



October 12, 2018

ELECTRONICALLY SUBMITTED

Australian Competition and Consumer Commission
23 Marcus Clarke Street
Canberra, Australian Capital Territory, 2601

Re: Request for Comments on Consumer Data Right Rules Framework (“Framework”),
September 2018

To Whom It May Concern:

Investnet Yodlee (“Yodlee”) appreciates this opportunity to share its perspective in response to the Australian Competition and Consumer Commission’s (“ACCC”) request for comments on its rule-making framework to implement the Consumer Data Right (CDR) Rules (“CDR Rules”). As the leading global financial account data aggregation platform provider, with nearly two decades in the industry, and eight years in Australia, Yodlee strongly supports technological innovation and rule-making to safely empower and protect consumers by increasing competition between responsible providers of products and services designed to improve the financial wellbeing of consumers and small businesses.

Yodlee is a business-to-business, consumer-permissioned financial data aggregation and analytics platform. Financial institutions and financial technology firms license the Yodlee platform to provide their customers with innovative products and services that help them achieve positive financial outcomes. These customers use Yodlee-powered services to enable millions of retail and small businesses consumers, borrowers and investors to access and share their financial data using the tools and providers they’ve selected to help them improve or maintain their financial wellness. These applications include use for personal financial wellness management, underwriting and affordability checks for responsible lending and investment advice.

Yodlee’s customers include 12 of the 20 largest banks in the United States and global institutions in more than 20 countries, including Bank of America, Goldman Sachs, Wells Fargo, and American Express. Leading global financial innovators like Kabbage and PayPal are also Yodlee’s customers, as are approximately 60 Authorised Deposit-taking Institutions (ADIs) and fintechs in Australia

The ACCC’s decision to seek public comment on the CDR Rules Framework and its application to Open Banking is both necessary and timely since industries across sectors are increasing their efforts to collaborate with regulators and policymakers on such important consumer protection issues. As an international services provider, Yodlee is engaged with policymakers globally to provide input into their national or, in some cases, continental, privacy standards. We appreciate this opportunity to contribute to the ACCC’s rule-making efforts.

1. General obligations and structure of the Rules Framework

Yodlee supports the ACCC's general structure of the Rules Framework. However, Yodlee strongly recommends that the CDR participants *expressly* include, starting with the first version of the Rules, the role of technology service providers that are intermediaries between the data holder and the ADI (specifically, data aggregators). This is considered later in the Rules and is a reoccurring theme in this submission. Only by including the data aggregator as a CDR participant can the core principles of consent, authorization and authentication be applied uniformly and with the full protections contemplated in the draft legislation. The UK Open Banking framework made the mistake of excluding the data aggregator from the authorisation framework, which has essentially invalidated the transparency and traceability requirements, rendering the liability protection provision incomplete.

2. Sharing data with third party recipients

Yodlee agrees with the general principles expressed in this section, with two important exceptions.

The first is in regards to the proposed Process Flow in Section 2.1 of the Rules Framework, which is missing the data aggregation technical services provider. As previously stated, this role in the ecosystem must be as an independently authorised party to fully support the core requirements of the CDR, starting with the first version of the Rules.

The second exception is the requirement in Section 2.2 of the Rules Framework, that application programming interface (API) is the only method of permissioned data access. This is the correct aspiration, but is not practical for the first version of the Rules for July 2019 nor, in our experience, for two to three years after that date. There are both technical and commercial impediments to fully achieving this goal. Technically, not all data holders' internal systems can access all their customers' data to generate a single view of the customer. Without this internal data facility, they cannot publish an API to access the data per the data access standard. The internal work necessary to publish all required data sets will take time and money, neither of which have been allocated on the ADIs' technical roadmaps and technology budgets.

If all the data sets are not available via the API, and the API is the only approved mechanism for data access, the consumers' rights to their data will be denied, which will lead to bad financial outcomes for consumers, especially those consumers already using financial tools and services. For this reason, Yodlee strongly recommends that the ACCC include in the first version of the Rules the express provision for screenless data capture as an alternative approved method of data access, and instruct the Data Standards Body to incorporate this in standards development. Screenless data capture is a type of screen-scraping that can be implemented with full adherence to the core principles of the CDR, including consent, authorization and traceability. The inclusion of screenless data capture will ensure that consumers are empowered and protected during the implementation phases of Open Banking and subsequent initiatives.

