Australian
Banking & Finance
Law Bulletin

Closing the deal on open banking

David Kreltszheim *CORNWALL STODART*

"Open banking" is shorthand for implementing the "consumer data right" (CDR) in the banking sector. The *Review into Open Banking: Giving Customers Choice, Convenience and Confidence*[1] (the Review) makes specific and detailed recommendations about implementation. But customer focus, competition, innovation, efficiency and fairness can sometimes be in the eye of the beholder: different interest groups will sometimes have different views about how to best create a CDR that achieves these aims. In responding to the recommendations of the Review, the federal government will need to balance the views of regulators, banking incumbents, new entrants and consumer groups.

What is the CDR?

The CDR is the right of Australian consumers to have "open access" to their data. This right was announced by the federal government on 26 November 2017,[2] in response to the Productivity Commission's recommendation in May 2017 that a "consumer" be given a new comprehensive right to access digital "consumer data" held by a data holder.[3]

In the context of the banking sector, "open access" means that a consumer can initiate a data sharing arrangement by directing the holder of their banking data to share their data with a third party (data recipient). That direction may include specific instructions on what data is to be shared and with whom, and the duration of the sharing arrangement. Broadly, the CDR is intended to enhance a consumer's ability to have their banking data used for the provision of a service that competes with, or complements, the service that the holder of their banking data provides to the consumer. These may include comparison services that will use a consumer's shared banking data to provide the consumer with tailored banking product recommendations.

Who can exercise the CDR?

The Productivity Commission recommended that the consumers who are entitled to exercise the data right should include single persons, family groups or other groups resident at a single address in the data holder's dataset, and any entity with an Australian Business Number (ABN) and a turnover of $3 million per annum or less.[4] In contrast, the Review[5] recommends that the CDR be available to *all* banking customers holding a relevant account in Australia.[6] This is because of the potential complexity of defining businesses within and outside the scope (eg, should the test be based on turnover or number of employees?), and the difficulty a holder of banking data will have in determining the status of a business at any point in time.

Who must comply with customer data sharing directions under the CDR?

The Review recommends that Authorised Deposit-taking Institutions (ADIs), other than foreign bank branches, should be subject to customer data sharing directions under the CDR.[7] Further, the Review recommends that the four major Australian ADIs should comply with their customers data sharing directions from the first day of operation of open banking, but the remaining ADIs should be obliged to share data from 12 months after that date, unless the Australian Competition and Consumer Commission (ACCC) determines that a later date is more appropriate.[8]

What data is within the scope of the CDR?

The Review's recommendations can be summarised as follows:

Type of data	Recommendation
Customer-provided data (eg, personal address and contact details, statements of financial position provided when opening an account or applying for a loan, and details of payees when instructing payments).	At a customer's direction, data holders should be obliged to share all information that has been provided to them by their customer (or former customer). But the obligation only applies where the data holder keeps that information in digital form. The obligation should not apply to information supporting an identity verification assessment.[9]

Transaction data (ie, data that is generated as a result of transactions made on a customer's account or service, such as records of deposits or withdrawals, account balances, interest earned or charged, and other fees or charges incurred).	At a customer's (or former customer's) direction, data holders should be obliged to share all transaction data in a form that facilitates its transfer and use. The obligation should apply for the period that data holders are otherwise required to retain records under existing regulations.[10] The obligation should only apply in relation to 16 specified types of deposit products[11] and 11 specified types of lending products.[12]
Value-added customer data (ie, data that results from effort by a data holder to gain insights about a customer — including income/asset checks, customer identity verification checks, credit reporting data, credit scores, data on an individual customer that has been aggregated across the customer's accounts and standardised, cleansed or reformatted to make it more usable).	Data that results from material enhancement by the application of insights, analysis or transformation by the data holder should not be included in the scope of open banking.[13] But if directed by a customer to do so, data holders should be obliged to share the outcome of an identity verification assessment performed on the customer, provided the anti-money laundering laws are amended to allow data recipients to rely on that outcome.[14]
Aggregated datasets created when banks use multiple customers' data to produce de-identified, collective or averaged data across customer groups or subsets (eg, average account balances by postcode or income segment, or average size of small business overdrafts by industry segment).	Aggregated data should not be included in the scope of open banking.[15]
Product data (features of the products that banks provide to customers).	Where banks are under existing obligations to disclose information on their products and services — such as on price, fees and other charges — that information should be made publicly available under open banking.[16]

Regulatory framework to implement the CDR

The banking sector is the first sector in which the CDR is to be implemented. As a result, the Review has outlined the proposed framework for implementing the CDR generally, as well as for implementing the specific rules needed for open banking. Broadly:

