12 October 2018

Equifax submission to Australian Competition and Consumer Commission
on the
Consumer Data Rights Rules Framework

Thank you for the opportunity to comment on the Consumer Data Right (CDR) Rules Framework (released 11 September 2018).

Equifax is a global information solutions company. We use data, innovative analytics, technology and industry expertise to transform knowledge into insights that help our customers make informed decisions. Headquartered in Atlanta, Equifax operates in North America, Central and South America, Europe and the Asia Pacific region.

Established as The Credit Reference Association of Australia in 1967, then as Veda and now Equifax, we have deep and long experience in data governance across the information lifecycle. We continue to invest in our data and security processes, systems, people and policies.

Our comments broadly follow the contents of the Framework, but we don't comment on all topics. For ease of reading we have grouped some related topics.

Intermediaries, Outsourcing and Data Minimisation

Various sections (for example, sections 6, 8, 9 and 12) of the Framework discuss outsourced service providers, intermediaries and the principle of data minimisation (disclosing only the minimum data necessary in each circumstance) through informed consent and fine-grained authorisation.

The Framework proposes that an outsourced service provider not be an accredited data recipient. It undertakes certain functions, such as collecting CDR data, on behalf of an accredited data recipient and has no rights under the CDR regime. A simple example is a cloud computing provider.

In contrast, as outlined in the Framework, an intermediary:

- 'would directly participate in the disclosure process flow [and] would need to be accredited'[1].
- may not necessarily interact with consumers directly but passes on CDR data to other accredited data recipients.
- may facilitate a tiered accreditation system.

Based on our experience both here and with the UK open banking regime, we believe a form of data governance intermediation will be necessary for the CDR regime to scale while maintaining privacy through data minimisation and facilitating innovation that benefits consumers.

Such a function might be more analogous to the clearing mechanism in the payments network or the Australian securities exchange. Such a data clearing function can be achieved either as an outsourced service provider (providing discrete services to each accredited data recipient as agreed) or an intermediary (accredited as a data recipient described in the Framework). We suggest a data clearing mechanism, operating as an accredited data recipient, will be more beneficial for the CDR regime.

The benefits include not only tiered accreditation, but also stronger data security, clearer lines of liability and responsibility and more direct regulatory oversight and control contributing to consumers' confidence in the CDR regime. This does not exclude the need for certain outsourcing arrangements, such as cloud computing services.

Many of the examples contemplated in the Framework and the related draft Bill[2] involve a single consumer requesting data from a single account, held with one bank and used for a single purpose. We expect reality to be almost entirely the complete opposite.

[1] Page 51 Rules Framework
[2] Treasury Laws Amendment (Consumer Data Right Bill 2018); released 24 September 2018.

Consumers typically have multiple accounts across multiple banks. Even use cases that only require one-time access to CDR data, for example comparing financial products to find one that best suits a consumer's circumstances, are likely to involve access to multiple relevant accounts across multiple banks.

More innovative uses cases, for example a personal financial management application (PFM App), are likely to require regular access to CDR data across multiple accounts and banks. Standard APIs make data sharing easier but are not seamless. For example, standards change over time (refer to API version control being proposed by the data standard body). It's inconceivable for every data holder to update all its APIs, across all accounts and data systems, at the same time as every data recipient updates their API request protocols. Different API versions will operate across the network of participants.

Behind the scenes, reality quickly begins to look like a web of connections and data flows rather than the highly idealised single, straight lines between consumer, data holder and data recipient.

A data clearing mechanism goes beyond maintaining the pipes between data holders and data recipients. The coarse-grained, non-derived CDR data that will be offered by data holders under a free-of-charge arrangement, may not be as useful as it appears on paper.

Four examples may demonstrate the point:

1. It is easy to add and subtract credit and debit transactions to arrive at an account balance. It is another matter to do calculations that a consumer may find more helpful; for example, to validate interest on the account. This requires knowing the date a transaction is cleared rather than the date the transaction is posted to the account and various other rules that apply to the account.
2. Generally, categories recorded against account transactions can differentiate a debit and credit or fees and interest charged by the bank itself. Those transactions won't record detailed merchant information. For example, where a merchant is a clothing store. Such information may be more useful for consumers if they want to manage discretionary spending via a PFM App, for example.

