CyberCX submission to the Senate Select Committee on Financial Technology and Regulatory Technology

December 2019

INTRODUCTION

CyberCX, a leading Australian cyber security service provider, strongly endorses the Commonwealth Government's Open Banking initiative and its attempt to encourage greater competition within the financial sector.

Underpinning Open Banking is the Consumer Data Rights (CDR) principle. This principle contends that consumers, have 'the right to safely access certain data about them held by businesses.'1

Open Banking will enable consumers to transfer data to third parties in order to determine whether they qualify for preferential financial goods or services. The Australian Competition and Consumer Commission (ACCC) has been appointed lead CDR regulator. Organisations wishing to participate in the Open Banking initiative will need to obtain ACCC accreditation. This involves adherence to a rigorous set of information security and privacy protection rules.2

Only third party financial organisations that achieve ACCC accreditation will be authorised to receive consumer data.

About CyberCX

Launched in October 2019, the CyberCX group has united 12 of the country's most trusted cyber security companies to create a comprehensive end-to-end cyber security services offering to Australian enterprises and governments.

[1] Commonwealth of Australia, Treasury, *Consumer Data Right Overview* (Canberra: Commonwealth of Australia, 2019) <https://treasury.gov.au/sites/default/files/2019-09/190904_cdr_booklet.pdf> (accessed 20 November 2019) p.1.
[2] Commonwealth of Australia, ACCC, *Consumer Data Right – Project Overview* [website], <https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0> (accessed 26 November 2019)

With a workforce of over 400 cyber security professionals and national footprint of over 20 offices across Australia, CyberCX offers a full suite of cyber security services including: Consulting & Advisory; Security Assurance; Governance, Risk & Compliance; Managed Services; Integration & Engineering; Incident Response & Digital Forensics and Education & Training.

CyberCX is led by two of Australia's industry leaders:

CEO, John Paitaridis is a recognised leader in the Australian technology industry and business community. Prior to his roles with BGH Capital and CyberCX, John spent seven years as Managing Director of Optus Business, where he was responsible for Optus' enterprise group and subsidiaries, one of Australia's leading Information Communications and Technology (ICT) organisations.

Prior to Optus, John held a variety of Executive level roles at Telstra. John is currently the Chair of the Australian Information Industry Association (AIIA).

Chief Strategy Officer, Alastair MacGibbon was recently the National Cyber Security Adviser, head of the Australian Cyber Security Centre (Australian Signals Directorate) and Special Adviser to the Prime Minister on Cyber Security.

He has a private sector and government background and has served as the Government's eSafety Commissioner and established the Australian High-Tech Crime Centre while a Federal Agent with the Australian Federal Police.

CyberCX's partnership with Government

Cyber security plays a critical role in Australia's economic future and our mission is to enable our customers to thrive in a digitally disrupted world. We believe in the importance of government, industry and academic collaboration and are keen to partner to identify, protect, manage and respond to cyber threats and work to shape policy and educate the public to make Australia more cyber secure.

CyberCX is committed to contributing its expertise to government, with regular liaison with government departments and agencies including Home Affairs, ASD, ASCS and the Attorney General's Department over security issues and strategies.

Consumer confidence and trust

At the heart of Open Banking is the need to encourage greater competition within the financial sector by implementing measures that will more easily facilitate consumers changing financial institutions. Widespread inertia or 'stickiness' results in consumer reluctance to 'shop-around' or change the financial institutions with which they transact.

In November 2018, the ACCC released the 'Residential Mortgage Price Inquiry' report which found evidence of widespread consumer inertia in the financial sector:

'Large numbers of existing residential mortgage borrowers do not regularly review their choice of lender. All banks profit from the inertia of their customers. However, widespread inertia makes it challenging for Other Banks to win market share from the big four banks.'3

The ability to easily transfer financial data from one institution to another should result in greater consumer willingness to switch financial institutions, resulting in greater industry competition.

However, for Open Banking to successfully encourage greater competition, it is essential to engender strong consumer support for, and participation in, the initiative. This can only be achieved if consumers have confidence in the system and trust that their confidential data is transferred and stored securely. If data breaches occur as a result of insecure API transfers, or due to financial institutions not handling and storing received data in accordance with best practice standards, consumer confidence and trust in the initiative will be severely undermined. The result would likely be consumer reluctance to participate in Open Banking which would severely limit the initiative's ability to achieve greater competition in the financial sector.

The challenge for small and start-up organisations

CyberCX supports the case for ensuring consumers retain greater access and control over their data, in line with the CDR principle. However, we also strongly believe that rigorous information security and privacy protection measures are absolutely essential to safeguard consumers.