3. CDR consumer – who may take advantage of the CDR?

Yodlee generally supports the ACCC's proposal for who may take advantage of the CDR for the first draft of the Rules. As contemplated by the draft legislation, this topic is both important and connected to the consent principle, so must receive attention for subsequent versions, as payment transaction data may contain information about other consumers (i.e. not the account holder) that could fall under the CDR.

4. Data holder – who is obliged to share data?

Yodlee agrees that a phased roll out is appropriate, but submits that the proposed approach is too conservative as it could lead to *less* competition and denial of consumer rights during the transition period. Specifically, limiting the first phase to the four major banks and not their related brands nor other ADIs does not recognize that consumers have already made competitive choices and exercised their rights in selecting their ADR(s). Therefore Yodlee recommends that the first phase include at least the related brands of the four major banks and offers incentives for other ADIs to accelerate their participation.

Yodlee also suggests that mortgage product data is essential to the competition and benefit goals of the CDR. As this is simply product data, it's inclusion in the first phase of the Rules is recommended.

In regards to the process to assess exceptions to the Rules, Yodlee cautions that consideration must be given to the impact of such exceptions to the consumer and their rights. In particular, the ACCC must consider the risk that incomplete data could cause a consumer to receive, for example, an incorrect lending decision or poor financial advice. In each of these examples, there is also impact to the ADR ranging from financial loss to compliance violations.

5. Data sets – what data is within scope?

The scope of data is an extremely important and complex topic that requires appropriate consideration in the Rules for the first phase. Yodlee submits as the guiding principle, that "minimum inclusion" is defined as all data available to the consumer via the data holder's native interfaces (e.g. online and mobile channels) so that this data are available to the consumer, and their designated ADR, via the technical standard.

6. Accreditation

Yodlee generally supports the ACCC's proposed rule-making for accreditation, but disagrees with Section 6.8 of the Rules in favor of accreditation of the data aggregation technology provider as an essential element to ensure end-to-end traceability and liability enforcement. To best support innovation, Yodlee recommends that as part of the inclusion of the data aggregation technology provider as an ADR, the aggregators' role be allowed to extend their control framework to their client's ADRs. The data aggregators, in general, have mature and rigorous control programs and, as is the case for Yodlee, are already assessing and managing

their clients in this way as part of their commercial governance. With each party carrying their own ADR authorization, the entire ecosystem is protected.

A risk-based, or tiered, system of accreditation is appropriate. In Yodlee's experience, objective criteria is essential to ensuring that ADRs understand their requirements and can demonstrate adequacy of their controls. References to national standards are helpful here, analogous to the way that defining prescriptive requirements like PCI-DSS are for the payment card industry.

7. The Register

Yodlee generally supports the ACCC's proposed rule-making for the Register

8. Consent

As the ACCC states, consent is a complex topic and requires consideration in the user experience to ensure that consumers are able to manage their consent and that ADIs and ADRs may rely on the consent architecture in their handling of the consumers' data.

In Yodlee's experience, there are two complementary forms of consumer consent. The first is the general consent the customer gives to their ADR to access and use their data. This consent is given as part of the terms and conditions of the ADR's service and encompasses the full relationship. The second is the consent the consumer gives to the ADI to release their data to the ADR. This consent informs the data set(s) to be provided and helps enforce the consent standards. This also amends the consent the consumer gave the ADI when they opened their account(s) regarding data sharing with unaffiliated third-parties; a typically thorny issue with pre-open banking data sharing mechanisms. You have captured this in Section 8.2 of the Rules.