- The Competition and Consumer Act 2010 (Cth) will be amended to set out the general (non-industry specific) objectives of the CDR.
- A particular industry sector (like banking) will be designated by ministerial direction as a sector in which the CDR will apply.
- The Competition and Consumer Act will enable regulations and operational rules to be established for the application of the CDR to a particular sector.
- The rules for open banking (and other sectors in which the CDR will apply) will be determined by the ACCC in conjunction with the Office of the Australian Information Commissioner.
- There will be a set of open banking standards sitting under the open banking rules: these standards are to ensure efficient and simple implementation and compliance, interoperability between accredited parties within and across sectors, and to promote competition (amongst other things, these standards will deal with methods for data transfer, data standards and security standards).[17]

Open questions about open banking

The Review is specific, detailed and wideranging. I do not know how it was produced so quickly. Almost every issue one can think of is identified and dealt with. What follows is a shallow dive into two areas that I believe would be of interest to banking, regulatory and fintech lawyers generally.

Is Tournier v National Provincial & Union Bank of England[18] (Tournier) adequate for customer data that is not personal information?

As noted above, the CDR will be exercisable by companies and other artificial legal persons, not just natural persons. The Review notes that as such customers' data may not be personal information, the Privacy Act 1988 (Cth) will not cover all of the data involved in open banking.[19] The Review adds that:

> … remedies for privacy breaches for some businesses will lie under the common law. The common law imposes a contractual duty of confidentiality on banks not to disclose the affairs of their customers — whether individuals or businesses — unless the disclosure falls within four limited exceptions.[20]

The Review then recommends that small business customers should be given access to external and internal dispute resolution services for confidentiality disputes similar to those that exist for individuals under the Privacy Act.[21]

There are several obligations that could (and perhaps should) be imposed on a bank when it handles a customer's data that is not personal information. In the same way that organisations handling personal information under the Privacy Act have obligations that go

beyond just keeping personal information confidential, should banks handling customer data that is not personal information be subject to obligations as to:

- the purposes for which they use that data
- the quality of that data
- notification of data breaches in relation to that data and
- other matters that apply to the handling of personal information under the Privacy Act?

Some other jurisdictions recognise that bank confidentiality should be expanded to address the proper use by banks of the confidential information that they hold.[22] If such an expansion is to occur in Australia, it would need to be by statute.

The Review notes that:

> The Rules, in conjunction with the Privacy Act, need to address customer rights and competition, as well as the confidentiality aspects of Open Banking. As the [Australian Privacy Principles (APPs)] in the Privacy Act do not apply to non-personal information, it may be necessary to include confidentiality rules in the CDR for such information (which includes business information) that mirror some of the protections in the APPs.[23]

The references to "confidentiality" and "some of the protections" may suggest that a CDR system participant's handling of customer data that is not personal information will be regulated in relation to disclosure (confidentiality) only, in line with *Tournier*. However, the Review includes example "direction to transfer" rules that stipulate that:[24]

> … though the data recipient does not need to inform the data holder of all intended uses, there are prescribed uses that should be presented to the customer for permission (consent) to be considered informed. These uses would be expected to include:
>
> - the primary purpose for which the data is being transferred
> - on-selling of data
> - direct marketing
> - transfer of data outside the Consumer Data Right system; and
> - transfer of data overseas.

I agree with this approach. In my view, there are conceptual and practical difficulties with imposing Privacy Act-type obligations across the board on data recipients when they handle customer data that is not personal information. But it would be appropriate to impose more limited Privacy Act-type use and disclosure and notification obligations on such data recipients, at least where the data relates to small business customers. This seems to be the direction in which the Review is heading.

Should "screen scraping" be prohibited?

The Review notes that in the absence of an open banking solution, "screen scraping" technology is used by many fintech businesses to access a customer's banking data:

> This involves the customer providing their FinTech, or an associated "data aggregator", with their access credentials that the FinTech uses to log into the bank's online banking interface. The technology then extracts the customer's data — such as their account balance and transactions — from the information that the customer would be able to see on the screen.[25]

The Review adds that screen scraping is "risky, unstable and costly" and is presently popular out of necessity, not because it is an elegant technology design for data sharing.[26]

In relation to risk, the Review notes that screen scraping may adversely affect a customer's protection from fraud. This is because the customer's handing over of login credentials to enable screen scraping may be a violation of the bank's terms and conditions. As a result, the customer may bear fraud risk if those credentials are compromised.[27]

In the end, the Review concludes that open banking should not prohibit or endorse screen scraping, but should aim to make this practice redundant by facilitating a more efficient data transfer mechanism.[28]

An issue that is related to screen scraping is the issue of "payment initiation" or "write access" as it is described in the UK. Write access is the ability of a customer to give third parties the ability to transact on the customer's behalf (eg, by initiating a payment). Write access is sometimes facilitated by screen scraping technology.[29] The Review notes that payment initiation or write access was not part of the terms of reference for the review and so has not been considered to be part of the initial scope of open banking in Australia.[30] As a result, write access, like screen scraping generally, still dwells in an uncertain place.