Under the Open Banking initiative, it is proposed that highly valuable consumer data be transferable via API and that multiple parties will be able to receive and store data. CyberCX is pleased to see the ACCC has developed extensive prospective rules around data transference, handling and storage requirements. We believe these rules, which align with many of the requirements of other information security regimes, such as APRA CPS234, will ensure consumer data is sufficiently protected.

It was therefore concerning to read in the Committee's Issues Paper that some small and start-up financial organisations believe the costs associated with meeting the ACCC rules will be a hinderance to their participation in the Open Banking initiative. According to the Issues Paper, FinTech Australia, which represents many small and start-up financial organisations, has stated that compliance costs of meeting the ACCC rules will average $50,000-$100,000 annually.4

---

[3] Commonwealth of Australia, ACCC, *Residential Mortgage Price Inquiry* (Canberra: Commonwealth of Australia, 2018) < https://www.accc.gov.au/system/files/ACCC%20Residential%20mortgage%20price%20inquiry%20-%20Final%20report%20November%202018_1.pdf> (accessed 26 November 2019) p.66.

[4] Commonwealth of Australia, Parliament of Australia, *Senate Select Committee on Financial Technology and Regulatory Technology – Issues Paper* (Canberra: Commonwealth of Australia, 2019) < https://www.aph.gov.au/~/media/Committees/fintech_cttee/Issues%20Paper%20-%20FinTech.pdf?la=en> (accessed 20 November 2019) p.19.

FinTech Australia goes on to suggest that compliance with the ACCC's CDR rules should be easier and cheaper than 'screen scraping'. There seems to be an indication that some small or start-up financial organisations would opt-out of Open Banking in favour of continuing to engage in 'screen scraping' unless the costs associated with meeting the ACCC rules are reduced.

'Screen scraping' by financial organisations typically occurs when a prospective consumer is seeking some form of loan. The proposed lender will obtain the consumer's login and password credentials to any of their pre-existing accounts with other financial organisations in order to determine the consumer's credit worthiness. CyberCX believes that 'screen scraping' of this nature is not best practice when it comes to information security or privacy protection. Often, consumers share their login and password credentials in an unencrypted format. Furthermore, many individuals use the same passwords to access a wide variety of online accounts. In the event of passwords being leaked, the individual risks having their other online accounts compromised. At a time when we should be seeking to instil in individuals a greater awareness of the importance of online security, encouraging people to reveal their passwords is precisely the wrong message. Our concern is that 'screen scraping' legitimises and gets consumers used to handing over their passwords to 3rd parties.

Maintaining high standards

CyberCX believes it is appropriate that participants in the Open Banking initiative meet the highest information security and privacy protection rules given the significant benefits they stand to gain from greater access to consumer data.

A way needs to be found that facilitates participation by small and start-up financial organisations in the Open Banking initiative, while not compromising data security by diluting the rules or encouraging 'screen scraping'. This is essential if competition within the industry is to be increased whilst ensuring public confidence and trust in the initiative is maintained.

It is currently proposed that there be one general level of accreditation under the CDR rules. However, there also seems to be a suggestion the ACCC may create more than one level of accreditation as the CDR regime matures.5 CyberCX would not wish to see a less onerous version of the ACCC rules in order to accommodate small or start-up financial organisations.

Were some financial organisations able to achieve accreditation through less rigorous rules, it would create an incentive for attackers to target those organisations. As stated previously, any data breaches would undermine consumer confidence and trust in the initiative.

[5] Commonwealth of Australia, Treasury, *Consumer Data Right Overview* (Canberra: Commonwealth of Australia, 2019) <https://treasury.gov.au/sites/default/files/2019-09/190904_cdr_booklet.pdf> (accessed 20 November 2019 p.8.

A compromise solution

CyberCX appreciates the financial challenges faced by new entrants into the industry. Meeting extensive security and privacy rules is a high barrier to entry. The Open Banking initiative will add to the rules in a number of ways, including through the extension of provisions contained in the Privacy Act to organisations with revenues under $3 million per annum.

Rather than resorting to 'screen scraping' or rule dilution, it would be preferable for the government to assist small and start-up financial organisations achieve the most rigorous information security and privacy protection standards. This could be accomplished through the establishment of either a loan or voucher scheme.

Loans could be offered to qualifying small and start-up financial organisations in order to invest in strengthening their cybersecurity postures and meeting the ACCC rules. These could be repaid once the organisation passes a specified revenue threshold. Alternatively, a voucher scheme could be established where government covers part of the costs of achieving a stronger cybersecurity posture.

Initiatives such as these will have the dual advantage of encouraging greater participation in the Open Banking initiative whilst enhancing the overall cybersecurity posture of the sector.

CyberCX welcomes any further opportunities to discuss the issues involved with the Open Banking initiative and the CDR principle.