3. The bank account won't record that a credit transaction is the consumer's employment income. This means it won't be possible for a bank, without further value-added analysis, to disclose only employment income and no other credit transactions.
4. Similarly, bank transaction records can't identify that a debit transaction is a payment to a medical specialist and mask such sensitive information before disclosure. Such fine-grained distinctions can be achieved by linking disparate data sets and smart analytics. That becomes value-added or derived data under the CDR regime.

Some data holders may be capable of offering such value-added analysis. But even larger data holders may consider providing such services, even for a fee, to accredited data recipients to be outside their core business priorities.

The Framework contemplates disclosure of only the minimum data necessary for the agreed use (data minimisation principle). Based on our experience, as the CDR regime expands to a network of interconnections, achieving this principle will involve some data clearing mechanism. It is preferable to contemplate how such a mechanism should operate from the outset.

We suggest overall trustworthiness and integrity of the CDR system is better achieved by:

- requiring intermediaries, that do more than simply store the data, to be accredited rather than outsourced service providers, thus;
- minimising the risk of data recipients evolving to offer somewhat token consumer services but whose business is really data clearing between industry participants.

Data Sets (Section 5)

The Framework lists various types of data under three data sets; Customer Data, Transaction Data and Product Data. In addition, we suggest:

- Product data specific to a consumer's account, for example applicable fees (which may be different standard product fees) and any credit limit.
- The interest rate applicable to the consumer's account, keeping in mind that interest rates change over time and may be stored like transactions rather than at the consumer or account level.
- Total interest and fees charged over the period requested (this could help consumers complete tax returns for example).

We make the following observations about the proposed data sets:

- Direct debit authorisations are not typically stored by the financial institution holding the account on which the debit is authorised. The authority is usually held by the organisation (for example a merchant) that initiates the direct debit.
- The proposed opening and closing balance may be misleading. For example, without the date a transaction clears, it will be impractical to accurately re-calculate interest. Unless the data is requested on the last day of the financial year the closing balance may not accurately reflect information that could help consumers complete tax returns for example.

Finally, we suggest deeper consideration may be needed for the following points:

- Account level contact details for complex account ownership. The Framework contemplates how joint account holders may be notified before a data recipient collects CDR data. How this notification operates is still being reviewed. However, it is conceivable that one joint account holder consents to sharing transaction and account data but does not consent to sharing their contact details.

- Some online banking systems allow consumers to attach related electronic documents (an invoice or email for example) to a transaction record. This represents a value-added service (usually free of charge) for consumers (akin to a service that might be offered by a PFM App, for example) rather than a potential CDR data set collected and maintained by the bank as original data holder.
- Electronic copies of account application forms, to the extent these are available, may hold additional personal information (for example, a signature) or other sensitive information that cannot be masked and poses an increased risk to privacy if included in the CDR data set.
- Transaction metadata can be valuable but some (for example, geolocation of a transaction) may pose an increased risk to privacy if included in the CDR data set. For example, it may be possible in some circumstances for geolocation data to be used to reasonably accurately re-identify anonymised data.

Accreditation (Section 6)

The Framework outlines strong criteria for accreditation. In addition, we suggest further consideration be given to what happens in the following circumstances:

- A data recipient's accreditation is revoked. Clearly the data recipient will not be able to receive new CDR data. But will the data recipient be required to de-identify or delete the CDR data collected while they were accredited? How would this be enforced if, for example, the data recipient goes out of business?
- A data recipient is taken over, or control changes or there are other material changes in circumstances (for example, insurance). Will the data recipient be reassessed and, if so, what happens to their ability to collect and use CDR data between the time of the change and the re-accreditation?

Consent (Section 8)

The Framework appropriately places the consumer at the centre of the CDR regime by laying down strong consent arrangements. With the intention of building on the resilience of the proposed arrangements, we suggest the following points may need to be considered.

Complex Accounts

Consistent with our comments above, it is important that joint account holders and joint operators (for example, directors of a company) have a clear mechanism to understand and manage consents and how data is being shared. There are significant differences between the UK open banking framework, its interpretation and implementation of the EU General Data Protection Regulation (GDPR) and the proposed Australian CDR regime. Rising ambiguity about the role of intermediaries and liability in the UK regime suggests caution in adopting, as is, the UK Customer Experience Guidelines (dated September 2018).