Customer focus, competition, innovation, efficiency and fairness (the guiding principles for the Review)[31] can sometimes be in the eye of the beholder: different interest groups will sometimes have different views about how to best create a CDR that achieves these aims. In responding to the recommendations of the Review, the federal government will need to balance the views of regulators, banking incumbents, new entrants and consumer groups.

David Kreltszheim
Special Counsel
Cornwall Stodart
d.kreltszheim@cornwalls.com.au
www.cornwalls.com.au

About the author
David is a banking, payments and regulatory lawyer. In addition to his work for clients, he publishes and presents widely on these topics.

The views expressed are the author's and do not necessarily reflect those of Cornwall Stodart.

Footnotes

1. The Treasury *Review into Open Banking: Giving Customers Choice, Convenience and Confidence* (2017) https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf.
2. See A Taylor "Australians to own their own banking, energy, phone and internet data" (26 November 2017) https://ministers.pmc.gov.au/taylor/2017/australians-own-their-own-banking-energy-phone-and-internet-data. Amongst other things, the government's media release noted that it would legislate a national CDR allowing customers open access to their banking, energy, phone and internet transactions. This was to enable customers to compare offers, get access to cheaper products and plans, and help them to "make the switch" and get greater value for money.
3. Productivity Commission *Data Availability and Use: Inquiry Report* Report No 82 (2017) 199 (recommendation 5.1).
4. Above n 3, at 198.
5. Released publicly on 9 February 2018. The reviewer (Scott Farrell) requested that any further detailed submissions be made by 23 March 2018.
6. Above n 1, at 41–2 (recommendation 3.7).
7. Above n 1, at 43 (recommendation 3.8).
8. Above n 1, at 97 (recommendation 6.2).
9. Above n 1, at 34–5 (recommendation 3.1).
10. Above n 1, at 35–7 (recommendation 3.2).
11. Namely savings accounts, call accounts, term deposits, current accounts, cheque accounts, debit card accounts, transactions accounts, personal basic accounts, GST and tax accounts, cash management accounts, farm management deposits, pensioner deeming accounts, mortgage offset accounts, trust accounts, retirement savings accounts and foreign currency accounts: above n 1, at 37 (table 3.1).
12. Namely mortgages, business finance, personal loans, lines of credit (personal), lines of credit (business), overdrafts (personal), overdrafts (business), consumer leases, credit and charge cards (personal), credit and charge cards (business) and asset finance (and leases): above n 1, at 37 (table 3.1).
13. Above n 1, at 38 (recommendation 3.3).
14. Above n 1, at 39 (recommendation 3.4).
15. Above n 1, at 39–40 (recommendation 3.5).
16. Above n 1, at 40 (recommendation 3.6).
17. Above n 1, at 14–21 (recommendations 2.1, 2.2, 2.3, 2.4 and 2.5).
18. *Tournier v National Provincial and Union Bank of England* [1923] All ER Rep 550; [1924] 1 KB 461.
19. Above n 1, at 58.
20. Above n 1, at 58. The Review cites *Tournier* and adds that the duty of confidentiality is implied into the contract between a bank and its customer and that the exceptions include where the disclosure is made with the express or implied consent of the customer, is required by law, is necessary for the fulfilment of a public duty or is necessary to protect the legal rights of the bank.
21. Above n 1, at 59 (recommendation 4.4).
22. G Godfrey, D Newcomb, B Burke, G Chen, N Schmidt, E Stadler, D Coucouni, W Johnston and W H Boss "Bank Confidentiality — A Dying Duty But Not Dead Yet?" (2016) 17(3) *Business Law International* 173 at 186, citing an Austrian statute that provides that banks may not disclose *or exploit* secrets that were entrusted to them, or to which they received access, solely based on the business relationship with clients.
23. Above n 1, at 18.
24. Above n 1, at 136.
25. Above n 1, at 72.
26. Above n 1, at 72.
27. Above n 1, at 72 and also 51–2.
28. Above n 1, at x.
29. Above n 1, at 51.
30. Above n 1, at 2.
31. Above n 1, at 8.