The considerations for the nature of consent are difficult to apply prescriptively uniformly across the ecosystem as consumers have varied levels of education, language skills, financial acumen and technical facilities. The risk of harm to the consumer from abuse of their consent must be balanced with the risk of harm from their inability to access the financial tools and services they need to improve their financial wellness. It is well known in the industry that those consumers most in need of financial assistance services are least able to navigate complex "legalese", especially on a small handheld device. Therefore disclosure language and consent granting user interfaces must be fit for all purposes; not just regulatory compliance.

The scope of consent, such as specificity and time, is also a complicated issue that requires balanced rule-making. For example, many ADR solutions are "set it and forget it", such as transaction alerts or roll-up saving plans. In such cases, asking the consumer to reauthorize every 90 days, absent an explicit trigger, is a poor user experience that could deny them the benefit of the service. Likewise, too much specificity of consent for the data set, for example at the field level, would require the ADR to update the consent for small innovations in the use of the data, which would result in a poor user experience. Yodlee recommends

that the consent architecture is developed with broad representation from the ADI and ADR communities, with direct connection to the accreditation and security aspects of the authorisation programme.

9. Authorisation and authentication process

Yodlee is generally supportive of this proposed rule-making, with some important exceptions.

We agree unreservedly that user testing is required and must be part of the body of work conducted by the Data Standards Body.

We also agree that multi-factor authorization is a necessary control for the data holder's release consent flow, but submit that the PSD2 RTS, while informative, is not sufficient for the entire ecosystem of data sharing under the CDR; so more work is necessary by the Data Standards Body; especially in the application of CDR and the technical standards to non-API data sharing.

We reiterate our recommendation that enforcement of a 90 day reauthorisation for all use cases is not warranted as it will lead to poor user experiences without a corresponding increase in protection.

We fully agree with rule-making that would prevent data holders from adding non-standard requirements as in our experience, this leads to poor user experiences and anti-competitive situations.

We agree that a consumer "dashboard", so that consumers can revoke consent at the data source, is desirable. However, in our experience, this can lead to non-compliance if not implemented correctly. Accordingly, we recommend this receive attention with broad input by the Data Standards Body.

10. Providing consumer data to consumers

Yodlee is generally supportive of the ACCC's proposed rule-making for the provision of data to consumers.

11. Making generic product data generally available

Yodlee is generally supportive of the ACCC's proposed rule-making for the availability of generic product data.

12. Use of data

Yodlee agrees that ADRs must be transparent about how they intend to use the consumers' data, obtain the requirement consent for such use and adhere to that consent so that the user is neither harmed nor surprised by the ADR's use of their data.

The proposed rules for the situation where a consumer instructs their ADR to share their data with non-accredited entities is problematic for those use cases that do not contemplate such a transfer. Yodlee is concerned that this rule would require ADRs to implement process and technical features in their services that would normally not be included or would be included for a fee. This rule could, therefore, interfere with innovation and competition. Yodlee recommends this is left for subsequent versions of the Rules.

Regarding Rules for non-accredited service providers, Yodlee reiterates its recommendation that such service providers are accredited as intermediaries to ensure the ecosystem participates, including the consumer, are fully empowered and protected.

13. Rules in relation to privacy safeguards

Yodlee is generally supportive of the ACCC's proposed rule-making for applying the privacy safeguards.

14. Reporting and record keeping

Yodlee is generally supportive of the ACCC's proposed rule-making for reporting and record keeping.

15. Dispute resolution

Yodlee is generally supportive of the ACCC's proposed rule-making for dispute resolution.

16. Data Standards Body

Yodlee is generally supportive of the ACCC's proposed rule-making for the Data Standards Body.

Yodlee commends the ACCC's leadership on implementing Open Banking and for its outreach to the public as it considers how best to pursue an effective balance between consumer enablement and protection, competition and innovation in financial services.

Yodlee appreciates the opportunity to provide input on ACCC's request for comments and thanks the ACCC for its thoughtful and approach to ensuring an effective, and consumer-focused approach to Open Banking. Yodlee hopes the ACCC finds this input beneficial. We look forward to further collaboration with the ACCC on its efforts.

Sincerely,

Matt Walterhausen,
Vice President
Australia & New Zealand
Envestnet | Yodlee