HERBERT SMITH FREEHILLS

A NEW WORLD OF OPEN DATA AND CYBER RISKS

17 August 2020 | Australia
Legal Briefings – By **Peter Jones, David J Ryan and Marine Giral**

As the world continues to grapple with Covid-19, entire workforces and systems are operating remotely, creating increased risk to businesses. Now more than ever, cyber risk management needs to be at the core of your CDR strategy.

With the roll out of the latest phase of the Consumer Data Right (**CDR**) on 1 July 2020, large banks can now be required to share, with other banks and fintechs accredited by the Australian Competition and Consumer Commission (**ACCC**), their consumer data for deposit and transaction accounts, as well as for credit and debit cards.

That they must do so while facing a range of unexpected challenges caused by the COVID 19 epidemic, including a spike in malicious cyber activity associated with the rising use of remote technology, and as the Government is proposing to introduce an enhanced cyber regulatory framework for entities across all essential services (including financial, energy, communication) as part of its 2020 cyber strategy,[1] with the potential – in exceptional circumstances – for direct Government action in connection with specific threat events, simply increases the challenges.[2]

The expected increase in data portability resulting from the implementation of the CDR will bring a new set of security risks with:

- customer data moving to potentially lower security environments;
- greater reliance on APIs exposing to the risk of 'man-in the-middle attacks', and
- increased flows and volume of data creating one-stop-shops for malicious actors.

The CDR data security framework imposes a range of information security obligations on CDR participants to manage the security of their CDR data environment.[3] However this only partially addresses open-data cyber related risks. Focused as it is on the protection of CDR data, the framework does not (and nor should it be expected to) consider other risks to an organisation's critical assets, systems and operations.

Regardless of from where a cyber-incident emerges, CDR participants are exposed to regulatory, legal and reputational risks where such incident impacts their CDR environments. Given this context, it is imperative that their cyber strategies address the challenges and risks associated with the mandated sharing of CDR data.

REGULATORY RISK: WHO IS IN THE CROSSHAIRS?

Large CDR participants, particularly major banks which have been the subject of increased regulatory scrutiny by prudential and corporate regulators in recent years, will likely be a main focus when it comes to CDR enforcement.

The ACCC and OAIC's compliance and enforcement policy for the CDR[4] applies, understandably, to all CDR participants. However, the extent to which the two regulators will pursue enforcement actions (beyond the most egregious breaches) against smaller participants that one of them accredited remains unclear, especially given the objective of encouraging data portability.

The policy contemplates a proportionate approach to enforcing CDR rules, considering factors such as the size of the business, due to the greater potential for consumer detriment caused by the conduct of larger organisations.[5]

Regulators will also likely consider COVID-19's business impact, in particular for smaller data recipients. Earlier this year, the ACCC acknowledged the challenges to CDR projects caused by the changes prompted by the epidemic, including the difficulties maintaining or securing funding, global supply chain disruptions leading to inability to progress technology development and loss of key clients.[6]

LEGAL RISK: WHO BEARS THE RISK FOR CDR CYBER-INCIDENTS?

CDR related cyber-incidents (whether or not involving a breach of CDR data) can lead to legal actions brought by customers, shareholders or other affected third parties. Large data holders can expect to be the targets of most of those actions.

In the absence of specific rules on the allocation of liability, general principles should apply and each CDR participant will be responsible for its own breach of CDR security requirements.

Assessing which of the data holder or the recipient is at fault will however not always be clear, for example, if a malicious actor intercepts customer's data during transmission. In such circumstances, the Government commissioned review into open banking preceding the CDR stated that data holders should be liable for the loss suffered by the customer because of their failure to transfer the data at the customer's direction (in line with banking law liability framework relating to the transfer of money).[7]

Although the CDR provides that a CDR participant will not be liable to any civil or criminal action for or in relation to the transfer or disclosure of CDR data done 'in good faith' and in accordance with CDR provisions in the Competition and Consumer Act and the CDR Rules,[8] establishing compliance with all elements of the CDR regime will be difficult especially for absolute obligations such as that to keep data secure.

Regardless of the liability framework, customers are likely to expect large data holders to compensate them if the data recipient is unable to do so.

Contractual protections will not always be available in the context of the mandatory sharing of data. Even with such protections in place, it may not always be practical for large data holders to seek indemnities from smaller participants (especially those facing financial difficulties due to COVID-19). Insurance requirements under the CDR rules, which are limited to covering the risk to CDR consumers, only partially mitigate this risk.[9]

DATA SECURITY CONCERNS: A SHORT STEP TO LOSING CONSUMER TRUST AND BUSINESS

Beyond regulatory and legal risks, reputational damage can result from an incident even through no fault of the data holder. For example, the 2019 breach of the Australia's New Payments Platform was largely portrayed as a failure by the major banks, even though the breach came through the system of a client of another financial institution using the platform.[10]

Lost business associated with customer turnover is the largest contributor of a data breach cost (nearly 40% according to a leading study in the field).[11] In the financial sector in particular, real or perceived data security issues are quick to eroding trust in an organisation's ability to servicing its customers. In the aftermath of the banking commission, and as they must face rising customer expectations and new competition, maintaining a steadfast focus on data security is non-negotiable for large financial CDR data holder.

