potential to create significant harms to the Australian financial system. ASIC's 2021-25 corporate plan[5] says a key priority is supporting enhanced cyber resilience and cyber security among ASIC's regulated population, in line with the whole-of-government commitment to mitigating cyber security risks.

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.

KPMG's 2020 Mutuals Industry Review reported that in 2020, the mutuals industry spent $231 million on technology expenses, an 8 percent rise from 2019 levels, and was driven primarily by technology expenditure in cybersecurity, mobile banking and technology changes to meet new regulatory requirements.[6]

Consumer products should have inbuilt malware and intrusion detection within the operating system or when connected to the internet. In an increasingly connected world from computers to whitegoods and children's toys, end point compromises make consumer products inherently vulnerable. We believe that proactive security measures such as built in cyclical updates could provide Australians with practical protections recognising that not every user understands the importance of updating in response to system vulnerabilities.

We note the interim report flagged automatic cyber incident reporting into security software. Enhancements to automated reporting, which reduce the burden on business to identify and report and have clear consent and usage disclosure, could assist greatly to keep consumers and businesses safe online.

Recommendation direction and information request 3.6 Coordinating the policy and regulatory environment

The following instances reflect poor coordination of policy and regulatory activity which have negatively impacted the innovation and productivity of COBA members. Our Regulatory Initiatives Grid

[4] APRA Corporate Plan 2021-25

[5] ASIC Corporate Plan 2021-25

[6] KPMG Mutuals Review 2020.

proposal is one way that financial services policy and regulation could be significantly improved for all stakeholders.

- *Scams*

The growing community cost of scam losses is a policy area where greater coordination is urgently required. Whilst many stakeholders, including regulators, law enforcement agencies and businesses have worked together to share information and strategies, gaps in the regulatory framework and a lack of coordinated approach has not effectively disrupted the scam cycle. Recent changes in telecommunications policy obligations have had a welcome impact but more remains to be done.

The government should establish a taskforce, comprised of regulators, banking representatives, payment providers, law enforcement officials, utility providers, relevant federal policy agencies and political representatives, to:

- Establish a framework for combatting scams via a strategy paper, similar to the Australian Cybersecurity Strategy 2020 and the Ransomware Action Plan 2021
- Establish themes and best practice for consumer messaging
- Establish and lead a workplan to measure and track the prevalence of scams and cybercrimes and any reductions

The creation of the AFP's Joint Policing Cybercrime Coordination Centre (JPC3) was a critical step in the right direction. Scams and cybercrime continue to pose a significant threat to customers and small businesses. While COBA welcomes existing efforts to combat cybercrime, governments must ensure that these crimes are not solely approached through a national security lens, but instead with a view to protecting consumers and convenient access to banking services.

- *Open Banking (CDR)*

Whilst COBA members support the intent of the Open Banking (CDR) regime, its implementation was unnecessarily burdensome, imposing significant opportunity costs on COBA members.

Implementation of CDR was a significant and complex technology transformation project occurring against a backdrop of a global pandemic and many other non-CDR regulatory change projects.

Whilst some COBA members are leaders in the CDR space, notably Regional Australia Bank, others have questioned the high priority that has been 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.

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

As noted elsewhere in this submission, some COBA members, along with other non-major banks, received 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 are working closely with the ACCC on individual roadmaps to compliance. The commercial marketplace for CDR compliance solutions remains developing rather than mature.

As challenger institutions in a market dominated by four major players, the key to improving the competitive position of our members in CDR terms is the capacity to become data recipients. 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.

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. CDR compliance is about enabling customers who wish to share their data with accredited recipients to do so in a safe and secure way. Above all, COBA members are determined to preserve the customer trust they have built up over decades.

The implementation of open banking made few concessions to proportionality. It exacerbated the competitive disadvantage of smaller financial institutions, who had no choice but to prioritise the resourcing of a regime that is yet to deliver clear consumer benefit.

As the Consumer Policy Research Centre noted, 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."[7]

The recent final report of the Statutory Review of the CDR[8] made the following recommendations:

- Recommendation 1.4 - To provide greater clarity and certainty to all participants, the Government, with CDR agencies, should provide greater transparency on CDR consultation processes and a timeline that outlines expected future developments.
- Recommendation 2.3 - CDR agencies should make it easier for participants and users to resolve issues and seek advice, including by clarifying responsibility and ownership of issues, coordinating consultation and system releases, and publishing comprehensive statistics on the progress of the CDR.
- Recommendation 2.5 - The current pace of CDR rollout into new sectors has not allowed enough time for the system to mature and capitalise on the lessons learnt. Focussing on improving CDR functionality and data quality within already designated sectors should be prioritised, balanced with overall forward momentum into new sectors over time.

The report made the following observations that may be useful to the PC:

> *"Many participants also noted that, aside from the consultation processes, the rules and standards had also not been implemented in a way that was appropriate to their business needs. Stakeholders felt that there was an assumption, upon release of rules and standards, that there were technical experts waiting at their computers for the latest implementation updates. This experience was exacerbated by concurrent consultations and updates to both rules and standards which made the CDR rollout a very demanding process for stakeholders."*

[7] CPRC, Stepping towards trust, p34

[8] https://treasury.gov.au/publication/p2022-314513 accessed 20/10/22

"We must also be alert to potential anti-competitive effects, The size, complexity and technical depth required to participate in the CDR does, of necessity, create a disproportionate burden for smaller, less sophisticated entities. The requirement to comply with rules and data standards should not be implemented in a way that stifles product innovation."

"The implementation architecture of the CDR is complex with multiple regulators. Given the economy-wide scope of the CDR and its deep technical demand and complexity, there is no obvious alternative at present. I believe that significant improvements are possible within the current architecture if all commit to greater coordination, so that roles are more clearly delineated, and I have been encouraged to see that CDR agencies are already actively working to this end."

- *Regulatory initiatives grid*

Existing regulation of financial services is labyrinthine and complex. While regulators are demonstrating greater sensitivity to the "should we" (decision for new regulation), the "how we" (proportionality) and the "when we" (timing) of new regulation at an individual level, the degree of coordination between creators of new regulation as a collective can be improved.

All significant regulatory policy decisions should be considered at a 'whole of system' level recognising that financial sector firms are subject to multiple layers of regulation and multiple regulatory bodies.

COBA is advocating to government that a pilot regulatory initiatives grid like that seen in the United Kingdom would assist regulators and policymakers to coordinate regulatory change and assist industry to plan and map out responses to regulatory change. This would be developed in continuing consultation with the financial services sector and other relevant stakeholders. It should be produced by Treasury given its role as the 'line agency' for the financial sector, utilising the Council of Financial Regulators as the coordinating body. This initiative would have minimal budgetary impact and would greatly assist businesses across the financial services industry to manage resources and focus on their customers

If you wish to discuss any aspect of this submission, please contact Sarah Wilson (swilson@coba.asn.au)

Yours sincerely

MICHAEL LAWRENCE
Chief Executive Officer