At the time of the first interaction with a consumer, the data recipient is unlikely to know that the account has a joint holder or operator or their contact details. Data holders will know the authorities to operate an account and will usually have the most up-to-date contact details. For this reason and to reduce ambiguities, we suggest that consent to share data is best aligned to the authorities to operate an account.

This approach raises a practical distinction between consent and notification. Explicit and informed consumer consent certainly occurs before any data collection. Notification may be more reflexive.

For example, the data holder receives (via the data recipient) a valid data request from an authenticated account holder who has authority to transact on the account. The data holder notifies any joint account owners of the valid and authenticated request to disclose data.

In this example, does the data holder need to wait until notification is acknowledged before sending the data? What happens if the notification is not received by the joint account holder (for example, they have changed contact details or are travelling)?

Other regulatory notification rules deal with notification using a reasonableness test (the data holder must take reasonable steps to notify joint account holders). The alternative of requiring a data holder to wait until all account operators have consented to the disclosure is likely to increase frictions without an offsetting benefit to consumers.

The importance of this consent and notification arrangement cannot be underestimated. It has significant potential implications in the event of a breakdown in relationship between account holders. Our submission is not intended to cover all the issues and perspectives but merely to raise the concern for further consideration.

Informed Consent

The Framework outlines how consent must be provided in a way that is easy to understand while ensuring consumers are fully informed. Such rules are essential to building long lasting trust in the CDR regime. However, we suggest care needs to be taken not to assume how consumers will interact with participants to use their data rights.

For example, the Framework states that consent should not cross-reference other documents.[3] This is a potential safeguard against important information being buried at the end of long documents that consumers can only access by clicking a series of links. However, this approach appears to assume consumers will interact through a computer or large screen device rather than a mobile phone application. Such assumptions could curtail many innovations designed to benefit consumers.

We suggest that testing consumers' comprehension of the consent process, as outlined in the Framework[4], is an effective way to ensure flexibility and innovation without compromising consumers' rights.

Consent Dashboard

The Framework sets out the need for data holders and data recipients to maintain a dashboard for consumers to review and manage consents and data sharing arrangements. We support this proposal however, as a practical matter, we question how these dashboards will be maintained over time and how consumers will obtain an overall view of their arrangements across multiple participants.

[3] Page 36
[4] Page 36

For example, will a consumer, who is no longer a user of a data recipient's service, still have access their historical consents? What happens to the consumer's dashboard if the data recipient ceases to operate the relevant business for which they were accredited?

Authorisation and Authentication (Section 9)

The evolution of the UK open banking regime highlights important lessons. As noted in the Framework, the UK regime operates as a read and write arrangement. An ability to make a payment on an account has significant implications for where to strike an appropriate balance between strong authentication, acceptable frictions in the workflows, ease of use and speedy access to data. This may be less relevant when balancing the risks and benefits in a read-only regime.

The recent version of the UK Open Banking Customer Experience Guidelines highlights the need for flexibility to adapt to how consumers prefer to engage with services and the standards they expect from participants. What started as a "redirect" authentication model for example, is expanding to both "decoupled" and "redirect" authentication.

Monitoring service level standards (the UK facilitates this via an open forum) and taking regulatory action against valid complaints and unacceptable frictions is likely to be an appropriate approach in the first phase of the CDR regime.

Providing data to Consumers (Section 10)

Many online banking systems already given consumers an ability to download data (account transactions and payee lists for example) in a variety of useful formats. As a practical matter, it's hard to envisage how a typical consumer would interact directly with an API. However, as the CDR expands to other industries, direct-to-consumer access may become more relevant.

We support direct-to-consumer access but raise one note of caution. Unscrupulous operators may seek to circumvent accreditation and liability by encouraging consumers to access their data themselves and pass it to an unaccredited recipient.

We would be happy to discuss any of the points raised in this submission, or other matters related to the Framework. Please contact Julie McKay, General Manager, Strategy Australia and New Zealand [redacted]

END OF DOCUMENT