HOW ORGANISATIONS CAN MANAGE CDR RELATED CYBER RISK IN THE CONTEXT OF COVID-19

In a CDR recovering world, CDR participants addressing cyber risks as part of the opening of their data environments now do so in a context where cyber resources have been reallocated to address more pressing and urgent threats as malicious actors seek to take advantage of the changes wrought by COVID-19.

Principles and steps to guide the transition to a post CDR implementation world include the following:

- Prioritisation between responses to immediate, short term and medium to long-term threats must be carefully thought through and treated as a key issue for boards as well as responsible executives;
- Cyber knowledge and expertise sharing within and between teams will be key to an efficient and strong cyber response and must be part of an organisation's culture:
    - Most of the steps organisations can take to improve cyber resilience against COVID-19 related threats (see our briefing on five practical steps to manage cyber security risk during the pandemic) will improve their cyber security posture more generally including in the CDR context;
    - CDR cyber security teams temporarily reallocated to COVID-19 response should continue to be kept informed of CDR projects' progress, and consulted where strategic decisions are made;
    - Beyond specialised teams, cyber management is an organisation wide issue. Boards and staff at all levels must be trained on cyber risk, regardless of where the threat comes from.

CONCLUSION

With the roll out of the CDR progressing (see our CDR landing page for further information and updates on this), it is critical that your organisation, whether a mandated participant in the CDR ecosystem or one contemplating accreditation, puts management of information security and cyber risk at the core of your strategy for engaging with the CDR.

Our global team of cyber risk and crisis management specialists, comprising experts with technology, privacy, dispute and regulatory capabilities covering all aspects of cyber incident management, from crisis response through regulator engagement and remediation to litigation management, would welcome the opportunity to speak with you about how best to deploy an organisation-wide CDR security strategy.

ENDNOTES

1. Department of Home Affairs, Australia's Cyber Security Strategy 2020.

2. See eg Australian Signals Directorate's Australian Cyber Security Centre (ACSC) update on COVID-19 malicious activity; 'Australian slams coronavirus crisis cyber-attacks' (20 May 2020) Australian Financial Review; 'Recent cyber-attacks just the tip of the iceberg for Australia' (18 May 2020) Australian Financial Review.

3. Privacy Safeguard 12, Consumer Data Rules, Schedule 2, CDR Draft Accreditation Scheme (Draft Supplementary Accreditation Guideline and Information Security and Draft Information Security Control Guidance).

4. Joint ACCC and OAIC compliance and enforcement policy for the Consumer Data Right.

5. Ibid p 6.

6. Australian Competition & Consumer Commission submission to the Fintech inquiry (received 17 March 2020), available here.

7. Review into Open Banking: giving customer choice, convenience and confidence (December 2017), Table 4.2 (Liability case studies) p 66.

8. Section 56GC of the Competition and Consumer Act 2010, introduced by the *Treasury Laws Amendment (Consumer Data Right) Act 2019*.

9. *Competition and Consumer (Consumer Data Right) Rules 2020*, 5.12; see also Consumer Data Right's supplementary accreditation guidelines: insurance.

10. See eg 'Banks told to tighten security after payments data breach' (26 August 2019) Australian Financial Review; 'PayID data breaches show Australia's banks need to be more vigilant to hacking' (18 September 2019) the Conversation.

11. Ponemon Institute, 'Cost of a Data Breach 2020', p 10.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

JULIAN LINCOLN
PARTNER, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

PETER JONES
PARTNER, SYDNEY
+61 2 9225 5588
peter.jones@hsf.com

KAMAN TSOI
SPECIAL COUNSEL, MELBOURNE
+61 3 9288 1336
kaman.tsoi@hsf.com

DAVID J RYAN
SENIOR ASSOCIATE, MELBOURNE
+61 3 9288 1831
david.j.ryan@hsf.com

MERRYN QUAYLE
PARTNER, MELBOURNE
+61 3 9288 1499
merryn.quayle@hsf.com

REBEKAH GAY
PARTNER AND JOINT GLOBAL HEAD OF INTELLECTUAL PROPERTY, SYDNEY
+61 2 9225 5242
Rebekah.Gay@hsf.com

LEGAL NOTICE